Internet of Things 19 (2022) 100551

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges

Md Shafiur Rahman [a,b,*], Md Amirul Islam [c,b], Md Ashraf Uddin [b,d], Giovanni Stea [c]

[a] National Academy for Computer Training and Research, Ministry of Education, Bangladesh
[b] Department of Computer Science and Engineering, Jagannath University, Bangladesh
[c] Department of Information Engineering, University of Pisa, Italy
[d] Internet Commerce Security Lab, Federation University, Melbourne, Australia

ARTICLE INFO

Keywords:
Blockchain
IoT
Healthcare
EHR challenge
Medical area

ABSTRACT

Blockchain (BC) technology has recently emerged as an essential component for different applications, including healthcare and IoT, because of its decentralized ledger, source provenance, and tamper-proof nature. The Internet of Things (IoT) and BC have enabled health systems to expand their scalability and maintain consistency on a decentralized platform. As a result, many researchers have developed BC-enabled IoT eHealth systems and explored the application of BC technology in diverse fields of eHealthcare. This paper conducts a comprehensive survey on the emerging applications of BC technology in healthcare. We summarize applications, research issues, security threats, research challenges, opportunities, and the future scope of BC technologies in the IoT-enabled healthcare system when BC is adopted to handle the privacy and storage of current and future medical records. Furthermore, we analyze the state-of-the-art BC works in the medical area, assessing their benefits-drawbacks, and guiding future researchers to overcome the limitations of the existing articles.

1. Introduction

BC technology has recently gained tremendous popularity among data-driven sovereign organizations due to its secure distributed ledger technology. BC can trace, correlate, bring out transactions, store data from numerous devices, and enable the creation of an applications environment that no need centralized storage [1,2]. Therefore, BC is an appropriate record technology that can positively impact different sectors, including financial and banking applications [3].

BC technology may alter the status quo in supply chain management, agriculture, the drone business, the education industry, logistics, the electricity industry, voting, computer gaming, and, finally, healthcare. BC can address the variety of problems in the eHealthcare system because of its fraud prevention and capacity to transmit information across nodes without requiring third-party trust [4].

BC is a chained data structure that chronologically combines transactions into data blocks. The interconnected blocks form a distributed ledger that cannot be tampered with or forged using cryptographic hashes. BC technology stores data in the form of a block, and it verifies and updates the block using distributed node consensus algorithms. In addition, it applies cryptographic algorithms to ensure secure data transmission and access [5].

* Corresponding author at: Department of Computer Science and Engineering, Jagannath University, Bangladesh.
E-mail addresses: shafiurcse@gmail.com (M.S. Rahman), mdamirul.islam@phd.unipi.it (M.A. Islam), mdashrafuddin@students.federation.edu.au (M.A. Uddin), giovanni.stea@unipi.it (G. Stea).

https://doi.org/10.1016/j.iot.2022.100551
Received 22 April 2021; Received in revised form 16 May 2022; Accepted 16 May 2022
Available online 24 May 2022

Table 1
Related literature reviews on Blockchain and IOT enabled Healthcare.

Year	Authors and Ref.	Main contributions
2021	Uddin et al. [7]	A recent survey paper that highlighted the application and challenges of blockchain in IoT. However, authors [7] did not comprehensively focus on the pressing issues of healthcare.
2020	Kavita et al. [9]	The authors reviewed IoT-based healthcare systems with their potential applications, issues, and challenges. However, many articles have recently proposed potential solutions for adopting blockchain in healthcare that is missing in [9]
2020	Leili et al. [10]	The paper presented a systematic review on blockchain-based healthcare systems considering publications between 2016 and January 2020. Therefore, a new review article is required to discuss the current problems and solutions
2021	Yaqoob et al. [11]	The authors mainly highlighted blockchain features and characteristics in healthcare data management. However, they did not focus on how blockchain works and eliminates the disadvantages of the conventional healthcare system.
2020	Houtan et al. [12]	The authors presented blockchain-based patient identity in healthcare
2019	Erikson et al. [13]	The authors discussed applications of the blockchain healthcare area. However, challenges and solutions were not focused
2019	Wang et al. [2]	The article focused on blockchain for the Internet of Things
2019	Taylor et al. [14]	They reviewed blockchain cyber security, but the discussion is not dedicated to healthcare applications

