Journal of Medical Systems (2019) 43: 320
https://doi.org/10.1007/s10916-019-1445-8

SYSTEMS-LEVEL QUALITY IMPROVEMENT

A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction

H. M. Hussien[1] · S. M. Yasin[1] · S. N. I. Udzir[1] · A. A. Zaidan[2] · B. B. Zaidan[2]

Received: 30 June 2019 / Accepted: 28 August 2019 / Published online: 14 September 2019

Abstract

Blockchain in healthcare applications requires robust security and privacy mechanism for high-level authentication, interoperability and medical records sharing to comply with the strict legal requirements of the Health Insurance Portability and Accountability Act of 1996. Blockchain technology in the healthcare industry has received considerable research attention in recent years. This study conducts a review to substantially analyse and map the research landscape of current technologies, mainly the use of blockchain in healthcare applications, into a coherent taxonomy. The present study systematically searches all relevant research articles on blockchain in healthcare applications in three accessible databases, namely, ScienceDirect, IEEE and Web of Science, by using the defined keywords 'blockchain', 'healthcare' and 'electronic health records' and their variations. The final set of collected articles related to the use of blockchain in healthcare application is divided into three categories. The first category includes articles (i.e. 43/58 scientific articles) that attempted to develop and design healthcare applications integrating blockchain, particularly those on new architecture, system designs, framework, scheme, model, platform, approach, protocol and algorithm. The second category includes studies (i.e., 6/58 scientific articles) that attempted to evaluate and analyse the adoption

Highlights

- Mapping the blockchain technology research landscape into a coherent taxonomy for healthcare applications
- Identification of the different types of blockchain technology used in healthcare applications
- Evaluation of the need to use blockchain in healthcare system
- Figure out the motivation to use blockchain technology in healthcare applications
- Highlight the open challenges and proposed solutions that hinder the use of blockchain technology in healthcare applications
- Recommend lists to improve the acceptance of blockchain integration with electronic record data to share medical data amongst different health and medical institutes
- Discussion of the purpose of blockchain technology with different applications in the healthcare sector

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ B. B. Zaidan
bilalbahaa@fskik.upsi.edu.my

H. M. Hussien
hassanalobady@gmail.com

S. M. Yasin
ifah@upm.edu.my

S. N. I. Udzir
izura@upm.edu.my

A. A. Zaidan
aws.alaa@gmail.com

[1] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Malaysia

[2] Department of Computing, Universiti Pendidikan Sultan Idris, Tanjong Malim, Malaysia

of blockchain in the healthcare system. Finally, the third category comprises review and survey articles (i.e., 6/58 scientific articles) related to the integration of blockchain into healthcare applications. The final articles for review are discussed on the basis of five aspects: (1) year of publication, (2) nationality of authors, (3) publishing house or journal, (4) purpose of using blockchain in health applications and the corresponding contributions and (5) problem types and proposed solutions. Additionally, this study provides identified motivations, open challenges and recommendations on the use of blockchain in healthcare applications. The current research contributes to the literature by providing a detailed review of feasible alternatives and identifying the research gaps. Accordingly, researchers and developers are provided with appealing opportunities to further develop decentralised healthcare applications through a comprehensive discussion of about the importance of blockchain and its integration into various healthcare applications.

Keywords Blockchain technology · Healthcare · Electronic health record (EHR) · Distributed ledger technology · Security · Privacy-preserving · Decentralised applications

Abbreviations

EHR	Electronic health record
EMR	Electronic medical record
HIPAA	Health insurance portability and accountability act
FHIR	Fast healthcare interoperability resources
HIE	Healthcare information exchange
PHR	Personal health record
PHI	Personal health information
TMIS	Telecare medicine information system
RPM	Remote patient monitoring
RHS	remote healthcare system
BSNs	body sensor networks
P2P	Peer to peer network
IoMT	Internet of medical things
IoT	Internet of things
DDoS	distributed denial of service
ECC	Elliptic-curve cryptography
IBE	Identity-based encryption
ABE	Attribute-based *encryption*

Introduction

Health care is an essential area of information technology (IT) because this sector has substantially evolved through electronic health record (EHR) [1–10], remote patient monitoring (RPM) [11–24 and population health management tools [25–32]. The medical data generated from these sources are vast and cumbersome, thereby leading to problems with the quality of medical data, such as complicated analysis, diagnosis and prediction and the risk in data confidentiality due to the increasing number of cybercrime cases [33–35]. Healthcare records or medical records have proven their importance to patients because of the valuable asset recorded in consonance with their point of view. Although sharing patient information amongst various healthcare providers through EHR may boost diagnostic accuracy, the health information repository may become a single point of failure and may be targeted by attackers resulting in ransomware attacks or denial of services. Therefore, data security is an important component of healthcare applications and plays a key role in protecting sensitive data. Healthcare data include patient details, which should not be disclosed to any untrusted third-party because of safety issues and misuse of information. This particular type of data comprise a list of patient information in medical repositories gathered from the beginning of patient illness to recovery. Such data also include a series of time-bound information recorded by hospitals (see Fig. 1). However, healthcare data or clinical information are spread amongst different medical repositories. Consequently, this feature may lead to the disclosure of patients' data and may not fulfil the legal requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). However, sharing and accessing medical records in EHR are extremely significant to receive intelligent and advanced medical services [36].

Emerging technological breakthroughs in blockchain and smart contracts are expected to provide promising solutions to secure patient data despite being shared and accessed through EHR. Shared health information exchange (HIE) relies on

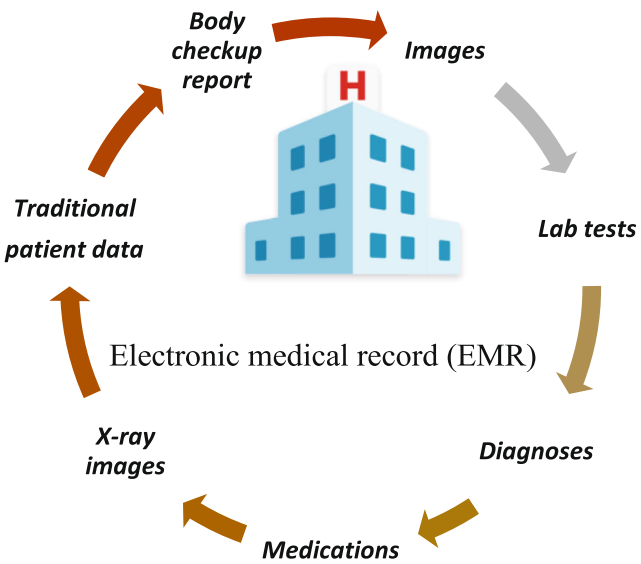

Fig. 1 Electronic Health Record Cycle

blockchain technology to remove restrictions that separate independent healthcare providers and make data on EHR universal and shareable. The integration of the healthcare system with blockchain may meaningfully contribute to human health and wellbeing [37–39]. Evidently, smart contracts can approve multiple signatures amongst patients and service providers, thereby allowing only authorised users or devices to access or attach recorded data in EHR. This feature ensures that patients can verify the authenticity of the data recorded in EHR whilst maintaining the anonymity of their real identity. Smart contracts also enable interoperability through collaborative version control to maintain record consistency. Additionally, smart contracts can provide researchers with access to some personal health information (PHI) and enable automatic micropayments to benefit patients and healthcare providers involved in the blockchain network. However, the majority of the applications developed on the public blockchain structure are limited by immature infrastructure and high development cost. Policy concerns have also been raised regarding the requirements of HIPAA and the ability of patients' participation to publish their personal information in the public blockchain network [40].

Blockchain technology is a fully distributed ledger in a peer-to-peer (P2P) platform that utilises advanced cryptography protocol to securely host applications. In 2008, Satoshi Nakamoto proposed this technology, which was implemented the following year in the form of a P2P electronic cash system, such as the cryptocurrency bitcoin [41]. The Ethereum blockchain offers the idea of a complete programming language in a blockchain environment through the implementation of new decentralised applications in financial or non-financial areas [42]. Smart contracts are decentralised applications that run via Ethereum or other blockchain platforms and support a complete programming language. Moreover, a smart contract is a complete program implemented in a decentralised manner and often handled with valuable digital units. Solidity is the most mature high-level programming language that supports writing a smart contract, through which miners can run user-defined decentralised applications [43]. Issues that concern blockchain or smart contract are related to security, privacy and scalability because every transaction on the main network is exposed to the public. Consequently, this situation exposes data to many threats. The Ethereum platform poses a serious challenge in the implementation of specific-use cases because the application runs on a P2P network for smart contracts. Moreover, the full source code of the application is visible to everyone in the network. To illustrate, one hacker exploited one bug in 2016 and stole over $50 million worth of Ether [44]. The development of decentralised applications on the blockchain network may enable anyone in the network to access transaction data owing to the transparent feature of the blockchain. This feature has led to restrictions on an entire range of privacy-based applications in the healthcare sector. Therefore, the impact of blockchain technology and smart contract suffers from the three factors of security, privacy and scalability [45–47]. The current systemic review seeks to provide valuable insights into the technological environment and assist researchers to understand the options and gaps present in healthcare applications based on blockchain. Subsequently, researchers could plan a research landscape through a coherent classification to identify blockchain features that are integrated into healthcare applications.

This study mainly contributes to the integration of existing healthcare applications and blockchain technology. We discuss this integration through various components, such as new architecture, system designs, framework, scheme, model, platform, approach, protocol and algorithm, upon the structure designs of decentralised healthcare application. Given that the majority of the associated problems relate to the integration of blockchain technology into healthcare, the proposed solutions are examined to meet the system requirements. This study also discusses the importance, motivation and challenges of blockchain technology and provides recommendations for future research and trends from the healthcare perspective. The remainder of this paper is organised as follows. Section 1 presents basic information on blockchain and evaluates the necessity of using blockchain in the healthcare system. Section 2 discusses the research methodology of the systematic review used in this study. Section 3 presents the results and discusses related studies that use blockchain in healthcare applications. Section 4 provides the results of the systematic review in terms of motivation, challenges, recommendations and future research direction. Lastly, Section 5 concludes this research.

Blockchain overview

Blockchain technology is a decentralised digital ledger that provides an opportunity to record and share information in a community. Each entry is transparent and searchable, thereby enabling community members to view its history. The cryptology in blockchain substitutes third-party intermediaries as trust keeper, whilst all participants run complex algorithms to certify the integrity of an entry. This technology can provide a new model for HIE by attempting to decentralise EHRs, thereby improving system efficiency and security. Although blockchain technology is not a panacea, this technology has been led to a rapidly evolving field in the industry. Blockchain is important because it brings trust to P2P networks. The key component of blockchain technology includes consensus mechanism, distributed ledger and public key cryptography. These components communicate and coordinate over a distributed network of devices owned and maintained by multiple entities. The blockchain platform adopts a decentralised architecture, in which all network members achieve the

required application purpose. A system state perceived in one machine is replicated through the execution of consensus mechanism logic and P2P networking protocol to all other devices in the network. The replicated state information is stored in the context of blockchain, which is referred to as distributed ledger and is uniformly managed by the members of the network. Thereafter, the public key is used with a hash function to create a public address that users use to send and receive valuable assets. The private key, which is used to sign a digital transaction to ensure that the transaction's origin is valid, is maintained confidential. Each block in the blockchain consists at least one transaction, signature of the block validators and reference to the previous block along with block headers. Blockchain provides opportunities for the standard architecture integration to radically transform our method of addressing various disciplinary systems issues, such as the Internet of Things (IoT) [48, 49], supply chain management [50] and Industry 4.0 [51]. This advantage is due to the decentralised nature of blockchain technology, in which many users own an entire database of a particular system. These decentralised database systems based on blockchain can reduce one of the cheating sources of database manipulation. Blockchain technology and cryptocurrencies have received significant industrial and academic attention [52]. Notable factors and opportunities will revolutionise the healthcare sector through its integration with blockchain technology [53].

- **Decentralised storage:** Blockchain stores information transparently and delivers it to third parties upon the consent of the originator. One of the most beneficial features of decentralising information storage is the retention of multiple copies of such an information in multiple locations.
- **Consent**: Consensus algorithm controls the access, storage and distribution of information within a network. If any decision is agreed upon by all participating parties in a network, then changing the data will be allowed.
- **Immutability**: Changing or altering data is impossible. When the information is stored in a particular block in the chain, modifications or changes are no longer allowed.
- **Increased capacity**: Blockchain does not support any mediation, has limited complex data authorisation in a network and efficiently preserves data privacy in some specific uses of healthcare applications.

Types of blockchain for healthcare system

Blockchain architecture describes the connection of nodes that run on a network for transaction or validation purposes. If the members of the nodes involved in blockchain are already known to the network, then such a blockchain is referred to as permissioned, such as Hyperledger Fabric [54] and Ripple [55]. When a system is open to the public, any individual or organisational node can be a member of the network; hence, this blockchain is referred to as public, such as Ethereum [42] and bitcoin [41]. The data structures of blockchain enable the creation and sharing of a digital ledger for distributed transactions between a P2P network of nodes. Figure 2 illustrates the blockchain architecture. Users are allowed to immediately conduct and verify transactions without a central authority. This decentralised manner significantly reduces the cost of system configuration, maintenance, modification and arbitration in communication because this process should only be performed once in a central location. Despite high efficiency in many situations, this type of system would induce a single or extremely limited set of failures and suffer from scalability problems [56].

Unpermissioned or public blockchains

A public blockchain is considered an unpermissioned ledger (e.g. Bitcoin or Ethereum) when nodes interconnected to the network are accessible to anyone via the Internet. Accordingly, any network member can validate a transaction and participate in the approval process through the consensus algorithm, such as proof of work or proof of stake. A blockchain is primarily designed to securely eliminate centralised authority in a digital asset scenario exchange. A block of chains is established in P2P transactions to ensure decentralisation. Each transaction is linked to the previous transaction through the cryptographic hash Merkle tree as a block of the chains prior to being entered into the immutable database of the system. Therefore, the blockchain transaction ledger is compatibility and synchronisation with every node in the network. Anyone with a computer and Internet connection will be allowed to register as a node and offered a complete blockchain record. The repetition of synchronised public blockchains with each node in the network makes the system completely secure. However, this type of blockchain has undergone a gradual and inefficient process of validating transactions. Huge electrical power is needed to validate each transaction and power should increase significantly when each node is added to the network [57].

Permissioned or private blockchains

This type of restricted blockchains allows a middleman to be relatively returned. Private blockchains have strict management of a network's data access authorisation. The membership of nodes in the P2P network cannot participate in verifying and validating transactions without permission. Instead, only companies or organisations can verify and validate every transaction in the network. A high level of efficiency will be provided in the verification and validation of transactions in

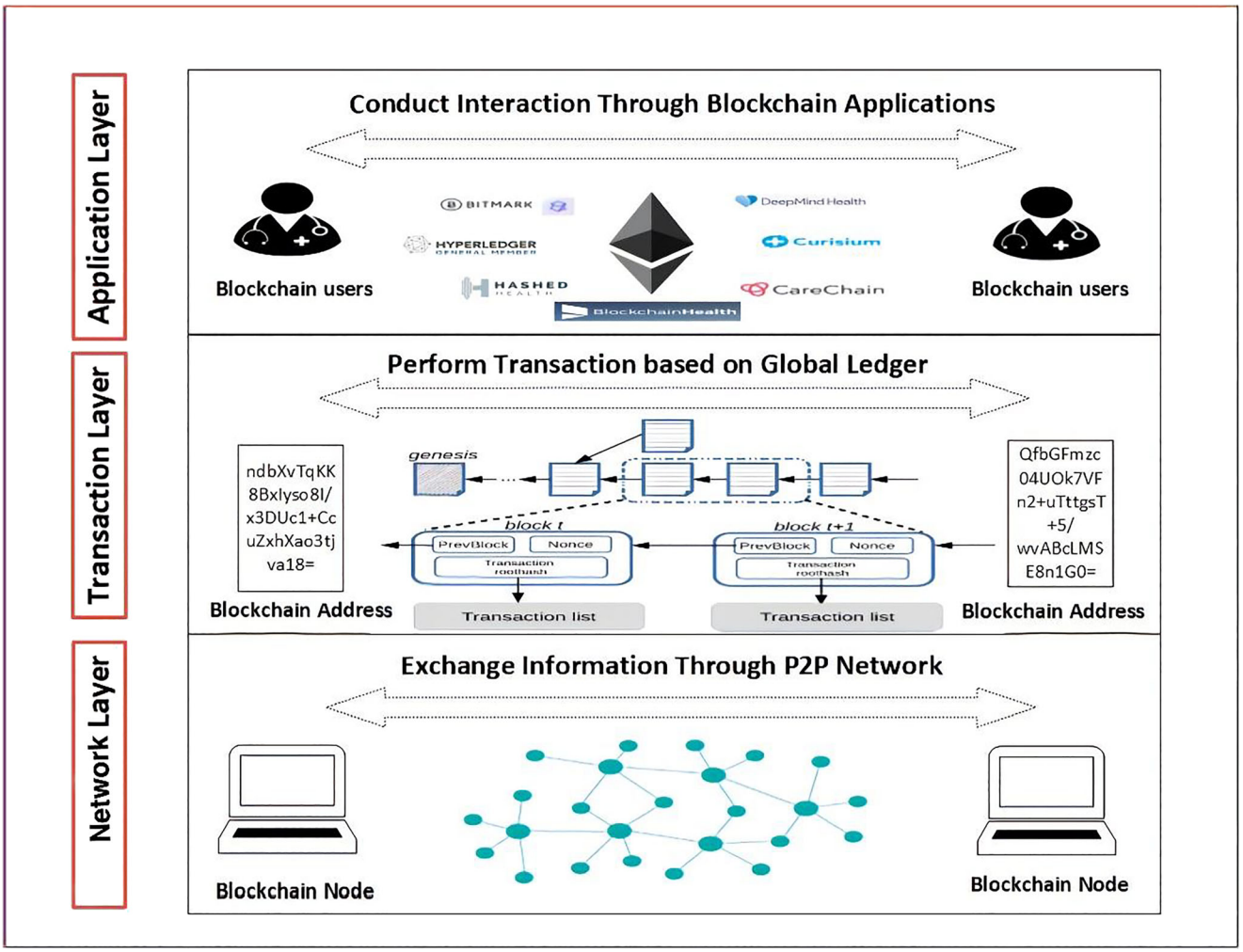

Fig. 2 Blockchain Architecture [47]

private blockchains. A considerable limitation of private blockchains is the inability to provide a decentralised system for secured databases, which is made available by public blockchains [58].

Consortium or federated blockchain

A consortium is an integration amongst public and private blockchains and can be considered partially decentralised. The detail of each data transaction in a blockchain network allows to be either public or private and nodes have the authority to be selected in advance. Consortiums and private blockchains are different from each other. Generally, consortium blockchains are the hybrid models amongst highly trusted private blockchains and untrusted entity models of a public blockchain. Private blockchains can be accurately recognised as a traditional centralised systems but with a strong cryptographic model to verify and validate transactions in the network. The development of the consortium blockchains in terms of reliability, authenticity and accuracy has yet to be clearly described [59].