The ability to handle a large number of transactions for a scalable solution is an important feature of BC. However, BC technology brings several issues and challenges while changing the existing infrastructure. These issues include maintaining fairness for bonuses for exploration, mining attacks, storage management, and ensuring privacy. McGhin et al. [6] highlighted that the current BC could not meet all the requirements of healthcare applications. Despite the tremendous possibilities of BC in IoT applications, current BC has several limitations. In emerging BC technology, every network node participates in processing transactions, making BC inefficient and inadequate to handle real-world applications at a rate of tens of thousands of transactions per second [7].

Our article aims to present uses of BC technology in eHealth applications, highlight the challenges, and provide readers with possible research directions in that field.

Existing healthcare systems are based on a centralized database that suffers from a single failure point and a performance bottleneck. Furthermore, the healthcare system is regulated and operated by a third party or a central authority, raising concerns about the system's legitimacy, privacy, and health data transparency. Therefore, many researchers applied BC to address the existing challenges of the healthcare system. In addition, the current BC technology requires addressing scaling to achieve broader acceptance in the eHealth system [8].

BC researchers have recently published many review articles [2,7,9–14] that cover diverse aspects of BC technology and IoT-enabled healthcare systems. The most relevant existing review articles in the field of IoT-enabled healthcare systems are presented in Table 1 and also presents the main contribution and limitations of the state-of-the-art review articles.

Smart contract technology has recently evolved because of BC. Smart contracts have many applications in numerous fields, including IoT, shipping management, and the Internet of Vehicles, among others. Ourad et al. [15] proposed a BC-based solution and architecture for securely authenticating users to access IoT devices, as well as demonstrating how their proposed architecture overcomes the flaws of existing authentication schemes and allows for traceability, integrity, and accountability through tamper-proof logs. Hasan et al. [16] suggested an effective supply-chain management system, including items shipped through smart containers. The proposed system can handle and supervise the cooperation between the sender and receiver by utilizing the properties of smart contracts in the Ethereum BC. For example, IoT sensors are utilized to maintain shipment conditions, automatic payment systems, sanctions, and issue a settlement in case of violations. Furthermore, they used IoT sensors to track and monitor shipping conditions, including position, unexpected collapse, crumbled seals, temperature, and moisture. The authors implemented smart contracts in the Solidity language, and the Remix IDE environment was used for testing.

The IoT transportation paradigm has revolutionized transportation management, connecting sensors and smart cars. In addition, this paradigm is utilized in the Social Internet of Vehicles (SIoV) to build relationships among intelligent devices based on their application requirements. However, SIoV generates a massive amount of data collected and stored at multiple layers. This requires mechanisms to control privacy at each layer of the SIoV. Butt et al. [17] categorized the obstacles associated with privacy management and evaluated the layered architecture of SIoV in terms of seven features and issues.

Furthermore, the authors discussed how BC-based solutions could help users maintain their privacy in SIoV. The study highlights the critical variables behind the creation of an effective trust model for the SIoV [18]. This paper also covered the unique challenges of designing a trust model for SIoV and an overview of fog networking or fogging. Finally, the author emphasized that BC technology can build a decentralized trust-based SIoV model with high efficiency in dynamic vehicular networks.

Our paper emphasizes the issued with BC-Based IoT eHealthcare, the most recent state-of-the-art applications and challenges. Our review article is distinct from prior review articles such as [19] in a number of respects. We have explored a wide range of blockchain applications in the healthcare industry, synthesizing the current state of the art in terms of objectives, data, platform, and smart contracts. For readers with a variety of expertise and ability levels, we have highlighted a substantial number of obstacles

posed by blockchain adoption in healthcare. In addition, we provided an overview of the strategies used by cutting-edge works to tackle the difficulty of traditional healthcare systems.