Evaluation of the need to use blockchain in the healthcare system

Blockchain features have brought several benefits to numerous industrial fields and can become an advantageous tool in healthcare system applications. However, blockchain technology may not be the ideal choice to solve every problem in industrial fields unless the application requires decentralisation. Blockchain technology may be useful if an application is required to be decentralised. For example, this situation occurs when an application is enhanced by running on a P2P network of computers instead of an individual device. Although certain healthcare applications may not be required to be decentralised, the majority of such applications may have benefited from an untrusted centralised system. To illustrate, a private network structure that relies on traditional databases

typically provides rapid and powerful tools for many applications. Therefore, certain features in healthcare application should be recognised before deciding whether a blockchain should be used. In blockchain integration, a general framework has been proposed to determine the use of blockchain in the healthcare industry. The following requirement analysis should be performed in detail.

Firstly, data transformation must be performed in a trusted environment. Current data transformation systems can be used to automatically perform multiple methodological tasks, thereby accelerating transactions amongst parties. Although a trusted network can be established through traditional healthcare application systems, two disadvantages have emerged. These situations often involve higher transaction fees than public blockchains and should be trusted nearly blindly without questioning the aspects of safety, internal policies or ethics [60].

Secondly, transparency and the tamper-proof features of blockchains can support public transaction logs. These logs include timestamp information that may be publicly disclosed and checked by all entities that interact with the blockchain. Healthcare applications can strictly follow this concept and store each transaction involved in a blockchain network to accurately audit and track medical records. Another advantage related to healthcare application involves requiring P2P connections to share data amongst parties concerned with the industrial processes. This situation is extremely common in the EHR structures that collaborate with one another to discover certain events or perform tasks. These features are traditionally provided by databases. However, the essential component is security, particularly when data are visible publicly on blockchains, thereby possibly leading to attacks on their availability or data privacy.

Lastly, the robustness of the distributed system should be achieved for dependability. Potential alternatives could accomplish the needs of systems provided by clouds or server farms. However, problems arise from lack of trust in the organisation that manages an infrastructure, such as cloud, or privacy requirements determined by the client [61]. Trust service providers must consider the infrastructure and defence in the storage of data. Legal and privacy concerns must be valued in countries where privacy and security data are not guaranteed. Figure 3 presents a flowchart that can be used as a general guide. This flowchart can determine the appropriate time to maximise the blockchain technology in a healthcare application.

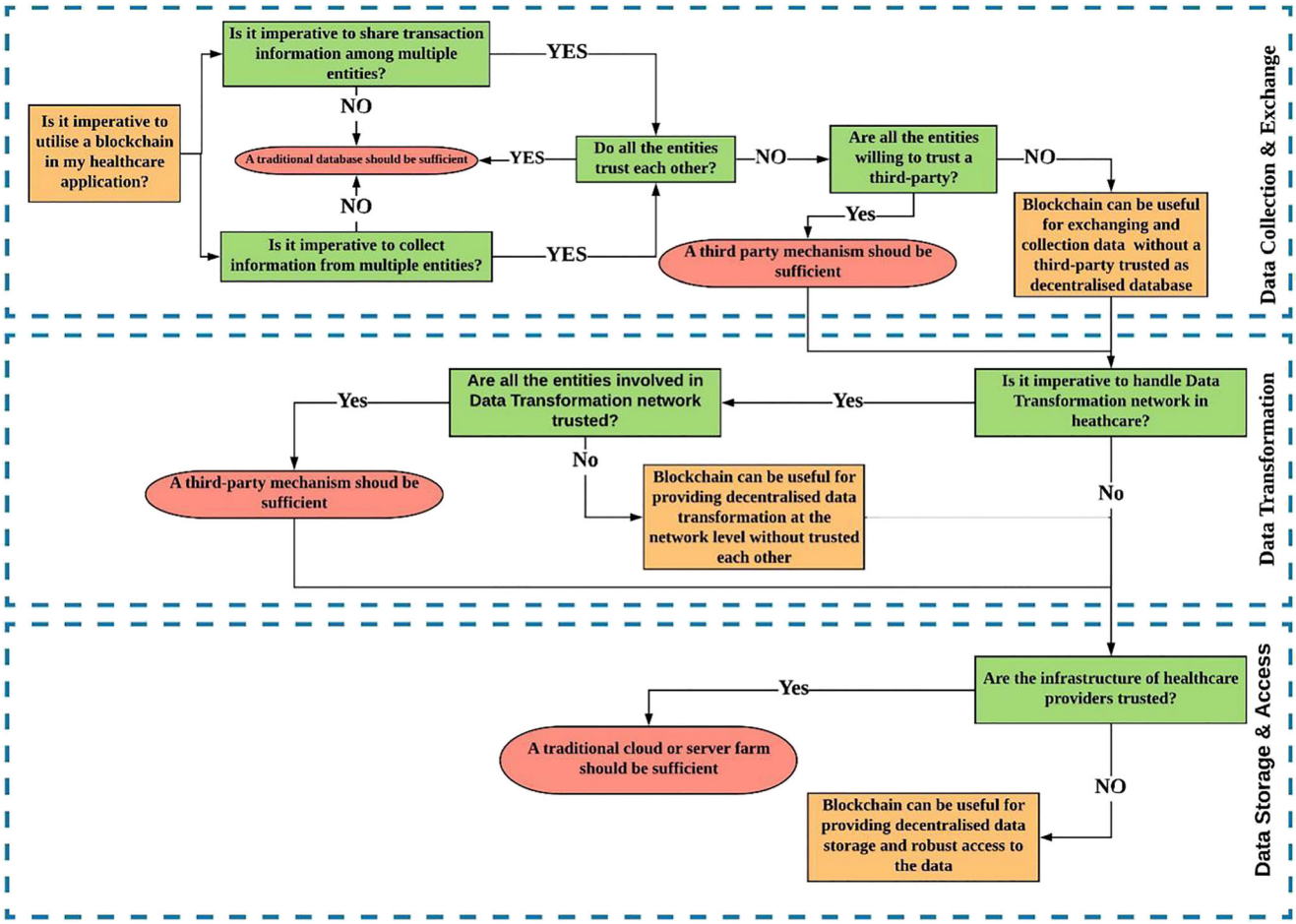

Fig. 3 Evaluating the Use of Blockchain Technology in a Healthcare System

Research methodology

This study performed a systematic review of and described the state-of-the-art integrated blockchain technology within the healthcare sector. Research questions and motivations provided an improved understanding of blockchain technology in relation to healthcare. Table 1 presents the research questions, motivation, challenges and recommendations.

Research objectives

This study examined and reviewed the latest research on the use of blockchain technology in healthcare applications. The objectives of this systematic literature review are as follows:

- determine the classification and categories of the relevant studies on the bases of different case studies;
- determine the motivations, challenges and recommendations of integrated blockchain technology with health care to enhance this technology's effectiveness; and
- investigate issues relevant to blockchain integration in heathcare applications and propose solutions in the scope of this study

Data sources

Systematic search was conducted using the following electronic databases: Web of Science (WOS), ScienceDirect and IEEE Xplore (see Fig. 4). These databases were selected on the bases of numerous gathered journals and conferences on emerging topics, including blockchain.

Study selection

The selection process of the relevant studies is relatively difficult, particularly if different areas of research are considered. This step is the most important aspect and may be the most overlooked in exploring a certain topic. The first stage was conducted by screening titles and abstracts to exclude irrelevant and duplicate research articles [62–65]. The second stage of the methodology was full text reading of the selected research articles [66–68].

Systematic literature review search

This study developed a query utilising particular key words to fulfil the research questions and objectives of our study. This step was conducted on 28 February 2019 in WOS, ScienceDirect and IEEE. We used the query '("blockchain" OR "blockchain") AND ("healthcare" OR "health" OR "medical" OR "medicine" OR "m-health" OR "mhealth" OR "ehealth" OR "e-health" OR "telehealth" OR "EHR" OR "EMR")'. With the advanced search selection in the database, we chose conferences and journals without considering other selections, such as books and book chapters. Figure 4 illustrates the search query, selection and exclusion and inclusion of the research articles.

Eligibility criteria

This study concentrated on blockchain technology in healthcare by including all research articles that met the criteria presented in Table 2 and Fig. 4. The research landscape on blockchain technology in healthcare application is divided into three categories with general taxonomy as the primary target (see Fig. 5). We determined these categories from a comprehensive study of surveys and review literature sources. After excluding duplicate research articles, we excluded studies that failed to fulfil the criteria specified [69–73]. Similarly, a study was included in this review if it successfully met the criteria provided in Table 2.

Table 1 Research Questions and Motivations

Research Questions	Motivations
RQ1: What is the current status of the systematic literature review on the integration of blockchain in healthcare applications?	Blockchain technology has been successfully implemented in various industries. The architecture and essential aspects of blockchain in healthcare applications should be understood.
RQ2: What is the distribution of research articles published in this topic based on year of publication, author nationalities, publishing house, purpose of using blockchains in healthcare and problems and proposed solutions and contributions?	The challenging task in healthcare applications is essential and may be improved by blockchain. Moreover, blockchain may enhance data security, privacy, sharing, interoperability and integrity and real-time update and access.
RQ3: What are the challenges and motivations of utilising blockchain in healthcare applications?	The best uses of blockchain in healthcare applications can be determined.
RQ4: What recommendations can be followed to ensure that the blockchain is successfully used in healthcare applications?	Information on blockchain technology that is effectively implemented in healthcare applications can be collated.

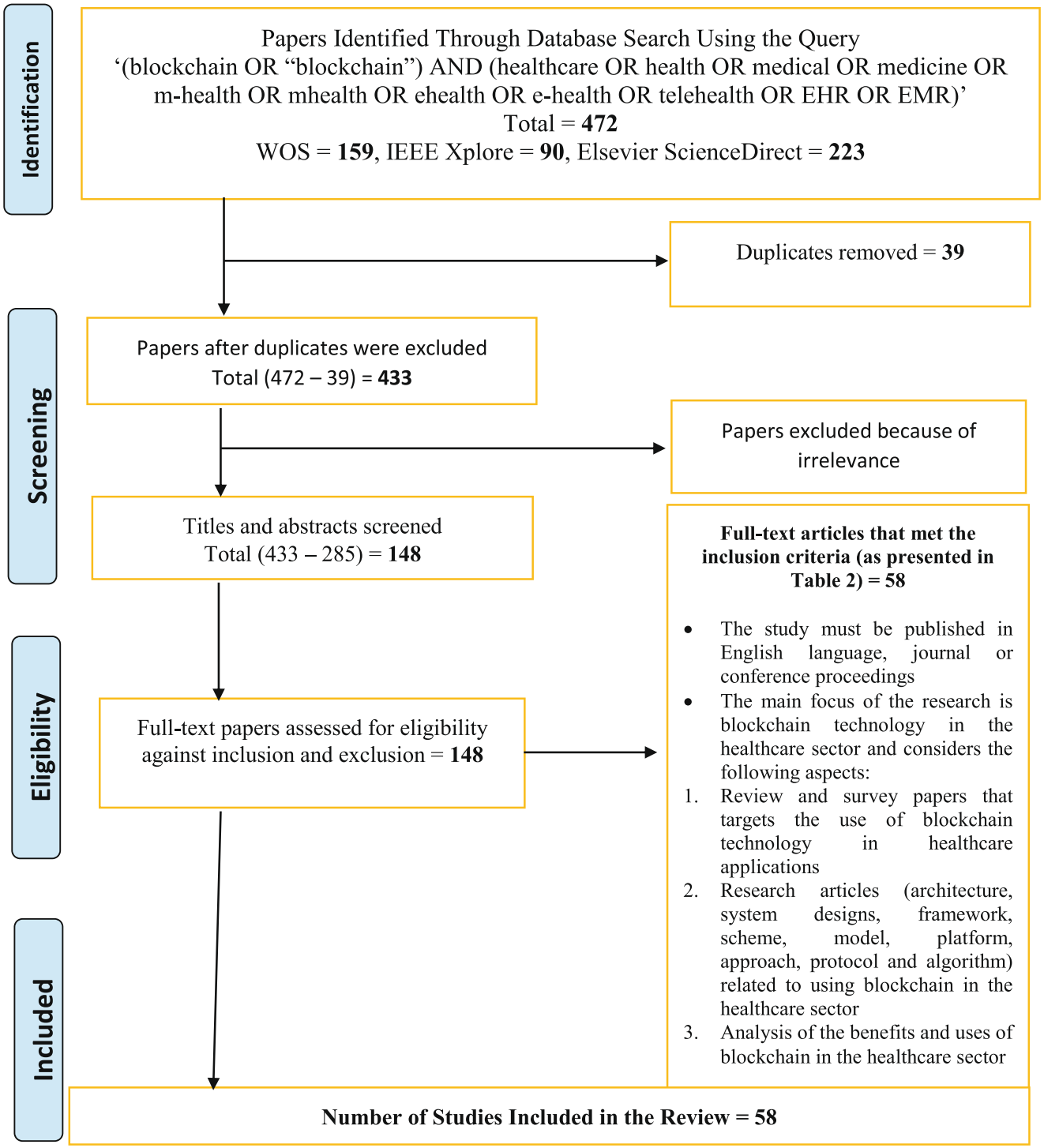

Fig. 4 Flow Diagram of the Study Selection, Including Search Query and Inclusion Criteria

Research article results on blockchain in healthcare applications

This section presents the results and discusses the related research articles that investigates the use of blockchain in a healthcare application system. Figure 5 describes the taxonomy and categorisation of selected studies into three main parts. The first part includes the development and design, which covers all articles that are proposed as new architecture, system designs, framework, scheme, model, platform, approach, protocol and algorithm of a blockchain-based healthcare system. The majority of the research articles (i.e. 43/58 scientific articles) are categorised under this part. The second part includes conducted studies (i.e. 6/58

Table 2 Inclusion and Exclusion Eligibility Criteria

Criteria	Specified Criteria	Grey Literature
Inclusion	Review and survey papers relevant to the use of blockchain technology in healthcare applications; Research articles (architecture, system designs, framework, scheme, model, platform, approach, protocol and algorithm) relevant to healthcare applications based on blockchain; Analysis of the advantages and uses of blockchain in healthcare applications	Scientific reports that present blockchain as the main contributor in the improvement of the current healthcare state
Exclusion	Thesis, books and book chapters • Non-English articles • Unrelated articles	Unrelated articles, non-English articles, theses, books and book chapters were excluded

scientific articles), which consist of evaluation studies on adopting blockchain in the healthcare system and analytical studies covering the new model that leverages the enhancement of the blockchain-based healthcare system. The third part targets surveys and reviews (i.e. 6/58 scientific articles) relevant to blockchain in healthcare applications.

Coherence taxonomy

This section presents the categories and subcategories of the relevant research articles. The definitions of each subcategory are provided on the bases of the research paper classification and types of solution proposed in the healthcare blockchain technology (see Fig. 5).

Development and design

Blockchain technology has the potential to transform the healthcare system by placing patients in the centre of the ecosystem environment whilst enhancing system security, privacy and interoperability. This section describes the development and design that include the architecture, system designs, framework, scheme, model, platform, approach, protocol or algorithm used for healthcare applications based on blockchain. The current category is classified into the following subcategories on the basis of taxonomy.

Electronic health record (EHR) EHR is a popular method of storing patient data amongst healthcare providers (e.g. hospital). However, privacy and security issues of the current EHR system limits the provision of individual patients' data summary from the various databases of healthcare providers. **Reference** [74] proposed a new system based on blockchain called MedBlock to handle the patient database stored in EHRs. The MedBlock system is a distributed ledger, in which patient data can be accessed and retrieved efficiently and securely. The enhanced consensus mechanism is compatible with EHRs without significant energy consumption and congestion within the network. MedBlock offers high-level information security that combines custom access control protocols with symmetric encryption. **Reference** [75] proposed a system prototype for identity and access management and uses the Hyperledger Fabric blockchain to support digital EHR authorisation and authentication. The proposed solution provides proof of concept on the basis of healthcare providers' use of an EHR scenario, where patient data should be immutable or auditable. For example, physicians in Denmark conduct basic authorisation and authentication operations of the proposed system in 2 to 3 s with an initial blockchain size of approximately 3.8 MB. **Reference** [76] proposed a new secure EHR system to remediate third-party dependence by presenting a new storage and security strategy based on blockchain decentralisation network. The proposed system intends to provide a solution to notify healthcare providers of the slightest alterations in patients' database. This system lowers the rates of medical error and enables users to consult transparently if they have been authorised. **Reference** [77] recommended a new framework (i.e. BHEEM) that relies on blockchain to effectively store and maintain EHRs. The BHEEM framework offers efficient and secure access to medical data in EHRs to patients, healthcare providers (e.g. hospitals) and third parties, whilst protecting private patient data. The current study aims to maintain the security and privacy concerns of third parties, providers and patients in EHRs.

Reference [78] proposed a novel decentralised attribute-based signatures (ABS) scheme for blockchain healthcare applications, thereby preserving the privacy of the signer identity authentication within the EHR system. An effective on- and off-chain collaboration storage model has been developed to ensure the efficient storage and verification of EHR data sharing amongst multiple healthcare providers (e.g. hospitals). The decentralised storage system based on blockchain guarantees that the medical information stored or shared in EHR is not manipulated, unforgeable and verifiable. **Reference** [79] presented an ABS-based scheme involving various authorities in decentralised EHRs to maintain the confidentiality of patient data. Various authorities lack intermediaries and could generate and distribute the public/private key of patients to avoid the key escrow problem, comply with the mode of distributing blockchain structure and assure data anonymity and

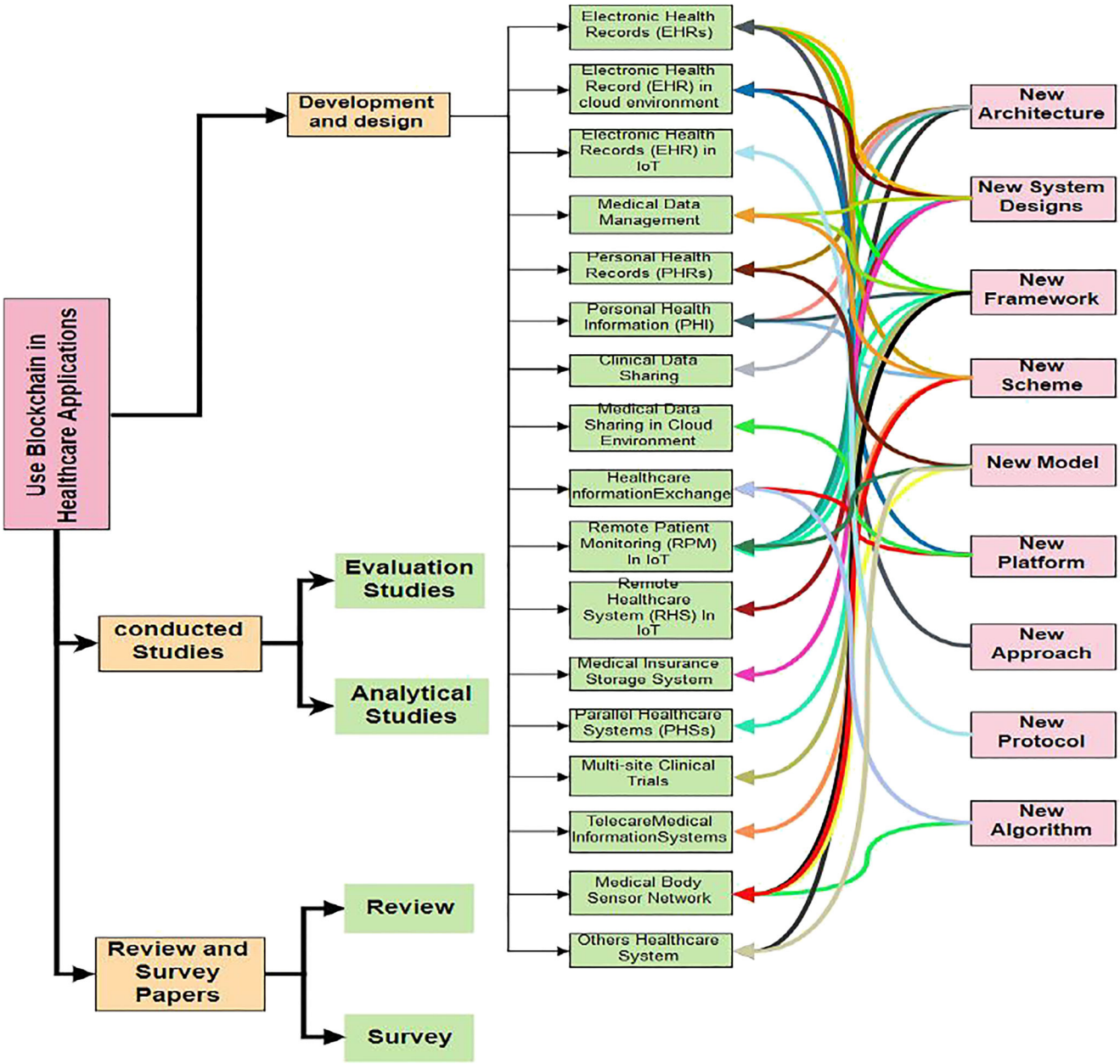

Fig. 5 Illustration of the Taxonomy of Blockchain Technology in Healthcare Applications

immutability. This protocol is resistant to collusion attacks in the N-1 corrupted authorities by implementing the bilinear Diffie–Hellman assumption in the sharing of the secret pseudorandom function seeds amongst authorities. **Reference** [80] proposed an EHR scheme to develop a secure and efficient mechanism of data accessibility for existing blockchain-based medical systems. The proposed system can fulfil the requirements of confidentiality, integrity and authentication that are set by the elliptic curve cryptography (ECC), which provides more lightweight public key cryptography operations than classic discrete logarithms or Rivest–Shamir–Adleman systems. Moreover, **Reference** [81] proposed a blockchain-based approach to build a decentralised healthcare network for secured EHR sharing. This proposed approach also uses a signcryption mechanism to provide data authenticity and a flexible method to access shared data. Attribute-based authentication generates a proven trace of users who have requested access to patient EHRs. The main concern of the aforementioned proposal is to resolve the security issues of confidentiality, access control, privacy and audibility of data stored in EHRs, as well as enable patients to obtain easily accessible, integrated and transparent data. **Reference** [82] proposed a new framework based on the blockchain Ancile for patients, healthcare providers (e.g. hospitals) and third parties to securely, interoperably and efficiently access medical data stored in it, whilst preserving the confidentiality of sensitive

data. The proposed framework utilises smart contracts in an Ethereum blockchain to increase access control and data obfuscation. Advanced cryptographic techniques provide additional security. The combination of artificial intelligence (AI) with blockchain in EHR provides a secure management system. **Reference** [83] proposed a new framework for the use of AI and blockchain. This current framework was modelled with the constrained goal model (CGM) to meet the system requirement.

Electronic health record (EHR) in a cloud environment A cloud storage system is critical for the efficient and convenient sharing of medical data in EHR with multiple healthcare providers (e.g. hospitals). The storage of medical data on an EHR-cloud server is subject to a variety of security threats, including those related to data integrity, data privacy and authentication. Consequently, **Reference** [84] proposed a secure EHR system based on cryptosystem and blockchain to support fine-grained access control and ensure secure authentication that is systematic and reliable and confidentiality of medical data in the EHR cloud. The proposed system is based on a new combined cryptosystem called C-AB/IB-ES, which is used to encrypt medical data and implement digital signatures using identity-based encryption (IBE) and attribute-based encryptions (ABE). This system substantially enables the management of the EHR system and does not need a variety of cryptographic schemes for various security requirements. The developments in the system utilise the basic paradigm of decentralisation in blockchains to ensure integrity and traceability of medical data records in EHR. **Reference** [85] proposed a blockchain-based platform for the storage and management of EHR within a cloud environment and comprise three main elements: doctors, patients and health insurance providers. This platform uses P2P architecture and eliminates third party necessity. After encryption, any transaction that is carried out throughout the network is fragmented and stored in different nodes. This feature ensures that transactional medical data are privately updated, thereby retaining data integrity with each new transaction in the blockchain ledger. **Reference** [86] proposed a new system (i.e. blockchain-based privacy-preserving data sharing (BPDS)) to protect the privacy of EHR data sharing based on a blockchain consortium, which stores medical information in the cloud and record indexes are entered into (tamper-proof) blockchain ledgers that address potential security risks of centralised data storage. The joint design of the access control mechanism and content extraction signature scheme ensure strong privacy preservation in data sharing and the use of smart contracts for predetermined permissions to ensure secure access to data.

Electronic health record (EHR) in IoT The multitier IoT–EHR framework proposed in **Reference** [87] aims to achieve the optimal protection of patient confidentiality through the application of the blockchain concept in communication entities of electronic health platform based on pseudonym-based encryption with different authorities (PBE-DA). Developments in the framework of the PBE-DA protocol can ensure patients access through the anonymous checking or updating of their sensitive EHR data.

Medical data management Dissemination of patient medical records lead to several risks to their confidentiality because malicious activity in these records may cause serious damage in finances and reputation. The existing approaches in medical data management have been proven insufficient in terms of medical data sharing, data management and protection of recorded data. Therefore, **Reference** [88] proposed the MeDShare system for data authenticity, auditing and protection in the exchange of medical data in an untrustworthy environment amongst multiple organisations, such as research and medical institutions. MeDShare was developed on blockchain technology using smart contracts to determine data behaviour effectively and detect cyberattacks of the entities' offending behaviour. **Reference** [89] developed a system that makes the technology secure, private and auditable by using the unique features of blockchain technology to share and manage medical data. This system is enhanced by requesting data entities to check the integrity of the medical data with the assistance of a blockchain infrastructure. The developments in the system have increased its value in terms of the integrity of patient data, anonymity of patients, automation of workflows, audit and accountability. **Reference** [90] proposed a new data preservation system (DPS) to use blockchain as a reliable storage solution, thereby ensuring that the stored data are primitive and verifiable, whilst maintaining user privacy. This system uses the combined blockchain with DPS to support frameworks and perpetually preserve important data, whilst the authenticity of data can also be verified if suspected manipulation occurs.

Reference [91] proposed a secure decentralisation system using a hyperledger blockchain (i.e. MediChainTM) to facilitate the efficient exchange of medical data amongst patients, caregivers and medical practitioners, whilst enabling a secure protocol for private medical data transfer. Developments in the decentralised architecture provide scalability to manage and assess medical data and enhance the security of these assessments. **Reference** [92] introduced a new blockchain-based prototype system for medical data management. This system is used to maintain a shared key that could be reconstructed by legitimate parties prior to starting the diagnosis and treatment process. Data in the diagnosis and treatment processes are encrypted using the sibling intractable function families (SIFF). Furthermore, data are entered into the Hyperledger Fabric blockchain to fulfil the requirements of medical data in terms of integrity, availability and privacy. Therefore, the conceptual medical record access and sharing mechanism framework proposed by **Reference** [93] is suitable for a

system operating within a regulated healthcare jurisdiction. This combination enables the development of a decentralised holistic care cycle, in which patient health data can be shared. However, the integrity of medical records and privacy protection is constantly conflicting, whilst interoperability is permitted. Additionally, a framework for cross-domain image sharing is developed in **Reference** [94], in which a blockchain functions as a distributed storage to establish a ledger of radiological studies and patient permissions. The development of this framework eliminates third parties to protect medical data and fulfil the criteria in an interoperable health system and generalise fields beyond medical images.

Personal health record Personal health record (PHR) is the management system of medical health records and patients are often unable to control their data stored in EHR databases. **Reference** [95] discussed the proposal of a new blockchain-based architecture called OmniPHR to manage PHR for patients and healthcare providers. OmniPHR presents a new architecture that could support distributed PHR, in which patients maintain their health history in a standardised view through any device. Health providers can monitor patient data from different healthcare organisations. **Reference** [96] developed a new model for sharing medical data on the bases of blockchain technology and proxy re-encryption to provide secure PHRs. This study highlighted six significant flaws in the use of blockchain to develop a PHR system. The proposed model resolves the first three problems of data privacy on the chain, limited storage of medical data and cancellation of consent.

Personal health information Reference [97] introduced a health data control gateway (HGD), which is a novel health architecture based on blockchain technology. HGD enables patients to easily and securely control and share their data without disclosure. The development of this system provides new potential for improving the intelligence of healthcare systems whilst protecting patient privacy. Centric access was performed to ensure the capability of patients to control their medical data and indicator centric schema was able to organise a variety of personal medical data types in a practical and easy manner. **Reference** [98] proposed a new scheme based on blockchain designed to ensure the confidentiality and security of personal data in the blockchain-based secure and privacy-preserving PHI sharing protocol for improved diagnosis in EHR. The consortium and private blockchains were combined into the system to achieve health record sharing and the proof-of-conformance consensus mechanism was designed to construct the verification of blocks. The development of the proposed PHI protocol ensured privacy preservation and robust security of stored data, whilst maintaining a secure search and support timeout session in EHR. **Reference** [99] designed an entirely new framework (i.e. i-Blockchain) to use personal health data as an individual-centric hub based on blockchain. The development of i-Blockchain combines the cold and hot storages by the adopted private and public keys, respectively, to improve the security of personal health data exchange.

Clinical data sharing Clinical data sharing should be secure and scalable for improved collaborative clinical decision-making, particularly in providing patients with effective treatment. Patients may have visited multiple medical clinic offices during their lifetime. These clinics should be able to exchange patient data in a timely and confidential manner to ensure that these facilities have access to the latest knowledge of patient conditions. **Reference** [100] proposed a new architecture that relies on the blockchain to satisfy the requirements of the Office of the National Health Information Technology Coordinator (ONC) by including the fast health interoperability resources (FHIR) HL7 standard for shared clinical data. **Reference** [101] developed a new architecture for a decentralised ecosystem of healthcare data based on blockchain. This system can be integrated with large volumes of clinical data and protect data confidentiality by utilising the Exonum blockchain framework for state-scale use in the healthcare system.

Medical data sharing in a cloud environment Medical data stored in a cloud environment are consistently exposed to cyberattacks because of complete lack of security, privacy, integrity, pseudonymity and accountability. Therefore, **Reference** [102] presented a medical data privacy preservation platform based on blockchain technology by determining a set of privacy and security requirements for medical data management systems. This platform is a decentralised approach that uses ECC to encrypt patient data and ensure network pseudonym to address the effects of such attacks. The developed platform leverages integrity, accountability, authenticity and privacy in the cloud medical data based on blockchain technology. **Reference** [103] developed a new framework for the secure management of shared and patient data based on cloud and blockchain storage. The development in the framework addressed the third-party storage of medical data. The use of blockchain is considered a storage supply chain, in which each transaction can be confirmed, manipulated and accounted for in case security and privacy are necessary for the system.

Healthcare information exchange (HIE) The existing blockchain in healthcare information exchange (HIE) considers only the storage and sharing of EHR data. Hence, various valuable personal health data and stored EHR data are disregarded into cloud environments with a complicated access control mechanism to prevent unwanted data dissemination. Nevertheless, this type of network architecture heavily relies on cloud environments security. **Reference** [104] proposed a new platform that relies on the BlocHIE blockchain for healthcare information exchange by considering two types of medical data (i.e. EHR and PHI). BlocHIE has two interconnected blockchains based on the

identification of the different requirements to store and share medical data. The first blockchain is EHR-chain for EHR and the second is HIE-chain for personal healthcare data. The development of the EHR-chain has integrated off-chain storage and on-chain verification techniques to ensure improved confidentiality and authenticity.

Remote patient monitoring in IoT IoT offers services for a wide variety of applications without human involvement, such as RPM. The challenges in designing IoT-based RPM systems include aggregating large streams of data whilst ensuring patient confidentiality. **Reference** [105] proposed a tier that relies on an end-to-end architecture with a patient centre agent (PCA) as the centrepiece for continuous RPM. The network of PCA-based blockchains maintains the privacy of data streaming from body area sensors and stores them securely. The improved architecture allows medical data to be inserted into the personal blockchain to be shared in EHR amongst different health organisations, whilst maintaining privacy. **Reference** [106] proposed a patient IoT-RPM based on smart contracts to manage medical devices to secure sensors when communicating with a smart device by which smart contracts record all events in the blockchain. This smart contract system has a secure immutable ledger. Moreover, automatic health event notifications would resolve security vulnerabilities associated with RPM and be trustworthy for patients to wear medical devices. **Reference** [107] proposed a novel framework of modified blockchains for IoT-devices based on their distributed nature and other additional network security and privacy properties to provide secure management and analysis of big data in RPM. These additional security and privacy properties in the framework are the integration of private and public keys, blockchain and many other lightweight cryptographic primitives to improve the access control of patients. This solution is provided to secure and anonymise IoT data and transactions across a network in the blockchain. Additionally, **Reference** [108] designed the FHIR chain model to enhance support for collaborative clinical decisions in the IoT-RPM by using blockchain technology and FHIR standards. The FHIR chain model and public-key cryptography addressed the challenges of the five major ONC interoperability requirements, namely, authentication, user identity determination, data access authority, data exchange protection and consistent data formats and system modularity.

Remote healthcare system in IoT A remote healthcare system (RHS) is proposed on the basis of smart contract in the Ethereum blockchain to recognise and protect individuals and information generated by devices. RHS is designed for healthcare providers (e.g. hospitals), physicians and patients to measure the health status of patients using sensors. This information is automatically entered into the blockchain. **Reference** [109] explained that a processing mechanism aims to efficiently and moderately store medical device information in accordance with the health status of patients.

Medical insurance storage system Insurance companies have constantly relied on verifiable and tamper-resistant records of patient expenses, and companies should know nothing about the records of expenses. Otherwise, a risk of leakage may occur. Therefore, **Reference** [110] proposed a new system based on the MIStore blockchain to store medical insurance data that will provide high-level credibility to individual patients. The hospital performs (t, n) thresholds on servers from which the insurance company can obtain data on patient expenses by conducting homomorphic computations. Thereafter, the data of patients' expenses are entered in the blockchain ledger to be protected by the tamper-resistant property. Accordingly, the insurance company is incapable of learning anything about patient expenses because the honest nodes exceed the thresholds (n, t).

Parallel healthcare systems Diseases require cross-border medical experts from various backgrounds to collaborate using technology. The demand for accurate medical care, personalised diagnosis and treatment is increasing owing to regional and individual differences amongst patients. This development considerably increases the importance of patient data in terms of integrity, scalability and safety. Therefore, **Reference** [111] presented a framework for parallel healthcare systems (PHSs) to improve diagnostic accuracy and treatment efficiency based on the approach called artificial system, computational experiments and parallel execution (ACP). This framework is combined with the consortium blockchain by linking patients, healthcare providers (e.g. hospitals) and medical expert communities to comprehensive data sharing in PHSs regarding medical record reviews and care audibility. The cryptographic mechanism behind this blockchain may mitigate the security risk associated with the entry of patient data and checking of new data.

Multi-site clinical trials Currently, designing a secure, efficient and robust infrastructure should enforce the regulatory obligations in a multi-site clinical research study and ensure an elevated level of data security and cost optimisation. **Reference** [112] proposed a new decentralised data management framework based on permissioned blockchain to reduce the administrative burden, time and effort of ensuring data integrity and privacy in multi-site trials. This framework used smart contracts and managed private channels to maintain the confidentiality of data communication and protocol enforcement.

Telecare medical information systems Telecare medicine information system (TMIS) enables patients and physicians to

access medical services or data from remote sites. Therefore, the privacy of patients' data should be protected. **Reference** [113] used blockchain technology to develop a novel scheme for multi-level privacy preservation of location sharing in TMIS. Multi-level location sharing privacy was achieved by implementing an order-preserving symmetric encryption (OPE) that enabled comparison transactions to be applied directly to encrypted data without decryption. Merkle tree enabled users to confirm the location data received from peers in the P2P network, thereby ensuring that the data are undamaged or unchanged, such that shared locations can be verified efficiently and securely. The development in the location sharing system addressed the requirements of blockchain dependability according to decentralisation, confidentiality, multi-level privacy protection and verifiability.

Medical body sensor network Blockchain is the appropriate technology to address the issue of data physiological monopoly and improve the robustness of data storage. However, this technology has limited protection for private physiological data. **Reference** [114] introduced a key management scheme for body sensor networks (BSNs) in healthcare blockchain application. BSNs and health blockchain are combined to design a lightweight key management scheme for backup and the efficient recovery of health blockchain keys. This development scheme includes storage keys entered into the blockchain ledger to resist statistical attacks, whilst encryption keys are changed regularly. Blockchain generates many historical keys that are properly stored and indexed. Therefore, a healthcare system can easily find the appropriate keys if users want a block to be decrypted. This scheme has many advantages, such as biosensor keys in BSN being responsible for the generation, backup and recovery of blockchain health keys and enhancing the security of those keys. These advantages enable each block of the blockchain to be encrypted by a key with low storage costs and performance.

Other healthcare system applications Reference [115] designed an architecture based on blockchain technology to meet the requirements of an e-health system and address special needs to maintain storage of EHR and preserve patient's privacy. Blockchain integration with the infrastructure of an e-health management system has resulted in enhanced outcomes in personal data storage by providing secure access to information. **Reference** [116] provided a new decentralised architecture for an eHealth system based on blockchain. This decentralised architecture is an effective mechanism for the exchange of medical information, improvement of data integrity, reduction of transaction costs and avoidance of third-party services when participating amongst various health organisations. The current research presents the distribution of registered data to create electronic medical cards of patients by developing an algorithm using smart contracts.

Conducted studies

This section addresses the second part of the taxonomy (see Fig. 5). The studies comprised evaluation research on the adoption of blockchain in the healthcare system. Furthermore, the analytical studies (i.e. 6/58 scientific papers) covered the new model leveraging the blockchain-based healthcare system.