Our contributions include the following:

- A background of BC technology describing its operation, structure, and importance is presented to benefit many readers.
- Analyzing IoT-enabled BC applications and challenges in the area of the healthcare system with the future research issues, opportunities, and directions on the blockchain.
- Outlining the benefits and pitfalls of current BC-based healthcare systems and identifying important open research challenges and future research directions.

The remainder of this paper is organized as follows: in Section 2, we report background material, including BC structure and operation. Then, BC-based IoT applications in the area of healthcare systems are discussed in Section 3. Next, research challenges in BC-enabled eHealthcare are discussed in Section 4. Finally, Section 5 gave the conclusion of our research works and highlighted upcoming research movements.

2. Overview of blockchain

BC implements a distributed ledger shared across a network of multiple localities or sites or several nodes or computing devices [20–22]. BC distributed ledger technology (DLT) has been widely researched since its conception in 2008. DLT eliminates the need for a centralized, trusted third party for distributed applications. This section presents the main functionalities and terminologies of BC.

Blockchain implements a distributed database of encrypted transactions across multiple network nodes. Transactions are bundled into a block, and all the confirmed blocks are interconnected using a cryptographic hash code to form a chain. Singhal et al. [23] described blockchain technology as an amalgamation of cryptography, game theory, and computer science. Ismail et al. [24] defined BC technology as a combination of distributed ledger, consensus protocols, and cryptography, i.e.:

$$Blockchain = \int (DL, CP, C) \tag{1}$$

where, DL = Distributed Ledger, CP = Consensus Protocol, C = Cryptography.

A BC's distributed database is securely accessed using cryptographic standards and protocols from different locations and time zones, including hash algorithms and PKI (Public Key Infrastructure). In addition, the distributed ledger is synchronized using different kinds of consensus protocols designed based on game theory. The most commonly used consensus protocols are Proof of Work, Proof of Stake, and Delegated Proof of Work.

2.1. Types of blockchains

Generally, BC can be classified into different categories based on the data being handled, the availability of that data, and the participants. Several types of BC are discussed below.

- *Permissionless Public Blockchain*: Anyone can join and leave the BC network in a public permissionless BC. A participant does not require permission to act as a miner or a normal BC node, and everyone has equal access. Participants' engagement and activities in such BC are ensured by providing incentives. Bitcoin, Ethereum, and Litecoin [19] are some popular permissionless public BCs that provide users with economic rewards.
- *Consortium Blockchain*: Unlike a public BC, a consortium-type BC enables only a chosen group of nodes to participate as controlling authorities in the distributed consensus process. Corda, Quorum, and Hyperledger are a few examples of consortium blockchain [19,25,26].
- *Private Blockchain*: A private BC is controlled, authorized, and governed by a particular entity. Users require permission from the authority to participate. Transactions are checked privately and might not be publicly readable. Private BCs typically produce blocks in shorter time frames and can result in more transactions than other types of BC. However, private BCs are vulnerable to data breaches as a single authority maintains the BC. On the other hand, a private BC guarantees a more significant level of security since only authorized miners to process the transactions [13]. Multichain [26] is an example of a private BC.

The basic operations of the blockchain technology have been demonstrated in the Fig. 1. Table 2 illustrates the types of BCs and compares their features (see Fig. 1).

Many studies describe BC technology by splitting functionalities among five layers, shown in Fig. 2 and discussed below.

- Application Layer: the application layer facilitates the environment and programming support needed to develop applications across multiple domains.
- Contract Layer: this layer embodies the static agreement information, including contract terms, situation reaction rules, and communication models. Significant technologies or components, including smart contracts, script coding, and incentive mechanisms, are included in this layer. Thus, this layer can be viewed as the static data of smart contracts, which incorporates guidelines about agreement summon, execution, and correspondence [5,29].

Table 2
Types of blockchains overview and comparison [6,27,28].