Evaluation studies Reference [117] aimed to develop and evaluate the use of blockchain-based mobile health system for cognitive insomnia treatment with a smartphone application. This application enables computational dependence on a decentralised network, which can be trusted and audited. Volunteer data were saved and forwarded to the Hyperledger Fabric network and all nodes were validated and updated successfully. The decentralised application ensured that EHRs registered with the blockchain network were resistant to manipulation. Reference [118] presented the implementation and evaluation in accordance with OmniPHR, which integrates with the distributed EHR using blockchain technology and open EHR interoperability standards. The aforementioned study evaluated the integration of the data of 40,000 adult patients. Medical documents from various databases have focused on non-functional performance, such as response time, CPU use, memory occupancy, disk use and anonymised network use. The prototype achieved 98% availability with an average response time of under 500 millisec in a scenario of 10 super peers and thousands of sessions competing simultaneously for health record operations. **Reference** [119] provided evaluation metrics for decentralised healthcare applications (DApps) on the basis of blockchain from a technical perspective in terms of feasibility and intended capacity. The aforementioned study provided a guideline for the development of successful DApps, which include complete workflow compliance with HIPAA, support for turning-completion, user identification and authentication support, support for minimum structural interoperability, scalability across healthcare participants and cost efficiency. **Reference** [120] proposed a new consensus mechanism model for the healthcare blockchain network called practical Byzantine fault tolerance (PBFT). The aforementioned study aimed to simulate the response times for PBFT with a continuous Markov chain (CTMC) model in terms of several factors, such as replica and primary node delays. Consequently, replica nodes have a minimum impact on the probability of implementation.

Analytical studies Reference [121] discussed the possible challenges and solutions to the adoption of biomedical/healthcare blockchain technology. Potential challenges can emerge in the adoption of blockchain technologies, such as openness/confidentiality, speed/scalability and the threat of

51% attacks that should be carefully addressed in the development and implementation of health applications. **Reference** [122] examined the interoperability of adopted blockchain in healthcare applications and how medical data sharing could be transformed amongst different hospital systems. The aforementioned study presented barriers to the interoperability of patients by facing five issues, namely, digital access regulations, data aggregation, data liquidity, patient identity and data stability.

Review and survey papers

This category includes reviews and survey papers to describe blockchain technology in healthcare applications. **Reference** [123] conducted a systematic literature review of state-of-the-art healthcare in blockchain research, revealed the potential applications of this technology and highlighted the challenges and possible research directions. **Reference** [124] reviewed the important uses of blockchain in health data management, pharmaceutical supply chain administration, drug adherence and billing/claims management and analytics. Healthcare organisations seek to develop blockchain technology to build fully decentralised applications, such as data provenance, counterfeit drug identification and consent management. **Reference** [125] reviewed the current and latest developments in the healthcare field by implementing blockchain as a model and discussing blockchain applications along with present challenges and future perspectives. **Reference** [126] investigated blockchain by reviewing recent state-of-the-art usage in healthcare applications in terms of promises, challenges and scenarios. The aforementioned study highlighted the properties of blockchains to achieve certain advantages for healthcare applications and identified challenges in terms of interoperability, security and privacy that should be addressed in the implementation of business models. **Reference** [36] investigated the literature on blockchain used in e-health and explored research trends. A total of 84 eHealth blockchain publications have been found, 18 of which were identified as relevant. Many of these publications have demonstrated the advantages and development of this technology in healthcare application. Only one survey paper was presented. **Reference** [127] indicated the unique requirements in certain health applications that are not addressed by blockchain technology. The adoption of blockchain in healthcare applications requires a high level of authentication, interoperability and record-sharing owing to legal requirements, such HIPAA. Specific vulnerabilities of blockchain technology and issues should also be addressed, such as mining incentives, attacks and key management.

Classification of research articles

This section classifies and discusses the final set of research articles on the bases of the following aspects: (1) year of publication, (2) author nationalities, (3) publishing house or journal, (4) purpose of using blockchain in healthcare applications and their contributions and (5) problem types and proposed solutions. Figure 6 shows the trend of article publications amongst the three databases (i.e. IEEE Xplore, ScienceDirect and WOS) from 2013 to 2019. The rate of publications shows annual increases. Therefore, blockchain technology in healthcare applications has gained increasing interest amongst researchers in recent years. The adoption of blockchain in healthcare applications significantly increased in 2018 and further studies are expected to be conducted.

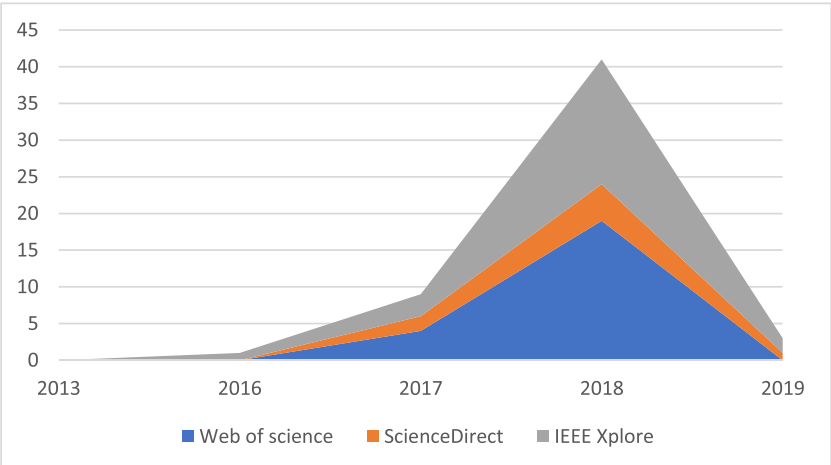

Fig. 6 Publication Trends amongst the Three Databases

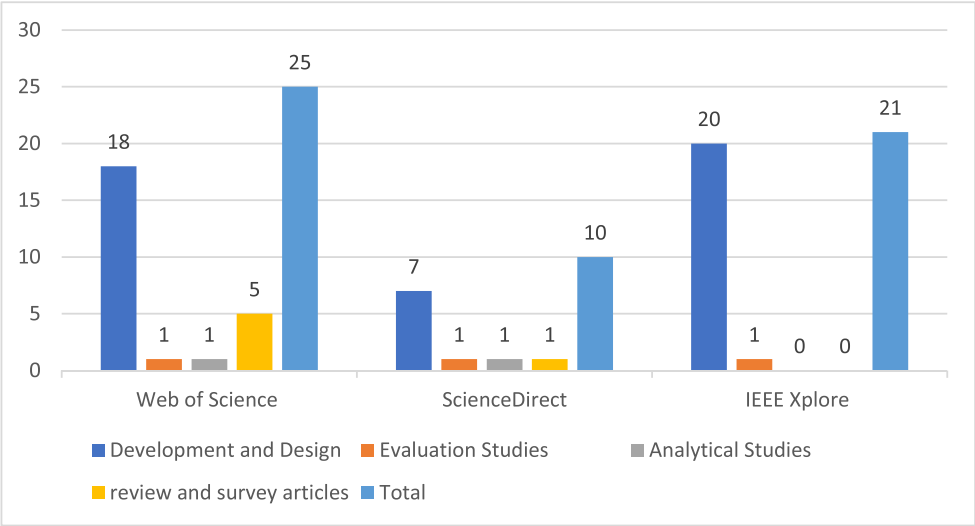

Figure 7 Statistical Articles in the Different Categories of Published Journals

Distribution by year of publication

Figure 7 illustrates the distribution of research articles in terms of digital databases and taxonomy categories. The systematic literature review consists of four primary categories, namely, development and design, evaluation studies, analytical studies and review and survey articles. WOS has published 25 articles in the following categories: development and design (18), evaluation studies (1), analytical studies (1) and review and survey articles (5). ScienceDirect has published 10 articles as follows: development and design (7), evaluation studies (1), analytical studies (1) and review and survey articles (1). Lastly, IEEE Xplore has published 21 articles as follows: development and design (20) and evaluation studies (1). However, analytical studies and review and survey articles were not published in IEEE Xplore.

Figure 8 illustrates the number of relevant articles for each year of publication within the four categories. A total of 58 articles have been published in the distribution of scientific articles related to the adoption of blockchain for healthcare applications between 2016 and 2019. The scientific articles are distributed as follows: 1 was published in 2016, 8 in 2017, 41 in 2018 and 8 in 2019.

Distribution by author nationality

Figure 9 illustrates the implementation of healthcare applications by the utilisation of blockchain in 23 countries and likewise provides the authors' nationalities. We observed that the relevant studies were conducted in countries where attempts were made to adopt a blockchain to cover cases in healthcare organisations, such as EHR. The nationality

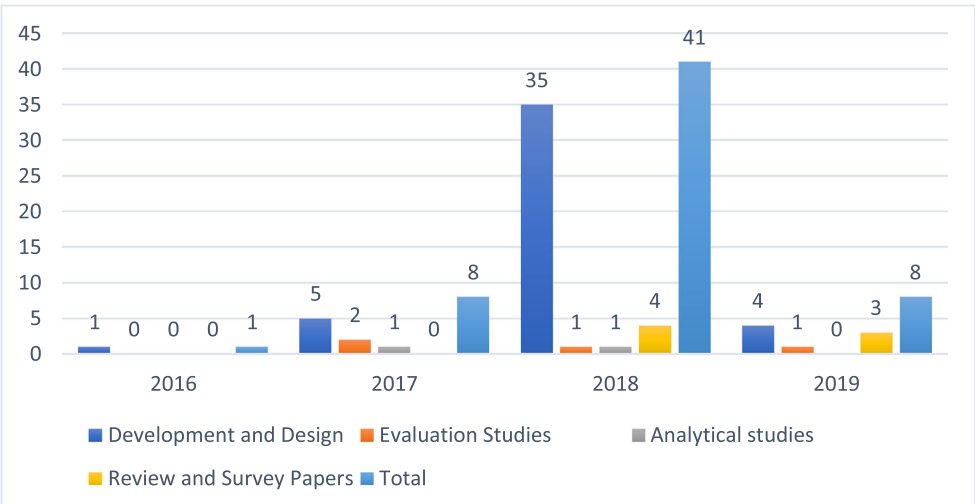

Fig. 8 Statistical Articles in the Different Categories by Year of Publication

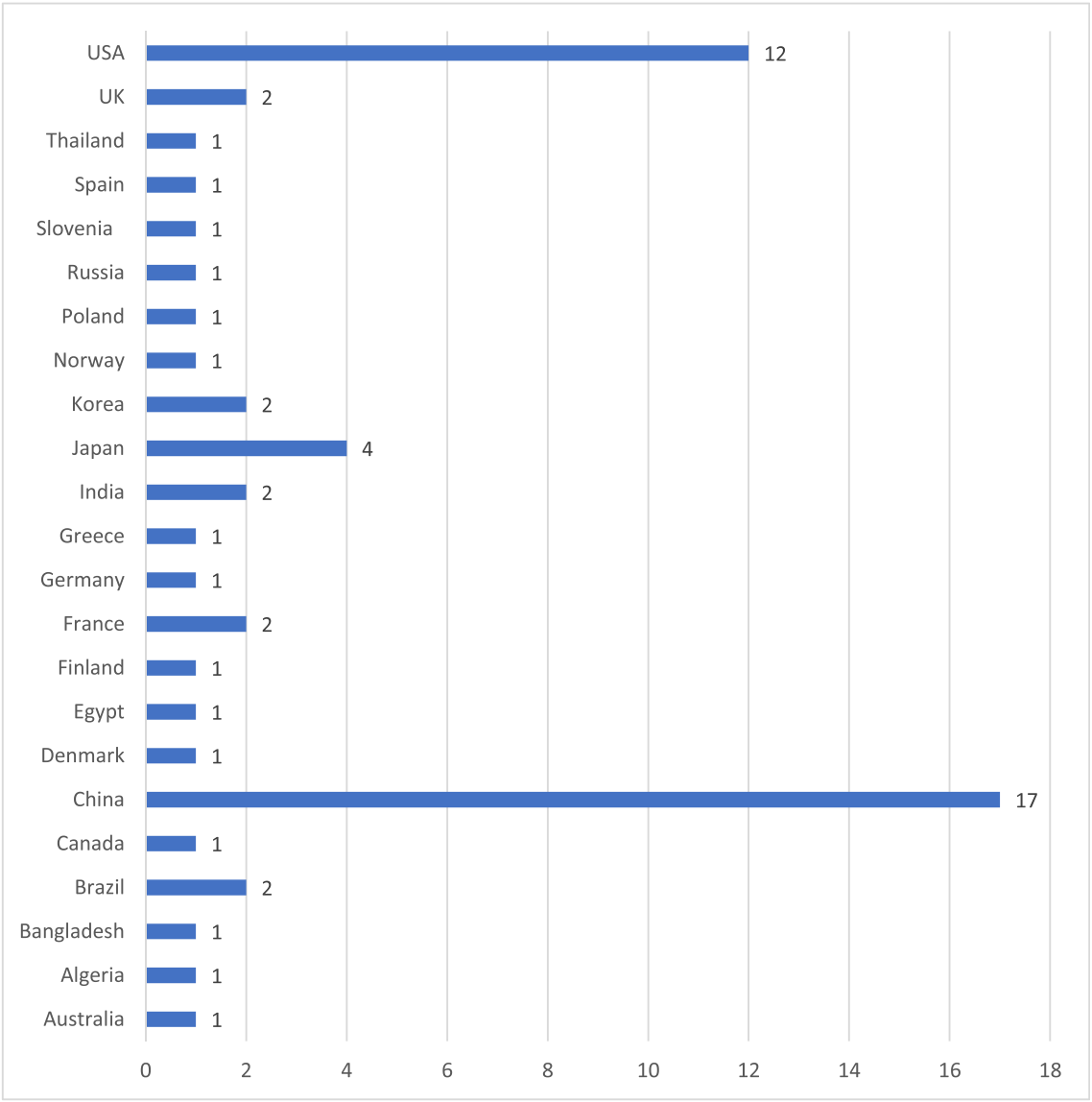

Fig. 9 Distribution by Author Nationality

distribution of the 58 articles in blockchain-based healthcare applications shows that the most productive authors are from the following countries: China (17); the US (12); Japan (4); France, Brazil, India, South Korea and the UK (2 each) and Algeria, Bangladesh, Canada, Denmark, Egypt, Finland, Germany, Greece, Norway, Poland, Russia, Slovenia, Spain and Thailand (1 each).

Distribution by publishing house or journal

Table 3 shows that the research articles have been categorised by publishers' journals and scientific conferences. This new categorisation paradigm is used in the systematic review of the literature to assist researchers target the journals relevant to the subject of a particular study.

Distribution by Use of Blockchain in Healthcare Applications

The systematic review shows that blockchain technology has been used to address several issues, such as security, data privacy, authentication, interoperability, inaccessibility and stored patient or provider data, in various fields of the healthcare application sector (see Fig. 10).

Table 4 reveals the distribution of each research article on the basis of author contributions. Out of the 44 publications, a new architecture occurred 7 times (15%) by employing blockchain technology in healthcare applications. Thus, new system designs were contributed by the authors in several cases of healthcare use (14 times (32%)). Moreover, the authors introduced a framework empowered by blockchain in different healthcare fields

Table 3 Categorisation of Articles by Journals, Publishers and Scientific Conferences

NO.	Name of Journals and CONFERENCES	References
1	Telehealth and Medicine Today (TMT)	[40]
2	Journal of Medical Systems (Springer)	[97, 98]. [36, 74, 84, 85, 90, 92, 103, 106, 110, 113]
3	Sensors (Switzerland)	[107]
4	Health Informatics Journal	[94]
5	JMIR mHealth and uHealth	[117]
6	Journal of the American Medical Informatics Association	[121]
7	Symmetry—MDPI	[123]
8	Cryptography—MDPI	[125]
9	IEEE Access	[79, 88, 105]
10	IEEE Transactions on Computational Social Systems	[111]
11	CAAI Transactions on Intelligence Technology	[114]
12	Computational and Structural Biotechnology Journal	[100, 108, 122]
13	Sustainable Cities and Society	[82]
14	Future Generation Computer Systems	[102, 125]
15	Procedia Computer Science Elsevier	[87]
16	Journal of Biomedical Informatics	[95, 118]
17	Journal of Network and Computer Applications	[127]
18	ArXiv	[86, 91, 112, 124]
19	International Journal of Health Geographic's	[126]
20	ICT Infrastructures and Services	[76]
21	Norwegian Information Security	[81]
22	Information Technology in Medicine and Education (ITME) IEEE	[99, 120]
23	E-health Networking, Application & Services IEEE	[115, 119]
24	Advanced Informatics: Concept Theory and Applications (ICAICTA) IEEE	[96]
25	IEEE Globecom Workshops	[77, 109]
26	Smart Trends in Systems, Security and Sustainability (WorldS4) IEEE	[101]
27	Computer Communication and Networks (ICCCN) IEEE.	[78]
28	Digital System Design (DSD) IEEE	[75]
29	Trust, Security and Privacy in Computing and Communications IEEE	[89]
30	Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) IEEE	[93]
31	Telecommunications Forum (TELFOR) IEEE	[83]
32	Smart Computing (SMARTCOMP) IEEE	[104]
33	Global Communications IEEE	[80]

(10 times (23%)). Proposed new schemes contributed to the combination of healthcare applications with blockchain accounted for 6 publications (13%). The remaining 8 publications (18%) presented a new platform, algorithm, approach, protocol and model.

The next analysis was performed through our systematic review for the purpose of using blockchain in the healthcare domain. Table 5 shows that the majority of the publications used blockchain to improve data security, data privacy and patient data management in EHR. Authors often stated multiple applications of blockchain technology in healthcare (e.g. data sharing and access control), which could be viewed as expected methods because blockchain technology entails specific applications. For example, distributed technology, such as blockchain, should be suitable for data sharing. Therefore, this area of research will often be discussed.

Distribution by type of problems and proposed solutions for each study

Many researchers have identified problems related to the integration of blockchain with healthcare applications and proposed appropriate solutions to solve these problems. This section provides insights into the problems that researchers have

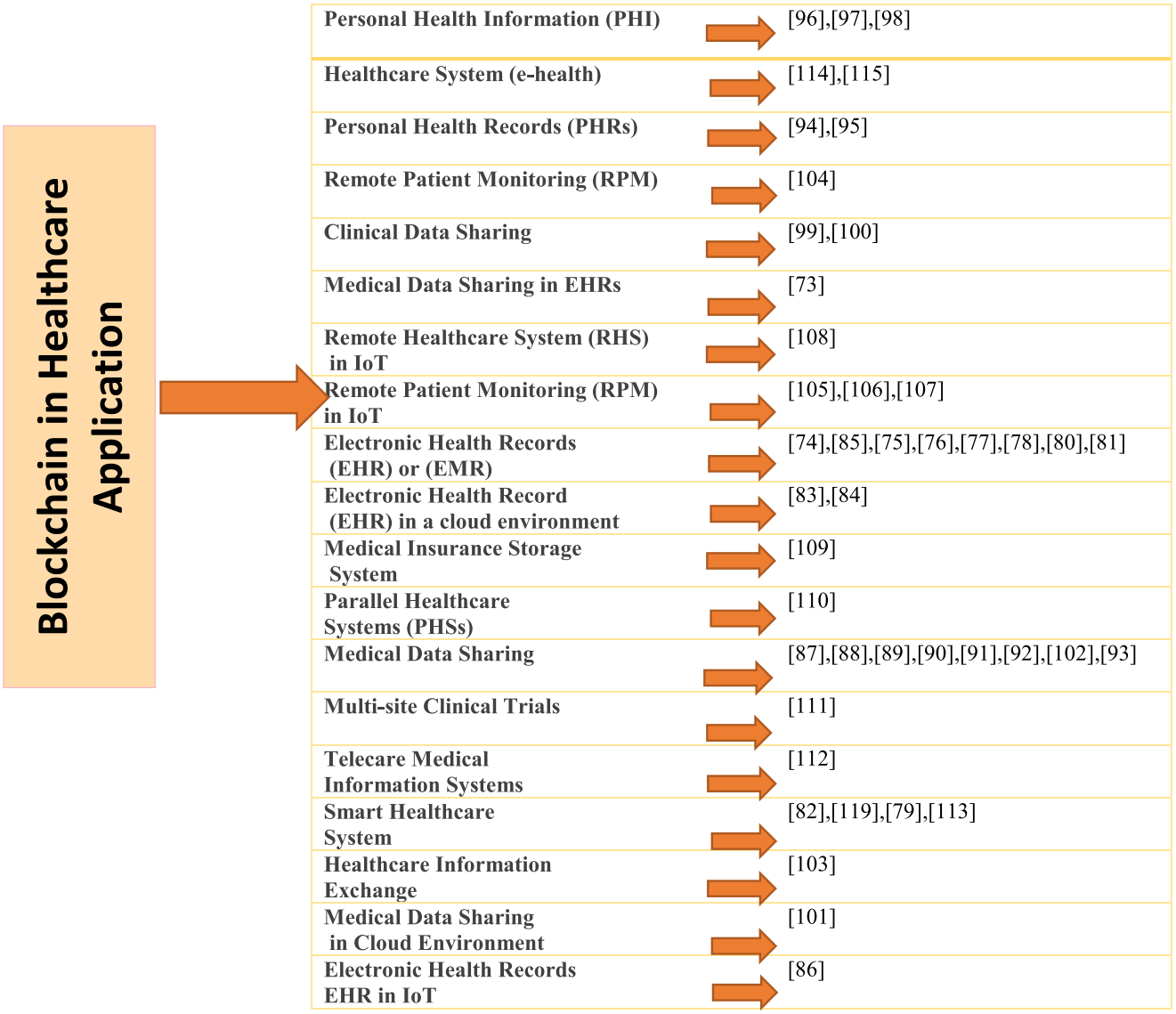

Fig. 10 Use of Blockchain in Healthcare Applications

encountered and their proposed solutions that involve the use of blockchain.

Table 4 Contributions Presented in the Research Articles

No.	Contributions	References
1	Architecture	[95, 97, 100, 101, 105, 115, 116]
2	System designs	[88–92], [74–76, 84, 86, 106, 109, 110]
3	Framework	[77, 82, 83, 93, 94, 99, 103, 107, 111, 112]
4	Scheme	[78–80], [98, 113, 114]
5	Model	[120]
6	Platform	[85, 102, 104]
7	Approach	[81]
8	Protocol	[87]
9	Algorithm	[104, 116]

Technical problems in previous studies

Six types of technical problems have been determined in previous studies (see Fig. 11).

The first type of technical problem discussed in several studies involves the security of medical data stored in EHR for patients or healthcare providers. Studies [76, 84, 85, 115] and [116] aimed to resolve the restriction of the existing EHR storage system dependent on trusted third parties (e.g. cloud servers) by replacing the infrastructure system in a decentralised manner, thereby ensuring that the EHR storage systems are resistant to security attacks and hacking of patient data. Studies [74, 93, 103, 104, 112] and [111] attempted to solve the problem of HIE in EHRs because the repository of medical data is a single point of failure and can be targeted by attackers, such as ransomware attacks or denial of services. Study [110] attempted to solve

Table 5 Purpose of Blockchain Use in Healthcare Applications

No.	Improvement of Healthcare Applications	References
1	Improved data security	[74, 76, 77, 80–84, 100, 103, 109, 110, 114–117]
2	Improved data privacy	[78, 79, 82, 86, 87, 90, 96–99, 102, 107, 113, 114]
3	Improved data integrity	[89, 92]
4	Improved authentication	[75, 108]
5	Improved interoperability	[122]
6	Improved real-time update and access	[95, 111]
7	Improved data sharing	[88]
8	Improved drug traceability	[85]
9	Improved patient data management	[93, 104–106]

the problem related to the medical data management system for the storage of personal data, in which providers must be trustworthy in handling patient data from resistance to manipulation and that each transaction should be verifiable. Study [77] attempted to resolve the complexity of current schemes that manage the security of EHRs to provide an effective balance between data protection and the need for patients and providers to regularly interact through data.

The last studies under this type of problem are associated with designing RPM systems on the basis of IoT to aggregate large data streams, whilst ensuring patient confidentiality [105]. These safety and privacy problems with medical data could result from delays in treatment and even endanger the life of patients [107, 108]. Therefore, IoT-RPM has raised many privacy and security issues because of the failure of the IoT server architecture to disrupt the entire network and the vulnerability of devices to DDoS attack, data theft, hacking and remote hijacking without exception [109].

The second type of technical problems concerns the protection of the privacy of medical data for patient and

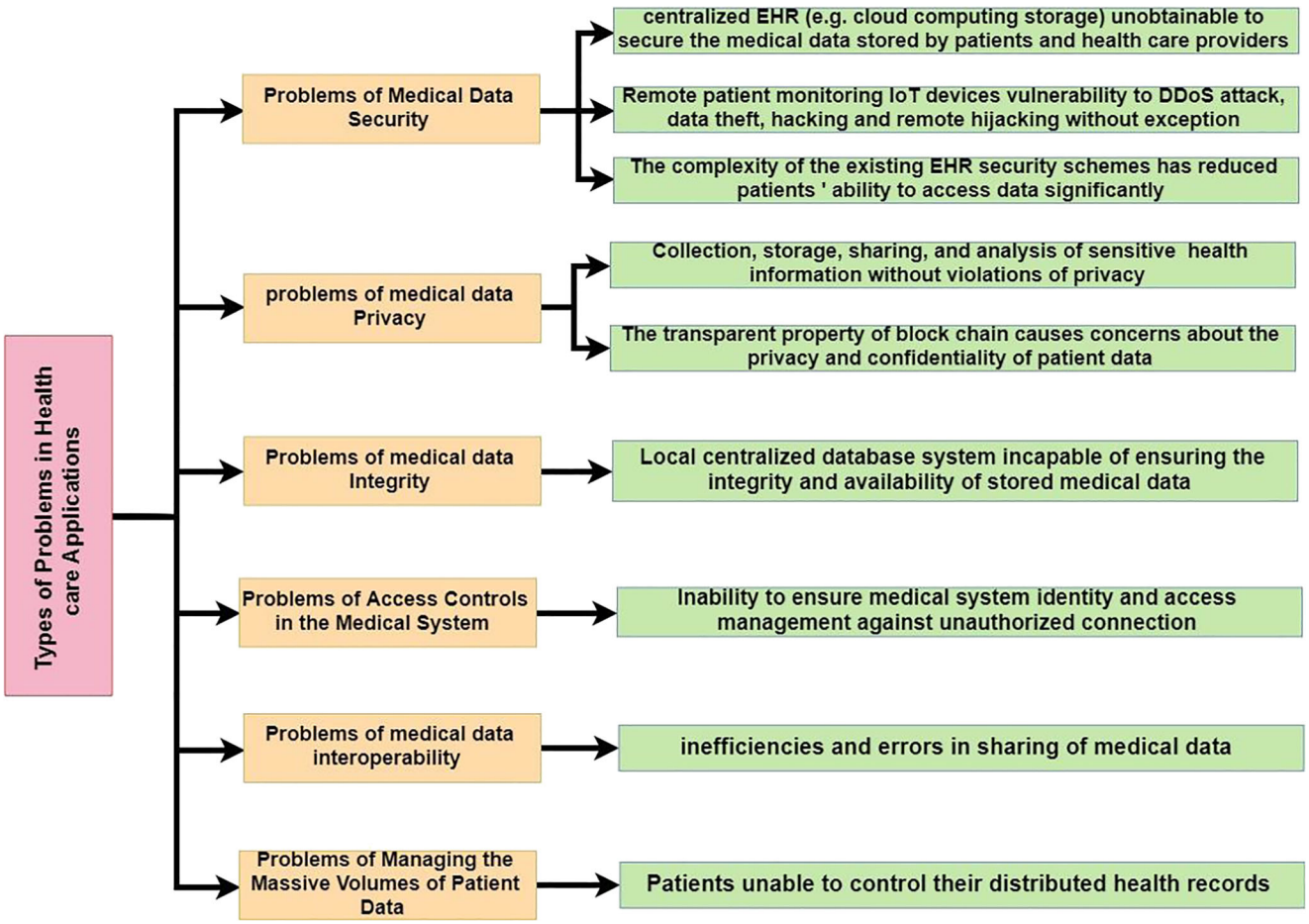

Fig. 11 Classification of Technical Problems in Healthcare Applications

healthcare providers in EHR. Studies [80, 81, 86, 87, 90, 102] and [98] focused on preserving the privacy of the EHR medical data in collecting, storing, sharing and analysing sensitive health information. Study [102] aimed to address the issue of privacy violations of stored cloud medical data against cyber-attacks, such as lack of accountability and pseudonymity. Studies [78, 79, 82, 96, 113] and [114] attempted to resolve the transparency property of the blockchain in the integration with EHRs to prevent privacy and confidentiality concerns for PHRs.

The third type of technical problems is related to guaranteeing data integrity and the availability of stored medical data. Studies [89, 92] attempted to solve the problem of integrity and availability of medical data storage in a centralised local database. The two methods to achieve integrity in the existing system involve formulating an access control strategy and encrypting medical data with the patient's key. The problem with the first method is the possibility of modifying or deleting data in the local database. The problem with the second method is the impossibility of sharing the key if the patient dies during diagnosis or treatment. Thus, data availability is affected by two problems.

The fourth type of technical problems relates to accessing controls in the medical system. Study [75] attempted to resolve the problem of unauthorised connections in EHR against security attacks when a patients' data are exchanged from one provider to another. Study [106] attempted to solve the node authorisation problem within the IoT-RPM device for patient treatment and by identifying the network connection to prevent hacker targets.

The fifth type of technical problems relates to medical data interoperability. The inefficiencies and errors in exchange, collection and analysis of medical data lead to a lack of interoperability in healthcare [94, 100]. Study [83] attempted to solve the problem of patient access to the EHR database because patients are unable to easily share data with providers or researchers. The challenge of interoperability amongst various providers involves the high-performance data sharing requirement resulting in the fragmentation of record data instead of cohesiveness. The dissemination of patient medical records risks patient confidentiality because malicious activities could seriously damage reputation and finances [88].

The sixth type of technical problems relates to issues of managing massive volumes of patient data in the healthcare application. Medical data are extensive and cumbersome and could result in the quality issues of medical data, such as complicated analysis, diagnosis and prediction, as well as the confidentiality of data because of the continuously increasing number of cybercrimes [97, 101]. Study [95] attempted to solve the problem associated with PHRs in EHR in terms of the ability of patients to view their distributed health records and healthcare providers to access up-to-date patient data and resolve duplicate health records in healthcare organisations.

Proposed solutions in previous studies

This section highlights the proposed solutions in previous studies depending on various technical problems. The currently relevant set of healthcare system security goals may include a variety of issues that should be addressed, such as confidentiality, integrity, availability, privacy, authenticity and trustworthiness, non-repudiation, accountability and auditability goals. Previous studies have attempted to address all these security requirements, whereas others have focused on one issue in addressing the security requirements of the medical data system. Hence, the solutions of previous studies are categorised on the bases of the contributions made to achieving safety goals (see Figs. 12 and 13).

Proposed solutions for medical data security problems

Previous studies have proposed several solutions to enhance the security value of existing medical systems by situating blockchain layers above legacy systems in conjunction with cryptographic techniques (see Fig. 12). Studies [76, 115, 116] and [85] transformed the centralised feature of network communication of EHRs amongst healthcare providers into a decentralised network by using the internal characteristics of blockchain, thereby bringing many benefits and resolving security issues. The decentralised EHR network has resulted in the elimination of third-party dependence, thereby improving the health infrastructure management system, management of personal data storage and provision of professional access to data, whilst guaranteeing security and privacy. Study [84] designed a new cryptosystem based on the attributes of existing cryptosystems (e.g. IBE, ABE) and blockchain to ensure confidentiality, authentication, integrity of medical information and support of fine-grained access control of the medical data stored on the cloud server. Studies [74, 93, 103, 104] and [112] maximised the consent feature in blockchain, in which the consensus algorithm controls the access, storage and distribution of medical data within an EHR network. The EHR system controls any decision, which is required to be agreed upon by all network participants. Hence, a new level of trust was added to the network prior to allowing data to be changed. This feature provided an additional layer of assurance in the medical data repository network that is less of a single point of failure and can prevent attacks, such as ransomware and denial of services from targeting them. Study [77] improved the security features and reduced the complexity of the current EHR system by introducing a cipher manager with the blockchain that incorporated encryption techniques before network records are sent and received. Every patient has a unique ID address and identifier in the blockchain network, thereby minimising the unauthorised use of records and achieving high-level data security. Study [111] solved security and scalability issues in the current HIE system by introducing a new combined ACP with consortium blockchain to improve

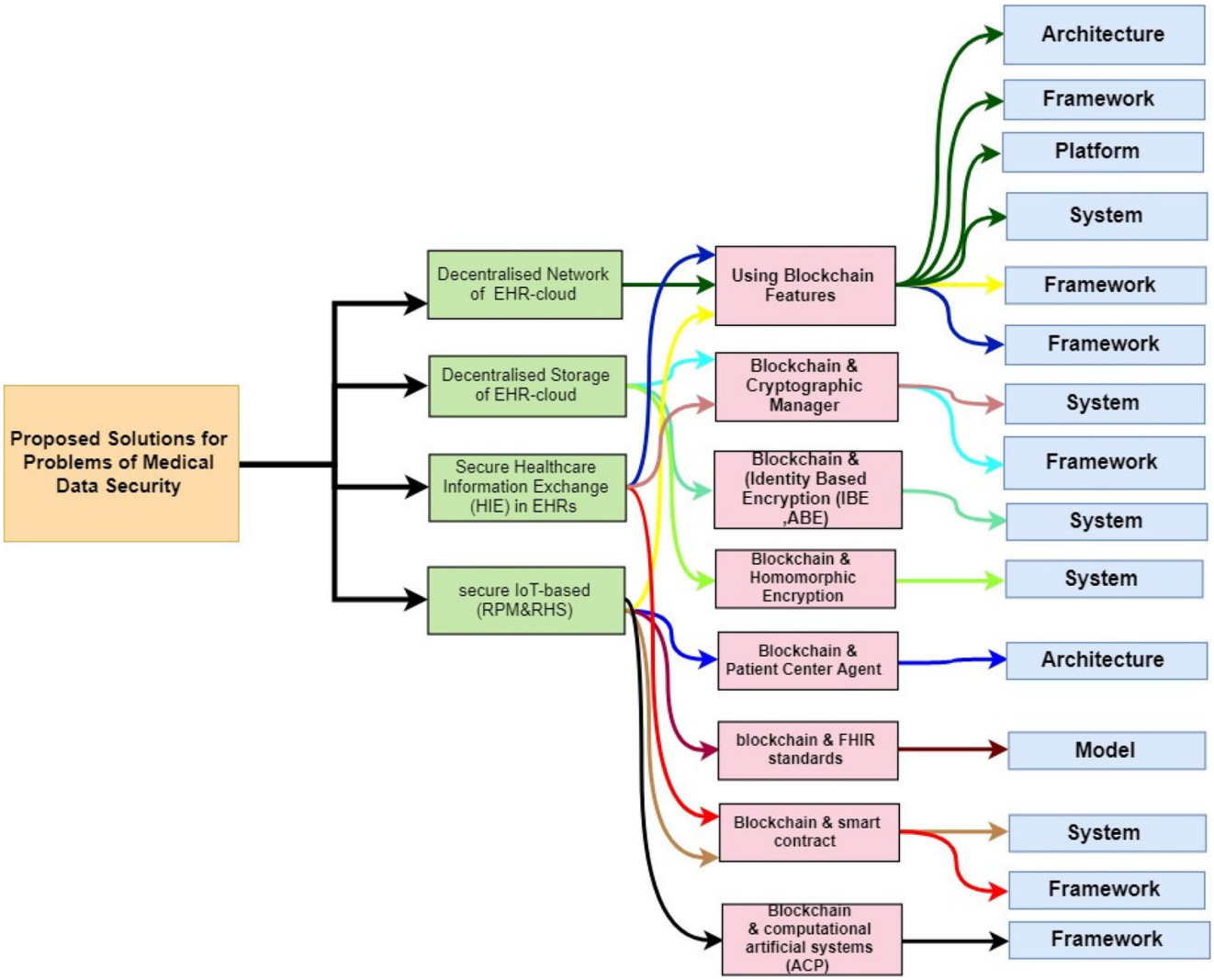

Fig. 12 Classification of the Proposed Solutions for Medical Data Security Problems

diagnostic accuracy and treatment effectiveness. Study [110] improved the security of insurance management systems by using blockchain and homomorphic encryption systems to achieve a secure, decentralised storage of patient data.

Study [105] proposed an end-to-end architecture combined PCA with blockchain to resolve the security issues of IoT-RPMS in collecting large amounts of data streams whilst guaranteeing patient confidentiality. Study [107] addressed privacy and security issues related to data transfer and transactions logging across IoT-RPMN. The modified model for IoT devices considers the advantageous feature of distribution in blockchain and other network privacy and security properties to ensure secure communication and analysis of big data in RPM. Study [108] adopted the security requirement in the FHIR standards and proposed the FHIR chain model for IoT-RPM in conjunction with blockchain distribution features to enhance patients' security and privacy with a collaborative clinical decision. Study [109] benefitted from smart contract implementation in the blockchain network by removing third parties and other features of self-executing, immutable, self-verifying and auto-enforcing to manage device-generated information in IoT-RHS. These components communicate and synchronise over a distributed network of IoT devices owned and managed by multiple entities to avoid certain types of security attacks, such as DDoS, data theft, hacking and remote hijacking.