Property	Public blockchain	Consortium blockchain	Private blockchain
Trust in the network	Not required	Required	Required
Consensus determination	Each & every miners/explorers	Approved set of nodes	Single organization
Network join permission	Open	Restricted/Authorized	Restricted/Authorized
Read permission	Public	Restricted/Public	Restricted/Public
Immutability	Nearly impossible	Could be tampered	Could be tampered
Throughput	Low		High
Transaction visibility	All members	Selected authorized groups	Selected authorized members
Data privacy	Low	High	High
Centralized	No	Partial	Yes
Efficiency	Low	High	High
Consensus process	Permissionless	Permissioned	Permissioned

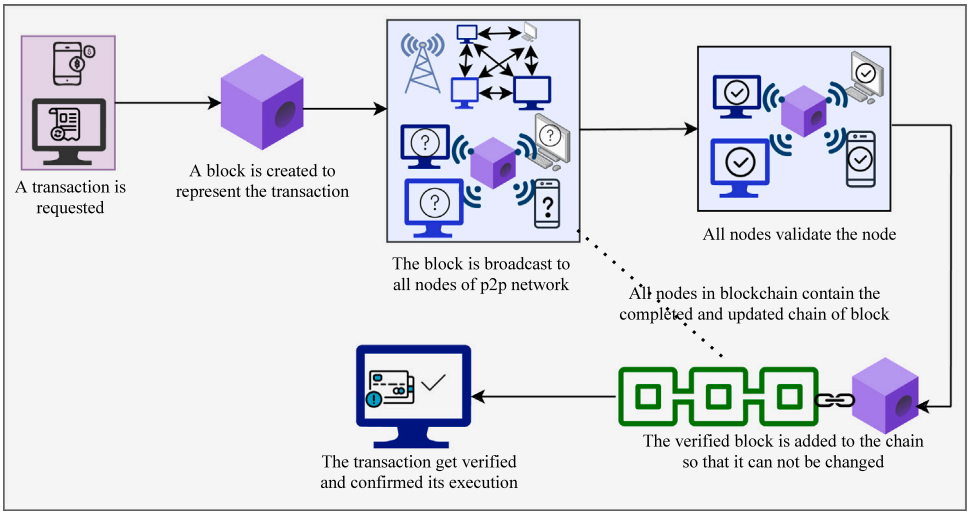

Fig. 1. The basic operation of BC technology.

- Consensus Layer: in the context of BC, the consensus mechanism refers to reaching an agreement among nodes regarding committing a block. The consensus protocol ensures that every node stores and maintains a unique chain. In other words, the consensus protocol indicates the guidelines required to guarantee that transactions are approved by following appropriate standards and principles of the BC.
- Network Layer: BCs work over a peer-to-peer (P2P) network. BC nodes are peers of the P2P network sharing information among themselves. This layer requires adopting privacy and security-related protocols.
- Data Layer: the data layer handles the structuring and storing of digital data in physical storage. The BC ledger consists of blocks linked between them using cryptographic hash code. A certain number of encrypted transactions using different encryption approaches are packed in Merkle trees.

2.2. Characteristics of blockchain

BC technology has a wide range of features, all of which are desirable in healthcare applications. More in detail:

- Decentralized Storage: BC technology's ability to decentralize a system is a crucial feature. Each and every transactions are processed and stored in a database that is replicated at, and managed by, all the nodes [24,30]. Anyone can connect to a BC network because the BC ledger is open to all (When BC is public).
- Transparency: One of the most appealing qualities of BC is its transparency. All transactions can be transparently inspected by anybody, possibly through the use of *block explorers*, used to search the blocks of a BC. At the same time, BC technology ensures data confidentiality, privacy, and authorization [11]. Furthermore, due to the transparent nature of the BC, clients can effectively update information and can unquestionably prevent information from being edited or robbed.
- Authentication: BC guarantees the authentication of private records and other data stored in the blocks. A particular private key that is attached to a public key initiates the formation/creation, editing, or inspecting of data reserve in the BC to achieve the authentication [31].