Proposed solutions for medical data privacy problems

Extensive effort has been exerted towards improving the privacy of medical data for patients and healthcare providers by establishing a cryptographic mechanism in the decentralised EHR network or other healthcare applications (see Fig. 13). Study [80] attempted to develop an efficient mechanism based on ECC above the existing blockchain-based EHR system to achieve the privacy preservation of data accessibility in the network. Study [102] addressed a privacy-preserving platform by establishing an ECC mechanism to encrypt the back and forth exchange of medical data stored in the cloud to prevent

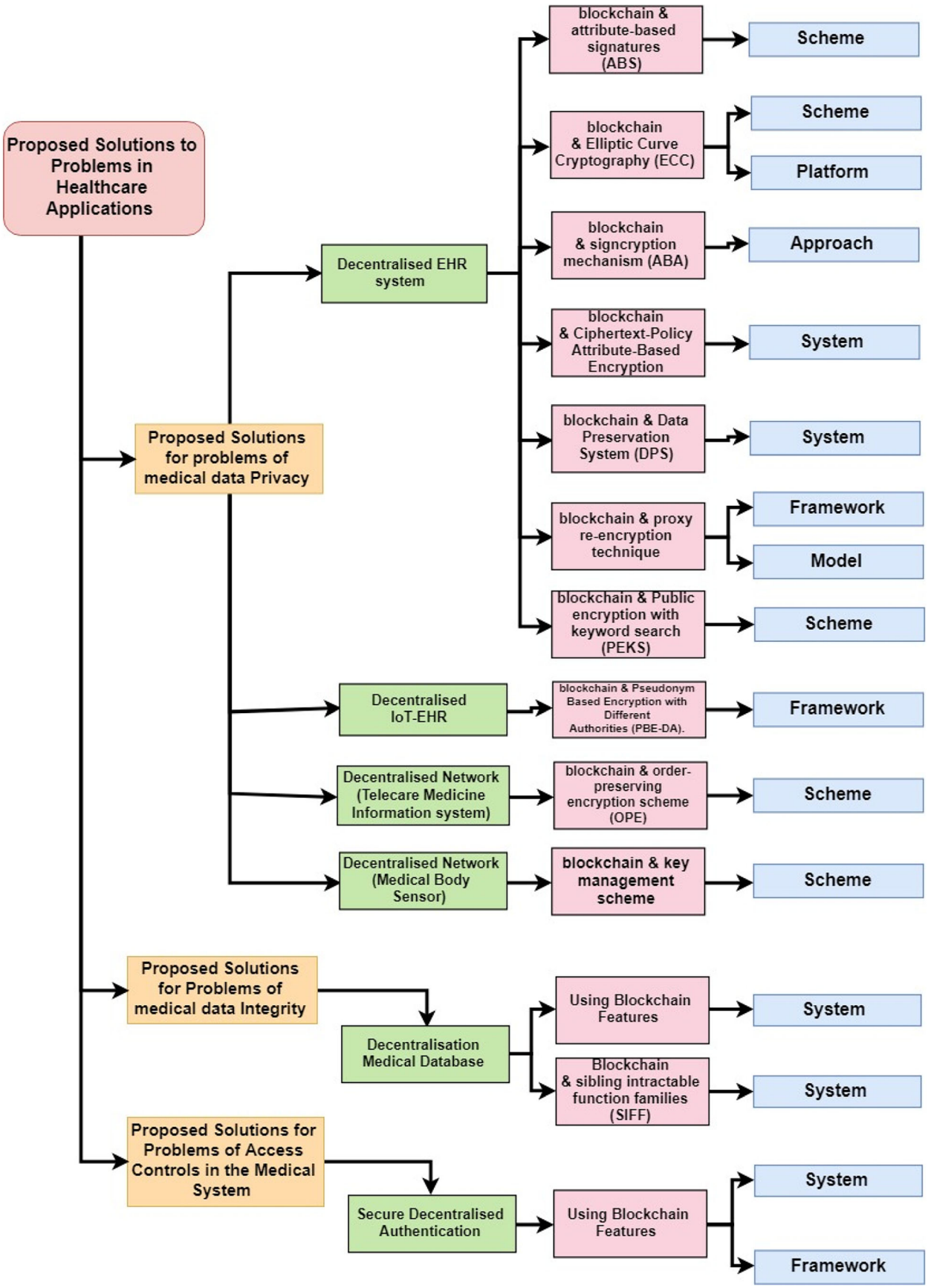

Fig. 13 Classification of the Proposed Solutions for Privacy, Integrity and Access Control Problems

DDoS cyber-attacks caused by pseudonymity in the blockchain network. Study [81] adopted a signcryption mechanism (i.e. ABA) to protect the sharing of medical data privacy in decentralised EHRs, thereby resulting in improved quality and reduced medical treatment costs. Study [86] provided data-sharing privacy protection in an EHR-cloud system based on consortium blockchain and ciphertext-policy attribute-based encryption (CP-ABE). CP-ABE provides strong privacy preservation in data sharing and permits data owners to exchange encryption data with authorised users in the cloud storage whilst maintaining access control mechanism to be blinded. Study [87] resolved the problems associated with protecting patient privacy by using PBE-DA in the multilayer protocol of an IoT-EHR system based on blockchain. Study [98] developed a scheme based on blockchain characteristics and the use of public keyword search encryption (PEKS) to secure and preserve the privacy of keyword search protocol for EHR by building a bilinear keyword polynomial map that provides proof of conformity for the blockchain, which functions as a consensus mechanism. Study [90] solved the problem of storing patients' medical records in the database by ensuring that the stored data are tamper-proof by leveraging the characteristics of the Ethereum blockchain. Data preservation system (DPS) is an accessible and distributed P2P network database and proof of primitivity as a consensus algorithm to perpetually preserve data in the blockchain.

Patients' access to EHRs through the blockchain database is extremely limited and patients are unable to easily share such data with providers or researchers. Study [79] addressed these limitations by proposing a scheme based on ABS with various authorities in decentralised blockchain-based EHRs to maintain patient privacy and improve interoperability. Study [78] enabled dual privacy preservation capabilities in decentralised EHRs amongst different healthcare providers (e.g. hospitals) by using ABS for blockchain healthcare applications, which preserve the privacy of signer identity authentication. Internal blockchain characteristics have provided many benefits to EHRs, but the transparent features could relatively lead to privacy and confidentiality leakage of PHRs. Studies [82, 96] solved these problems by modelling the proxy re-encryption technique above the blockchain application. This technique divides the re-encryption between multiple nodes. Subsequently, the symmetric keys in the EHR system are separated and functional internally within the node. That is, private transactions preserve the data integrity offered by the blockchain whilst increasing privacy. The healthcare application based on the blockchain records transactions are open to the public in the network and may be leaked. Study [113] provided a multi-level confidentiality sharing of patient locations in the TMIS based on the OPE to guarantee the confidentiality of locations recorded in the blockchain. Study [114] combined the key management scheme and blockchain to leverage privacy protection in the healthcare system, which contains sensitive information.

Proposed solutions for medical data integrity problems To solve the problem of integrity and the availability of stored medical data in a centralised local database, Study [89] presented a system that allows data sharing and medical data management to be transformed into a decentralisation medical database. This system ensures security, privacy and integrity by leveraging the unique properties in the blockchain. Additionally, this development system employs the secure digital blockchain ledger to ensure the integrity of the stored medical data by making a hashed copy of the data. Thereafter, copies can be given to entities wanting to access data (e.g. medical research centres) to verify the integrity of the data whilst preventing the threat model of the malicious database administrator. Therefore, the procedure is performed automatically through smart contracts when the entities request access to patient medical data. Study [92] used blockchain in combination with SIFF to achieve integrity, availability and privacy in medical data management by storing medical data in a decentralisation medical database, establishing an access control technique and encrypting patient data with a symmetric key. The integrity characteristic in medical data was determined by honest participants, in which data can be recorded in a Hyperledger Fabric blockchain, thereby resulting in the impossibility of altering or deleting data by any adversary.

Proposed solutions for access control problems in the medical system Study [75] solved the problem of centralised authentication by setting up a secure decentralised authentication provider to prevent system threats to certain security attacks when patient data are accessed from one provider to another. The proposed system addressed the issues of authentication and authorisation of exchange of sensitive data amongst multiple healthcare providers in existing EHR medical systems. Of interest is that blockchain can be used as an authentication provider. Study [106] proposed a blockchain-based solution that enables IoT-RPM to be authenticated and securely communicated to stored devices generated by health information systems. The use of blockchain technology can grant user authentication and authorisation to protect against such threats, in which anyone cannot physically steal information.

Proposed solutions for medical data interoperability problems Study [83] combined AI with the EHR blockchain to improve the confidentiality and security of and interaction with medical data. The proposed system solved the problems faced by the medical system in interoperability and sharing medical data amongst different healthcare providers. The use of blockchain transactions ensures coordination between different EHR stakeholders without fragmentation of data. Study [88] used blockchain features to solve the problem of

compromised patient confidentiality in the interoperability of medical data sharing amongst medical big data providers in an untrustworthy cloud service environment. The utilisation of blockchain ensures the efficient sharing of medical data and zero errors because the consensus algorithm controls the distribution and synchronisation of data between different EHR providers. Study [100] addressed the issue of collaborative clinical decision-making to be substantially secure and scalable in data sharing by using the FHIR HL7 standard and blockchain. This combination effectively improved the exchange of information and made effective treatment decisions. Study [94] focused on the axis of exchange of medical imaging data in EHR by proposing a framework for cross-domain image sharing that uses a blockchain as a distributed data storage to establish a list of radiological studies and patient-defined access permissions.

Proposed solutions for problems related to managing massive volumes of patient data Study [97] used a new blockchain-based architecture called healthcare data gateway (HDG) to easily and securely control and share patient data without violating privacy. The development of the architecture solves the problem associated with healthcare systems in terms of collecting, storing and analysing personal healthcare data without raising privacy violations and ensuring that data are owned and controlled by the patient instead of being scattered across different healthcare providers. Study [95] presented an OmniPHR blockchain-based architecture to integrate PHR between patients and healthcare providers to solve problems related to patients' distributed data records in managing and accessing up-to-date and recording duplicate data. Study [101] proposed a new architecture of a blockchain-based decentralised health data ecosystem that can be integrated with large volumes of clinical data whilst protecting confidentiality. The architecture developed deals with vast medical data to ensure the quality of medical data in terms of complicated analysis, diagnosis and prediction.

Discussion

This systematic literature review presents the most relevant studies on state-of-the-art healthcare applications using blockchain technology to highlight research trends. This review differs from previous reviews because it is current and focuses on the use of healthcare applications in the blockchain rather than as individual applications. Various articles deal with the subject under an introductory perspective, examine existing applications and develop actual decentralised healthcare application based on the blockchain. Figure 5 illustrates the taxonomy of the literature, which enables sorting various studies into meaningful, manageable and coherent designs. The structure introduced by the taxonomy is intended to provide researchers with a wide range of important insights into the topic. For example, the taxonomy of healthcare applications based on blockchain in the current research shows that researchers are inclined to develop, design and operate applications. Thus, a possible path in this area is based on the contribution of each paper, such as new architecture, system designs, framework, scheme, model, platform, approach, protocol and algorithm.

Another possible area includes the combination of IoT applications with blockchain and their use in healthcare systems, such as RHS, RPM and EHR. The possibility of using blockchain in a medical database aims to obtain a secure and scalable decentralised storage of EHR in a cloud environment. Another possible perspective is to maximise the combination of blockchain with artificial intelligence in the healthcare system. Blockchain aims to resolve the major problems of traditional healthcare systems, such as security, privacy, authentication, interoperability, inaccessibility and storage of patient or provider data. The taxonomy reveals gaps and highlights the lack of studies on the development of healthcare applications in blockchain technology. Three aspects of the literature content are identified on the basis of the review: (1) motivations behind the development of healthcare system in blockchain technologies, (2) challenges for the successful utilisation of these technologies and (3) recommendations to address these difficulties.

Motivations

The motivations behind the use of blockchain technology in healthcare applications were extracted from the review of

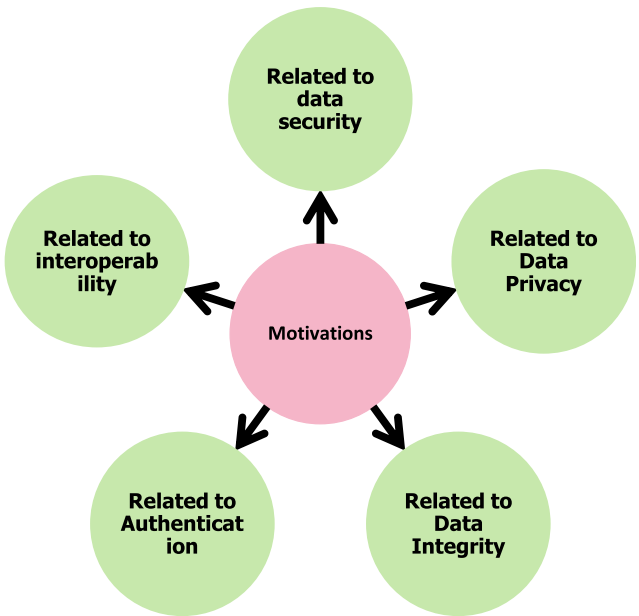

Figure 14 Motivation Categories for the Use of Blockchain in Healthcare Applications

studies. We have grouped these motivations into several categories (see Fig. 14).

Motivations related to data security

The volume of digital data in healthcare is increasing and innovative methods of processing and storing data are required. The immediate task is to ensure the safety of the transmission and storage of medical data. Blockchain technology has been utilised to demonstrate the effectiveness of safe storage and data transfer in the healthcare system. Numerous studies have been conducted to improve healthcare application security through the use of blockchain. As an EHR, blockchain technology stores patient data with significantly increased security [76, 77, 103]. The different interactions of patients in a blockchain healthcare system have multiple checkpoints rather than a single gateway, thereby improving the safety of sensitive data [114]. The manner by which patients monitor their health information could have an impact. Patients who are part of the blockchain could approve or deny any sharing or modification of their data, thereby ensuring high-level protection and enhanced control [84, 96, 109]. Although this situation is similar to how HIEs can operate, several EHRs will participate in a decentralisation architecture [74, 81]. The validation aspect of distinguishing blockchains from other traditional systems involves secure and scalable clinical data sharing [100]. HIE must be trustworthy for patients and healthcare providers when records move between hospitals and other organisations. Blockchain participants will also know that the data have been validated [104] and patients will not spend time collecting own data from multiple healthcare providers to send to a new clinic. The new medical providers can be simply added to the node of the blockchain network. Then, medical providers can access the same data of patients who already participated in the blockchain healthcare system through secure and efficient data accessibility [80, 92, 117].

Motivations related to data privacy

The protection of sensitive data against unauthorised access is highly important. Therefore, a major problem with healthcare application is that data privacy has been affected by leakage of sensitive information. Over the past years, effort has been exerted to ensure privacy in healthcare. These approaches have focused on different data privacy solutions. Blockchain has received considerable attention as a promising technology to protect the privacy of personal data owing to a decentralised distributed ledger. That is, the transactions content patterns are only accessible to specific users in the blockchain network and their real identity remains anonymous to the public. Transaction privacy is essential in various healthcare applications based on blockchain (e.g. EHR as anonymous authorisation and authentication), where patients may want enhanced privacy and prevent the release of their personal information to any curious blockchain entity. Numerous studies have attempted to adopt blockchain technology to protect the privacy of medical data, such as privacy-preserving of PHR [97, 99] and individuals may benefit from personal health data for enhanced treatment. The use of blockchain technology could protect the privacy of data sharing in EHR [86, 98]. The privacy of blockchain-based EHR data sharing could be improved by using the ABS scheme [78, 79]. Privacy preservation of blockchain-based EHR could address access the issues of control and interoperability of medical data [82]. Accordingly, a new DPS has been proposed to protect the privacy of a medical data system [90]. Moreover, the decentralised characteristic of blockchain is essential for the privacy-preserving process of devices in IoT-healthcare [107]. The achievement of a perfect privacy preservation for patients can be based on PBE-DA [87]. The use of blockchain would benefit the protection of healthcare data privacy in a cloud environment [102]. Blockchain has also been applied to protect telecare medical information system sharing location [113].

Motivations related to data integrity

Data integrity is important because patients can be identified and tracked from one level of care to another. Data trustworthiness means that healthcare data should be complete, accurate, consistent and up-to-date because providers use data in decisions related to patient care [116]. In a medical insurance storage system, blockchain properties (e.g. tamper-proof) can offer high credibility to users, hospitals, patients, insurance and servers. The majority of the verification processes occur with the use of record nodes in the blockchain, thereby requiring only a few CPUs and memory usage for healthcare providers (e.g. hospital), insurance providers and servers [110].

Motivations related to authentication

Authentication is a crucial component of a medical system and blockchain technology can prevent unauthorised access to such a system by using data integrity, non-repudiation and authentication [75]. Identity access management (IAM) strategies can address unauthorised access issues by formalising software access and relevance whilst responding to the daily needs of users. The integration of blockchain with IAM in EHR is a genuine strategy to ensure the confidentiality of healthcare data through access rights and a password policy that provide users with secure access to medical data [108].

Motivations related to interoperability

Interoperability in healthcare has historically focused on the exchange of data between entities within entirely different hospital systems. The major challenges in healthcare interoperability are healthcare organisations' different levels of maturity in information quality, governance mechanisms and standardisation. Several healthcare organisations tend to use different standards of medical data exchange, such as FHIR, CDA and HL7 2.x to share medical data with multiple healthcare providers. The varying data standards directly reduce the interoperability of healthcare organisations. Blockchain assists in overcoming this challenge by accessing data via APIs to standardise data formats to facilitate data transmission seamlessly in EHR communication. Additionally, blockchain addresses current challenges in the synchronisation of patient information with multiple healthcare providers whilst guaranteeing the privacy and security data of patients via a distributed identity management framework [122].

Challenges

Blockchain provides a trustworthy solution to specific healthcare application challenges, such as security, privacy, integrity, sharing, interoperability, accessibility and real-time updates of medical data, particularly when applied correctly. However, blockchain has restrictions and limitations. Despite the advantages of blockchain technology, development and deployment in healthcare applications presupposed serious research challenges that require further investigation. This section discusses and identifies the challenges posed by blockchain technology. Figure 15 presents the category of these challenges.

Challenges related to security

The architecture and implementation of blockchain technology have several specific security vulnerabilities. Blockchain security vulnerabilities are often linked to problems with the traditional consensus mechanism used to confirm and verify transactions. These security vulnerabilities include DDoS, transaction malleability, difficulty raising, block discarding, eclipse, selfish mining, Sybil, 51%, block withholding and double-spending attacks. Consensus mechanism algorithms are unable to prevent these security threats in the distributed blockchain system. Thus, solving the threats with theoretical consideration is impossible owing to the expensive resources required [45, 46]. To overcome these security threats, the design of consensus mechanisms has minimal significance. That

Figure 15 Challenge Categories in Using Blockchain Technology in Healthcare Applications

is, a protocol with countermeasures that will prevent these attacks should be provided within an ideal solution. Security bugs allow malicious software activities to implement decentralised applications based on the developed blockchain. These malicious attacks exploit security bugs in the implementation of a smart contract to facilitate further offences, such as identity theft and data exfiltration [44, 127]. The use of blockchains presents another potential vulnerability (i.e. pseudo-anonymity), in which the flow of transactions can be traced to obtain physical identities or other additional information because of the public nature of the blockchain network [47].

Challenges related to privacy

The current secure communication architectures of EHR disregard users or patients' privacy, such as the exchanging system revealing all the data without the permission of owners or noise in the data requester summary. However, if the existing EHR applications are based on a blockchain, then the requester needs precise patient data to provide personalised services. The key challenge of protecting the privacy of patient data is to propose a framework that uses cryptographic mechanisms for data privacy and integrity on a blockchain-based EHR. This feature makes recognising any particular patient difficult by means of his current account number. In any similar framework, shortcomings should be addressed in maintaining patient's private data. Firstly, patients should share their data with ease of use because using blockchain-based frameworks within EHR requires high computational power and take substantial time to complete each task. Secondly, adding a new node to the blockchain network, which new patients need, requires numerous steps to verify the honest patient [77, 98].

Challenges related to latency and throughput restrictions

The majority of blockchain technologies will take time for consensus to be reached and transactions confirmed, which could be a problem in integrating blockchains into healthcare applications that need to react to events and data collected in real-time implementation. In the case of transaction latency, a blockchain takes time for processing transactions. For example, the bitcoin blockchain's latency requires 10 min to confirm any transaction in the network. Despite the fact that five or six blocks must be added to the chain before confirmation, the recommendation is to wait approximately one hour for confirmation of each transaction. By contrast, most traditional database systems only require a couple of seconds to confirm a transaction. [88]. In connection with throughput restrictions, RPM [106–108] and EHR [87] in IoT are based on a blockchain, in which systems typically need to handle huge volumes of transactions per second, thereby presenting possible challenge for blockchains. For example, the original bitcoin blockchain can reach up to seven transactions per second. Given that many transactions can be optimised (e.g. increasing block size), throughput is an essential parameter to consider in the selection of the appropriate blockchain for IoMT deployment [88].

Challenges related to blockchain size

When each device conducts transactions, such as IoT-RPM [106] and EHR [87], blockchains are constantly increasing and require the use of stronger miners. The traditional resource-constraint IoMT devices are incapable to handle even small size of blockchains. Therefore, compression methods in the blockchain with alternative approaches, such as mini-blockchains, should be studied [107, 108].

Challenges related to computing power limitations

IoMT device data gathered by blockchain are often computationally limited, such that cryptographic mechanisms may not be used [107]. In many health-related applications, cryptosystems in resource-constraint devices that handle sensor and actuator protection have extremely limited computational resources in terms of memory and processing power. That is, they are confronted with modern, secure public-key cryptography schemes. The majority of blockchains utilise public-key cryptosystems on the basis of ECC and have efficiency and security issues, thereby making the selection of the appropriate cryptography challenging. Cryptosystems in blockchains should be aware of the post-quantum computing threat and look for energy-efficient quantum-safe algorithms to keep data secure for a long time.

Challenges related to storage requirements

A blockchain requires significant storage to record whole transactions in the network, which can be a problem for restrictive nodes that send data to the network. Blockchain can ensure that the stored and shared EHR data are not manipulated, unforgeable and verifiable but can effectively suffer from storage requirements of large-scale distributed EHR data [78, 91].

Challenges related to scalability

The blockchain system presents another challenge in scalability and increasing overhead or computational resources in IoMT devices because of the increased number of system participants. Such a challenge could lead to computational requirements for the entire blockchain infrastructure. This situation becomes an increasingly difficult issue if many smart devices or sensors are present because these devices' computational capabilities are less than the average computer. The IoT devices in the

blockchain network are computationally demanding and involve a high overhead bandwidth resulting in data delays and significant processing power. Such devices may lack the computational power required to use blockchain capabilities, thereby possibly causing devices to run at suboptimal or potentially excessive speeds, thereby preventing them from even running their original or blockchain software simultaneously [127].

Challenges related to interoperability and standardisation

The lack of information collection, exchange and analysis structures leads to a lack of interoperability in healthcare applications. The existing EHR systems are managed with centralised local databases and offline architecture, whilst cloud-based blockchain technology is decentralised. Accordingly, moving healthcare systems towards this direction and implementing blockchain technology will firstly require an efficient EHR system capable of facilitating collaboration and interoperability between medical and scientific communities [84, 85]. Many technical challenges should be addressed in terms of EHR's migrated data to the blockchain technology. The existing healthcare ledger (database) is not distributed, which may not be integrated or developed to a wider scale [102].

Recommendations

This systematic review provides a few recommendations to mitigate the challenges faced by researchers and developers in integrating blockchain technology in healthcare application. These recommendations are categorised according to their nature (see Fig. 16).

Recommendations to researchers

Blockchain use offers many advantages, which can be used to solve various record-sharing, security and privacy problems within the healthcare application. Blockchain may not be the ideal solution that can be utilised in any situation. Instead, a thorough examination of specific blockchain issues and how they affect the application for healthcare should be evaluated. In healthcare applications, mining incentives that are the core mechanism of blockchain and specific blockchain attacks that can stop the entire system are not fully considered. We listed several recommendations as follows.

Improve blockchain security Numerous studies have been published on strengthening the security of the healthcare system through the use of blockchain as the new secured EHR [74, 76, 77, 80, 81, 83, 84, 92, 96, 100, 109]. Data security is an important part of healthcare and plays a crucial role in protecting sensitive data. Therefore, researchers should concentrate on certain problems and attacks associated with the blockchain, such as block withholding, 51%, double spending, selfish mining, eclipse, block discard, difficulty raising, pseudo-anonymity issues and smart contract software vulnerabilities. Further research should also focus on key management and security and the ability to replace lost or compromised keys easily.

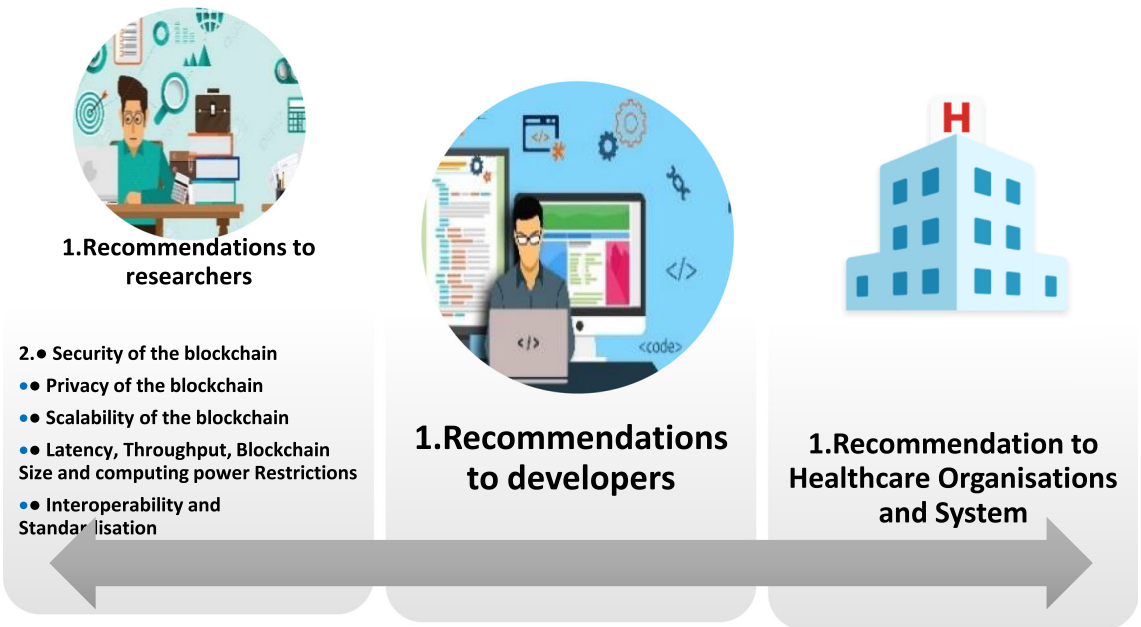

Figure 16 Categories of the Recommendations Using Blockchain Technology in Healthcare Applications

Improve the privacy of the blockchain Many studies have attempted to adopt blockchain technology to protect data health privacy in various situations [78, 79, 82, 86, 87, 90, 97, 98, 102, 107, 113]. The privacy protection of public blockchain in healthcare applications must fulfil the following prerequisites: (1) the connections between transactions should not be discoverable or visible and (2) the content of transactions patterns is known only to their participants. Nevertheless, a healthcare application based on a private or consortium blockchain capable of establishing an access control policy to fulfil the data protection prerequisites. For a public blockchain setting, the privacy protection of transactions is a 'double-edged sword'. On the one hand, a well-behaved patient would like to maintain his identity and action privately. On the other hand, a malicious entity may abuse the privacy protection mechanism for an illegal transaction. From the legal traceability and accountability perspectives, the protection of blockchain transactions in healthcare applications may be conditioned, such that the authority is reliable. Researchers should investigate how to track a targeted user and collect all the messages he has disseminated whilst protecting the sensitive information of the user from the public. From the improvement perspective, one potential research challenge is to enhance privacy in a blockchain but with untrustworthy environmental assumptions and low computational costs. Secure multiparty computation (MPC) is a promising solution to enable an untrusted third party to perform calculations on patient data without violating their privacy [97].

Improve the scalability of the blockchain Research should be conducted on the scalability of blockchain in healthcare applications as medical data increase. As the number of system members or patients increases, the applications enabled by blockchain will become exponentially difficult to run [127].

Improve latency, throughput, blockchain size and computing power restrictions Such issues as increasing throughput, reducing latency and reducing computing power have been associated with IoMT devices based on blockchain but can be extrapolated to other blockchain applications. The developments of healthcare applications for IoMT devices based on blockchain, the IoMT network, has a wide range of devices that communicate with each other simultaneously, requiring a network with high throughput and latency. Blockchain throughput and latency are affected by how the consensus algorithm works and how blocks are added to the blockchain network. Consensus algorithm confirms the transaction of each block added to the network, which often reduces latency and increases the overall throughput of blockchains, thereby significantly affecting the performance of the entire application. The insufficient performance of both factors usually adds difficulty in providing real-time responses to system events. In the case of blockchain size and computing power limitations, the use of mining, inefficient P2P protocols and computationally complex cryptographic algorithms have an impact on the energy consumption in every scenario, although such factors are critical when battery-operated devices are used. Therefore, future studies on the current topic are recommended.

Related to interoperability and standardisation Further research should be conducted with open-source real-world data sets to allow other researchers to verify results and disseminate findings. Many experiments focused on proof-of-concept and we should explore opportunities for collaboration between healthcare organisations and researchers to use real-world healthcare data to evaluate the proposed systems (e.g. security, performance, scalability and other essential properties, including privacy preservation).

Recommendations to developers

Blockchain allows multiple healthcare system entities to remain synchronised and share data on a commonly distributed ledger. Given such a system, participants can share and track their data and other activities that occur in the system without having to seek additional integrity and security options. Two types of blockchain, namely, permissioned (public) and permissionless (private), can be used on the bases of the requirements and access permissions of participants in a network. Permissioned blockchain is a closed network, where all participants involved in the system have access to the network. This blockchain is built and used inside organisations and enterprises to exchange information and secure transactions. Once a transaction is processed through consensus, the output will be treated as a permanent record and added as a new block to the existing blockchain. Permissionless blockchains provide access to anybody for creating an address and begin interacting with the network. Anyone on the network can interact with other participants on the same network by creating their address on the network [122]. The private or consortium blockchain is recommended to be used as an underlying system for the healthcare application model to mediate other problems, such as performance, energy consumption and scalability [98].

Recommendations to healthcare organisations and system

In the healthcare application, important patient data remain prevalent in different departments and systems. Hence, important data may not be accessed and easily available in times of need. Given that health care is a complex system with multiple entities, it requires patients to share their data and medical records across the ecosystem. The current healthcare ecosystem cannot be considered complete because many players in the system do not have a system in place to manage operations smoothly. Additionally, the increase in the number of patients

has resulted in increasing data, thereby leading to difficulties in managing patient information in hospitals and clinics. Moreover, this inadequate handling of information exchange requires some major challenges. For example, the misuse of available data prevents healthcare organisations from providing appropriate patient care and quality services for improved health. Nevertheless, these organisations are unable to meet patient needs despite a significant increase in the number and sophistication of studies that have responded to patient care and provided quality demand facilities. Blockchain has the potential to achieve significant breakthroughs in the healthcare ecosystem because it can easily make specific changes in patients' healthcare management. This technique will enable power to return to the people. Individuals will be responsible for dealing with their records, thereby gaining full control over their data. Blockchain technology can improve the quality of patient care whilst maintaining the security objectives of the system, such as confidentiality, integrity, availability, privacy, authenticity, trustworthiness, non-repudiation, accountability and auditability. All challenges and obstacles in multi-level authentication can be removed through the blockchain. As the adoption rate increases, blockchain is integrated into the healthcare sector. Even in its first phase, this technology is positively accepted by people in the healthcare ecosystem [104].

Future research directions

Compromised confidential data to unauthorised party in healthcare applications have reduced the level of patient trust towards the EHR system. Therefore, public trust may not be maintained if the privacy of sensitive health information is leaked. Although the current EHR system is considerably feasible and convenient, patients are constantly concerned with the safety and confidentiality of their health information. Therefore, we plan to propose the development and implementation of a platform for sharing EHRs amongst various health care institutions in Malaysia using blockchain and considering security and privacy protocols for handling patient data. Blockchain is the main component of a platform for patients to act as administrators for their data. Given the decentralisation and transaction transparency features of blockchain, the complete protection of patient privacy information cannot be maintained by using blockchain technology. A blockchain transaction in the EHR system can be defined as the process by which patient data are updated, created, deleted or transferred amongst the different nodes of a connected network. This platform makes enables the easy recognition of a particular node that visits the provider and the visit frequency, thereby enabling the collection of private patient information, such as names, disease and current address. Additionally, properly arranging the collected information and determining the connections within a blockchain network are issues that should be addressed. To conduct private and confidential transactions, we plan to propose a framework using the model of cryptographic protocols, such as trusted execution environments and non-interactive secure multi-party computation, which will enable private computation of encrypted transactions before being available into the blockchain. This framework would be used to preserve the data privacy of patients in the transaction of the EHR-based blockchain, thereby making the data confidential whilst anyone can verify the transaction without revealing any data publicly. In the future, we will explore the practical implementation of using a cryptographic protocol model for the encrypted transaction and attempt to evaluate the performance of enhanced blockchain on the decentralised healthcare application. The performance measurements of enhanced blockchain will be conducted on the transaction throughput, latency, execution time and resource consumption (CPU, Memory, Network IO).

Conclusion

The number of studies on blockchains in healthcare application continues to increase, although they have limitations that remain unaddressed. Blockchain is an emergent topic that warrants further investigation. The main contribution of this study is the comprehensive survey and classification of appropriate research articles on blockchain and their integration into different healthcare applications, in which particular literature trends are observed. Blockchain platform provides the development of a decentralised application, in which the pattern of data transactions is uncontrolled by any intermediary organisation. The entities' data transaction is stored in a decentralised database in a verifiable, secure, immutable and transparent manner with time stamp and other relevant details. Blockchain technology also offers the opportunity that could be used in healthcare applications for many prospective implementations. In the early stages of design and development, many studies have proposed solutions that have the potential to increase healthcare data transparency and operating efficiency. However, the security, privacy and scalability of blockchain technology will necessitate further research before substantial-scale production deployment. Consequently, the use of blockchain in healthcare applications should be assessed because this technology has security vulnerabilities and performance issues that must be addressed. Additionally, many healthcare applications have unique requirements that should be explored and addressed by blockchain. Despite the excellent potential of and vast interest in blockchain technology, we have found that its impact on healthcare remains in the documentation phase and research and clinical care applications have yet to be developed. The majority of the studies on healthcare applications based on blockchain solutions

continue to remain in the form of novel concepts and in a few operating products with restricted user base. The future of blockchain technology that eliminates intermediaries has immense potentials to exert a significant positive effect on health care and other industries.

Funding This study was funded by Universiti Pendidikan Sultan Idris, under Rising Star Grant, research code: 2019-0125-109-01.

Compliance with ethical standards

Conflict of interest The authors declare no conflict of interest.

Ethical approval All procedures performed in studies with human participation were in accordance with the ethical standards of institutional or national research committee and with the 1964 Helsinki declaration and its amendments or comparable ethical standards.

Informed consent Informed consent was obtained from all participants of this study.

References

1. Alanazi, H. O. et al., Secure topology for electronic medical record transmissions. Int. J. Pharmacol. 6(6):954–958, 2010.
2. O. A. Hamdan, et al., "Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance," J. Med. Plant Res., vol. 4, no. 19, pp. 2059–2074, 2010.
3. Nabi, M. S. A. et al., Suitability of SOAP protocol in securing transmissions of EMR database. Int. J. Pharmacol. 6(6):959–964, 2010.
4. Nabi, M. S. A. et al., Suitability of Using SOAP Protocol to Secure Electronic Medical Record Databases Transmission. Int. J. Pharmacol. 6(6):959–964, 2010.
5. Kiah, M. L. M. et al., An Enhanced Security Solution for Electronic Medical Records Based on AES Hybrid Technique with SOAP/XML and SHA-1. J. Med. Syst. 37(5):9971, 2013.
6. M. S. Nabi et al., Suitability of adopting S/MIME and OpenPGP email messages protocol to secure electronic medical records. In *Second International Conference on Future Generation Communication Technologies (FGCT 2013)*, 2013, pp. 93–97.
7. Kiah, M. L. M. et al., Open source EMR software: profiling, insights and hands-on analysis. Comput. Methods Prog. Biomed. 117(2):360–382, 2014.
8. Zaidan, A. A. et al., Evaluation and selection of open-source EMR software packages based on integrated AHP and TOPSIS. J. Biomed. Inform. 53:390–404, 2015.
9. Alanazi, H. O. et al., Meeting the Security Requirements of Electronic Medical Records in the ERA of High-Speed Computing. J. Med. Syst. 39(1):165, 2015.
10. Zaidan, A. A. et al., Multi-criteria analysis for OS-EMR software selection problem: A comparative study. Decis. Support. Syst. 78: 15–27, 2015.
11. Salman, O. H. et al., Novel Methodology for Triage and Prioritizing Using 'Big Data' Patients with Chronic Heart Diseases Through Telemedicine Environmental. Int. J. Inf. Technol. Decis. Mak. 16(05):1211–1245, 2017.
12. Mat Kiah, M. L. et al., Design and Develop a Video Conferencing Framework for Real-Time Telemedicine Applications Using Secure Group-Based Communication Architecture. J. Med. Syst. 38(10):133, 2014.
13. Almahdi, E. M. et al., Mobile patient monitoring systems from a benchmarking aspect: Challenges, open issues and recommended solutions. J. Med. Syst. 43(7):207, 2019.
14. Almahdi, E. M. et al., Mobile-Based Patient Monitoring Systems: A Prioritisation Framework Using Multi-Criteria Decision-Making Techniques. J. Med. Syst. 43(7):219, 2019.
15. Mohammed, K. I. et al., Real-Time Remote-Health Monitoring Systems: a Review on Patients Prioritisation for Multiple-Chronic Diseases, Taxonomy Analysis, Concerns and Solution Procedure. J. Med. Syst. 43(7):223, 2019.
16. Kalid, N. et al., Based on Real Time Remote Health Monitoring Systems: A New Approach for Prioritization 'Large Scales Data' Patients with Chronic Heart Diseases Using Body Sensors and Communication Technology. J. Med. Syst. 42(4), 2018.
17. Kalid, N. et al., Based Real Time Remote Health Monitoring Systems: A Review on Patients Prioritization and Related" Big Data" Using Body Sensors information and Communication Technology. J. Med. Syst. 42(2):30, 2018.
18. Albahri, A. S. et al., Real-Time Fault-Tolerant mHealth System: Comprehensive Review of Healthcare Services, Opens Issues, Challenges and Methodological Aspects. J. Med. Syst., 2018.
19. Albahri, O. S. et al., Real-Time Remote Health-Monitoring Systems in a Medical Centre: A Review of the Provision of Healthcare Services-Based Body Sensor Information, Open Challenges and Methodological Aspects. J. Med. Syst. (9):42, 164, 2018.
20. Mohsin, A. H. et al., Real-Time Remote Health Monitoring Systems Using Body Sensor Information and Finger Vein Biometric Verification: A Multi-Layer Systematic Review. J. Med. Syst. 42(12):238, 2018.
21. Mohsin, A. H. et al., Real-Time Medical Systems Based on Human Biometric Steganography: a Systematic Review. J. Med. Syst. 42(12):245, 2018.
22. Albahri, A. S. et al., Based Multiple Heterogeneous Wearable Sensors: A Smart Real-Time Health Monitoring Structured for Hospitals Distributor. IEEE Access 7:37269–37323, 2019.
23. Albahri, O. S. et al., Fault-tolerant mHealth framework in the context of IoT-based real-time wearable health data sensors. IEEE Access 7:50052–50080, 2019.
24. Napi, N. M., et al., Medical emergency triage and patient prioritisation in a telemedicine environment: a systematic review. Health and Technology, 9:1-22, 2019.
25. Nidhal, S. et al., Computerized algorithm for fetal heart rate baseline and baseline variability estimation based on distance between signal average and alpha value. Int. J. Pharmacol. 7(2):228–237, 2011.
26. Zaidan, B. B. et al., Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns. Int. J. Pharmacol. 7(3):382–387, 2011.
27. Kiah, M. L. M. et al., MIRASS: Medical Informatics Research Activity Support System Using Information Mashup Network. J. Med. Syst. 38(4):37, 2014.
28. Zaidan, B. B. et al., A Security Framework for Nationwide Health Information Exchange based on Telehealth Strategy. J. Med. Syst. 39(5):51, 2015.
29. Zaidan, A. A. et al., Challenges, Alternatives, and Paths to Sustainability: Better Public Health Promotion Using Social Networking Pages as Key Tools. J. Med. Syst. 39(2):7, 2015.
30. Hussain, M. et al., The landscape of research on smartphone medical apps: Coherent taxonomy, motivations, open challenges and recommendations. Comput. Methods Prog. Biomed. 122(3):393–408, 2015.

31. Hussain, M. et al., Conceptual framework for the security of mobile health applications on Android platform. Telemat. Informatics 35(5), 2018.
32. Alsalem, M. A. et al., Multiclass Benchmarking Framework for Automated Acute Leukaemia Detection and Classification Based on BWM and Group-VIKOR. J. Med. Syst. 43(7):212, 2019.
33. Enaizan, O. et al., Electronic medical record systems: decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. Health Technol. (Berl).:1–28, 2018.
34. Hussain, M. et al., A security framework for mHealth apps on Android platform. Comput. Secur. 75:191–217, 2018.
35. Iqbal, S. et al., Real-time-based E-health systems: design and implementation of a lightweight key management protocol for securing sensitive information of patients. Health Technol. (Berl).:1–19, 2018.
36. Alonso, S. G., Arambarri, J., López-Coronado, M., and de la Torre Díez, I., Proposing New Blockchain Challenges in eHealth. J. Med. Syst. 43(3):64, 2019.
37. Mohsin, A. H. et al., Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. Comput. Stand. Interfaces, 2018.
38. Mohsin, A. H. et al., Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication. Comput. Stand. Interfaces., 2019.
39. Mohsin, A. H., Based medical systems for patient's authentication: Towards a new verification secure framework using CIA standard. J. Med. Syst., 2019.
40. Bennett, B., Blockchain HIE Overview: A Framework for Healthcare Interoperability. Telehealth Med. Today 2(3):1–6, 2018.
41. Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, p. 9, 2008.
42. Founder, G. W., and Gavin E., Ethereum: a secure decentralised generalised transaction ledger, 2014.
43. Ethereum Foundation, *Solidity 0.4.24 documentation*. 2018.
44. N. Atzei, M. Bartoletti, and T. Cimoli, A survey of attacks on Ethereum smart contracts (SoK), *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10204 LNCS, pp. 164–186, 2017.
45. Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K., Where is current research on Blockchain technology? - A systematic review. PLoS One 11(10):1–27, 2016.
46. Li, X., Jiang, P., Chen, T., Luo, X., and Wen, Q., A survey on the security of blockchain systems. Futur. Gener. Comput. Syst., 2017.
47. Feng, Q., He, D., Zeadally, S., Khurram, M., and Kumar, N., A survey on privacy protection in blockchain system. J. Netw. Comput. Appl., 2018.
48. Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M., On blockchain and its integration with IoT. Challenges and opportunities. Futur. Gener. Comput. Syst. 88:173–190, 2018.
49. Panarello, A., Tapas, N., Merlino, G., Longo, F., and Puliafito, A., Blockchain and IoT integration: A systematic survey, vol. 18, no. 8. 2018.
50. Gao, Z., Xu, L., Chen, L., Zhao, X., Lu, Y., and Shi, W., CoC: A Unified Distributed Ledger Based Supply Chain Management System. J. Comput. Sci. Technol. 33(2):237–248, 2018.
51. Fernández-Caramés, T. M., and Fraga-Lamas, P., A Review on the Application of Blockchain for the Next Generation of Cybersecure Industry 4.0 Smart Factories. IEEE Access 7:45201–45218, Feb. 2019.
52. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H., Blockchain Challenges and Opportunities: A Survey. Int. J. Web Grid Serv.:1–24, 2016.
53. Radanović, I., and Likić, R., Opportunities for Use of Blockchain Technology in Medicine. Appl. Health Econ. Health Policy, 2018.
54. Androulaki, E., *et al.*, Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *ArXiv*, 2018.
55. Chase, B., and MacBrough, E., Analysis of the XRP Ledger Consensus Protocol. *a*, 2018.
56. Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., and Wang, J., Untangling Blockchain: A Data Processing View of Blockchain Systems. IEEE Trans. Knowl. Data Eng. 30(7): 1366–1385, 2018.
57. Anoaica, A., and Levard, H., Quantitative Description of Internal Activity on the Ethereum Public Blockchain, *2018 9th IFIP Int. Conf. New Technol. Mobil. Secur.*, pp. 1–5, 2018.
58. Feng, L., and Zhang, H., System architecture for high-performance permissioned blockchains. Front. Comput. Sci.:1–15, 2018.
59. Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., and Thompson, C., A Distributed-Ledger Consortium Model for Collaborative Innovation. Computer (Long. Beach. Calif). 50(9): 29–37, 2017.
60. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., and Saadi, M., Big data security and privacy in healthcare: A Review. Procedia Comput. Sci. 113:73–80, 2017.
61. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., and Toval, A., Security and privacy in electronic health records: a systematic literature review. J. Biomed. Inform. 46(3):541–562, 2013.
62. Zaidan, A. A. et al., A survey on communication components for IoT-based technologies in smart homes. Telecommun. Syst., 2018.
63. Zaidan, A. A. et al., A review on smartphone skin cancer diagnosis apps in evaluation and benchmarking: coherent taxonomy, open issues and recommendation pathway solution. Health Technol. (Berl). 8(4):223–238, 2018.
64. Albahri, O. S. et al., Systematic Review of Real-time Remote Health Monitoring System in Triage and Priority-Based Sensor Technology: Taxonomy, Open Challenges, Motivation and Recommendations. J. Med. Syst. 42(5), 2018.
65. Talal, M. et al., Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors: Multi-driven Systematic Review. J. Med. Syst. 43(3):42, 2019.
66. Zaidan, A., et al., A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. *Springer*. 2018.
67. Alsalem, M. A. et al., Systematic Review of an Automated Multiclass Detection and Classification System for Acute Leukaemia in Terms of Evaluation and Benchmarking, Open Challenges, Issues and Methodological Aspects. J. Med. Syst. 42(11):204, 2018.
68. Alsalem, M. A. et al., A review of the automated detection and classification of acute leukaemia: Coherent taxonomy, datasets, validation and performance measurements, motivation, open challenges and recommendations. Comput. Methods Prog. Biomed. 158:93–112, 2018.
69. Zughoul, O. et al., Comprehensive Insights into the Criteria of Student Performance in Various Educational Domains. IEEE Access:1–1, 2018.
70. Khatari, M. et al., Multi-Criteria Evaluation and Benchmarking for Active Queue Management Methods: Open Issues, Challenges and Recommended Pathway Solutions. Int. J. Inf. Technol. Decis. Mak.:S0219622019300039, 2019.
71. Talal, M. et al., Comprehensive Review and Analysis of Anti-Malware Apps for Smartphones. Telecommun. Syst., 2019.
72. Shuwandy, M. L. et al., Sensor-Based mHealth Authentication for Real-Time Remote Healthcare Monitoring System: A Multilayer Systematic Review. J. Med. Syst. 43(2):33, 2019.

73. Alamoodi, A. H. et al., A Review of Data Analysis for Early-Childhood Period: Taxonomy, Motivations, Challenges, Recommendation, and Methodological Aspects. IEEE Access, 2019.
74. Li, H., Fan, K., Yang, Y., Ren, Y., and Wang, S., MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. J. Med. Syst. 42(8):1–11, 2018.
75. Mikula, T., and Jacobsen, R. H., Identity and access management with blockchain in electronic healthcare records. In *Proceedings - 21st Euromicro Conference on Digital System Design, DSD 2018*, 2018, pp. 699–706.
76. Tamazirt, L., Alilat, F., and Agoulmine N., Blockchain Technology: A new secured Electronic Health Record System. In *2018 International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE'2018)*, 2018, p. 134.
77. Vora, J., *et al.*, BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. In *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018, no. 1, pp. 1–6.
78. Sun, Y., Zhang, R., Wang, X., Gao, K., and Liu, L., A Decentralizing Attribute-Based Signature for Healthcare Blockchain. *2018 27th Int. Conf. Comput. Commun. Networks*, pp. 1–9, 2018.
79. Guo, R., Shi, H., Zhao, Q., and Zheng, D., Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. IEEE Access 6:11676–11686, 2018.
80. Ramani, V., Kumar, T., Braeken, A., Liyanage, M., and Ylianttila, M., Secure and Efficient Data Accessibility in Blockchain based Healthcare Systems. In *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, no. pp. 206–212.
81. Yang, H., and Yang, B., A Blockchain-based Approach to the Secure Sharing of Healthcare Data. in *Norwgian Information Security Conference*, 2017.
82. Dagher, G. G., Mohler, J., Milojkovic, M., and Babu, P., Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. 39:283–297, 2018.
83. Wehbe, Y., Al Zaabi, M., Svetinovic, D., and Member, S., Blockchain AI Framework for Healthcare Records Management: Constrained Goal Model. *2018 26th Telecommun. Forum*, pp. 420–425, 2018.
84. Wang, H., and Song, Y., Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. J. Med. Syst. 42(8), 2018.
85. Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., and Chang, V., A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. J. Med. Syst. 42(8), 2018.
86. Liu, J., Li, X., Ye, L., Zhang, H., Du, X., and Guizani, M., BPDS: A Blockchain based Privacy-Preserving Data Sharing for Electronic Medical Records. *arXiv:1811.03223*, 2018.
87. Badr, S., Gomaa, I., and Abd-elrahman, E., Multi-tier Blockchain Framework for IoT-EHRs Systems. Procedia Comput. Sci. 141: 159–166, 2018.
88. Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., and Guizani, M., MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. IEEE Access 5:14757–14767, 2017.
89. Theodouli A., Arakliotis S., Moschou K., Votis, K., and Tzovaras, D., On the design of a Blockchain-based system to facilitate Healthcare Data Sharing. *2018 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng.*, pp. 1374–1379, 2018.
90. Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., and Liu, S., Blockchain-Based Data Preservation System for Medical Data. J. Med. Syst. 42(8):1–13, 2018.
91. Rouhani, S., MediChain TM: A Secure Decentralized Medical Data Asset Management System. *arXiv Prepr. arXiv1901.10645*, no. Section II, pp. 1533–1538, 2019.
92. Tian, H., He, J., and Ding, Y., Medical Data Management on Blockchain with Privacy. J. Med. Syst. 43(2):26, 2019.
93. S. Alexaki, G. Alexandris, V. Katos, and N. E. Petroulakis, "Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions," *2018 IEEE 23rd Int. Work. Comput. Aided Model. Des. Commun. Links Networks*, pp. 1–6, 2018.
94. Patel, V., A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics Journal, 2018.
95. Roehrs, A., André, C., and Righi, R., OmniPHR : A distributed architecture model to integrate personal health records. J. Biomed. Inform. 71:70–81, 2017.
96. Thwin, T. T., and Vasupongayya, S., Blockchain Based Secret-Data Sharing Model for Personal Health Record System, In *ICAICTA 2018 - 5th International Conference on Advanced Informatics: Concepts Theory and Applications*, 2018, pp. 196–201.
97. Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W., Healthcare Data Gateways : Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J. Med. Syst., 2016.
98. Zhang, A., and Lin, X., Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J. Med. Syst. 42(8), 2018.
99. Ito, K., Tago, K., and Jin, Q., i-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data. *2018 9th Int. Conf. Inf. Technol. Med. Educ.*, pp. 829–833, 2018.
100. Zhang, P., White, J., Schmidt, D. C., Lenz, G., and Rosenbloom, S. T., FHIRChain : Applying Blockchain to Securely and Scalably Share Clinical Data. Comput. Struct. Biotechnol. J. 16:267–278, 2018.
101. Velvkzhanin A., Kotsiuba I., Yanovich, Y., Bandurova, I. S., Zhygulin, V., and Dyachenko, Y., Decentralized e-Health Architecture for Boosting Healthcare Analytics. In *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE,* 2019, pp. 113–118.
102. Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., and Rahman, M. S., Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Futur. Gener. Comput. Syst. 95:511–521, Jun. 2019.
103. Chen, Y., Ding, S., Xu, Z., Zheng, H., and Yang, S., Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J. Med. Syst. 43(1), 2018.
104. Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., and He, J., BlocHIE: a BLOCkchain-based platform for Healthcare Information Exchange. *2018 IEEE Int. Conf. Smart Comput.*, pp. 49–56, 2018.
105. Uddin, A., Stranieri, A., Gondal, I., and Balasubramanian, V., Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture. IEEE Access PP(c):1, 2018.
106. Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., and Hayajneh, T., Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J. Med. Syst. 42(7):1–7, 2018.
107. Dwivedi, A. D., Srivastava, G., Dhar, S., and Singh, R., A decentralized privacy-preserving healthcare blockchain for IoT. Sensors (Switzerland) 19(2):1–17, 2019.
108. Brogan, J., Baskaran, I., and Ramachandran, N., Authenticating Health Activity Data Using Distributed Ledger Technologies. Comput. Struct. Biotechnol. J. 16:257–266, 2018.
109. Pham, H. L., Tran, T. H., and Nakashima, Y., A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract.

In *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018, no. 1, pp. 1–6.

110. Zhou, L., Wang, L., and Sun, Y., MIStore: a Blockchain-Based Medical Insurance Storage System. J. Med. Syst. 42(8), 2018.
111. Wang, S. et al., Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. IEEE Trans. Comput. Soc. Syst. PP: 1–9, 2018.
112. Choudhury, O., Fairoza, N., Sylla, I., and Das, A., A Blockchain Framework for Managing and Monitoring Data in Multi-Site Clinical Trials. *arXiv:1902.03975*, pp. 1–14, 2018.
113. Ji, Y., Zhang, J., Ma, J., Yang, C., and Yao, X., BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. J. Med. Syst. 42(8):147, 2018.
114. Zhao, H., Bai, P., Peng, Y., and Xu, R., Efficient key management scheme for health blockchain. CAAI Trans. Intell. Technol. 3(2): 114–118, 2018.
115. Liu, W., and Krieger, U., Advanced Block-Chain Architecture for e-Health Systems. In *In e-Health Networking, Applications and Services (Healthcom), 2017 IEEE 19th International Conference on IEEE.*, 2017, no. Etpha, pp. 37–42.
116. Novikov, S. P., Kazakov, O. D., Kulagina, N. A., and Azarenko, N. Y., Blockchain and Smart Contracts in a Decentralized Health Infrastructure, *2018 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol.*, pp. 697–703, 2018.
117. Ichikawa, D., Kashiyama, M., and Ueno, T., Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR mHealth uHealth 5(7):e111, 2017.
118. Roehrs, A., da Costa, C. A., da Rosa Righi, R., da Silva, V. F., Goldim, J. R., and Schmidt, D. C., Analyzing the Performance of a Blockchain-based Personal Health Record Implementation. J. Biomed. Inform.:103140, 2019.
119. Zhang, P., Walker, M. A., White, J., Schmidt, D. C., and Lenz, G., Metrics for assessing blockchain-based healthcare decentralized apps. In *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services, Healthcom 2017*, 2017, vol. 2017, pp. 1–4.
120. Zheng, K., *et al.*, Model Checking PBFT Consensus Mechanism in Healthcare Blockchain Network. *2018 9th Int. Conf. Inf. Technol. Med. Educ.*, pp. 877–881, 2018.
121. Kuo, T. T., Kim, H. E., and Ohno-Machado, L., Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. 24(6):1211–1220, 2017.
122. Gordon, W. J., and Catalini, C., Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Computational and Structural Biotechnology Journal 16. The Authors:224–230, 2018.
123. Hölbl, M., Kompara, M., Kamišalić, A., and Zlatolas, L. N., A systematic review of the use of blockchain in healthcare. Symmetry (Basel). 10(10), 2018.
124. Katuwal, G. J., Pandey, S., Hennessey, M., and Lamichhane, B., Applications of Blockchain in Healthcare: Current Landscape & Challenges. *arXiv:1812.02776*, pp. 1–17, 2018.
125. Ahmed, K., Junejo, A., Siyal, A., Khalil, A., Zawish, M., and Soursou, G., Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. Cryptography 3(1):3, 2019.
126. Kamel Boulos, M. N., Wilson, J. T., and Clauson, K. A., Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. Int. J. Health Geogr. 17(1):1–10, 2018.
127. Mcghin, T., Choo, K. R., Liu, C. Z., and He, D., Blockchain in Healthcare Applications: Research Challenges and Opportunities. J. Netw. Comput. Appl., 2019.