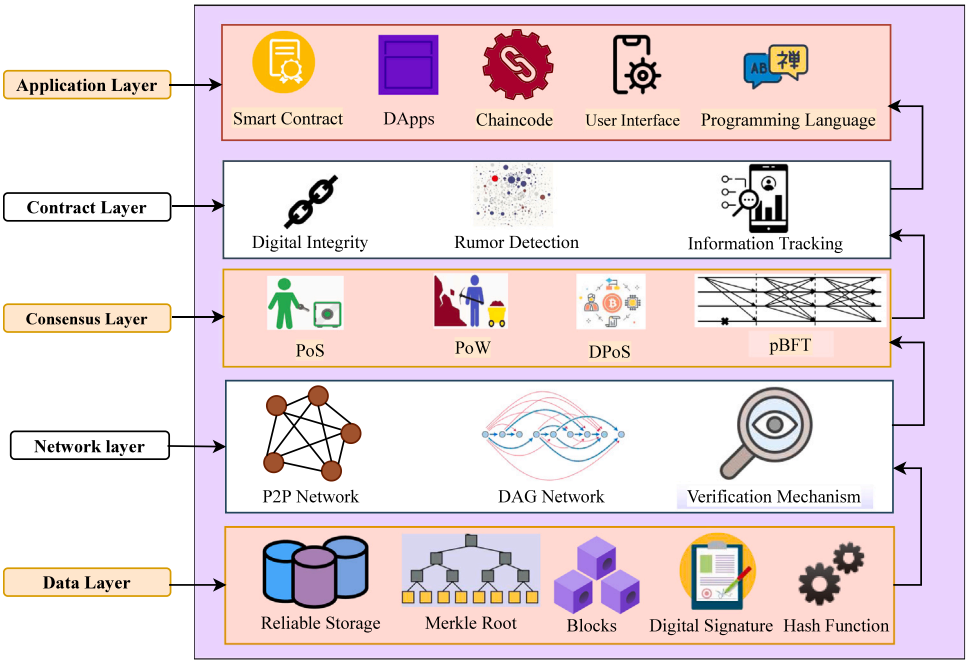

Fig. 2. Different layers of BC technology.

- Anonymity and Programmability: Anonymity is one of the most important characteristics used in public BC technology. Asymmetric encryption is used in BC. This anonymity guarantees that both senders and receivers involved in a transaction remain untraceable [5]. On the other hand, new transactions and controls can be automated through smart contracts by using programmability features [11].
- Enhanced Security: BC can tolerate malicious behavior. All participants in the BC hold identical copies of the ledger. Likewise, all members of the BC hold indistinguishable duplicates of the ledger. Any messing with the information will be distinguished and dismissed by BC peers [32]. In BCs, a primary component of security is the usage of private or public foundations, which can confine extortion and criminal operations in any area [7].
- Persistence: A transaction included in a BC cannot be rolled back or deleted. However, BC technology validates the transactions as soon as possible and also detects blocks that contain invalid transactions [28].
- Auditability: The distributed, transparent nature of BC technology makes it simpler to trace complex transaction events, for example, in a supply chain [33]. Furthermore, each update in the condition of the resource can be traced back to its inception. This facilitates auditing, with respect to financial or regulatory compliance, making a BC network safer, more productive, and straightforward. Additionally, BC can store and track the previous records of a patient that are significant for the patient's consideration [24].
- Immutability: The core concept of BC is built on a chain of immutable blocks, each of which holds important data. All transactions that occur in the BC are validated with the consensus mechanism and the code cannot be changed or altered after deployment [11,32,34].
- Autonomy: The BC framework is autonomous and independent, which means that every node on the BC framework may securely access, move, store, and update data, making it reliable and free of outside intervention [30].

2.3. Structure of blockchain

In a BC, the majority of data processing, validation, and manipulation takes place at the data, and network layers of the stack [5]. The BC refers to a back-linked list of blocks of transactions for storing digital data. Fig. 3 illustrates the architecture of a BC. In general, a BC contains three fundamental components: a block, a chain, and a network:

1. Block: A block is a group of valid or accurate transactions. For example, in a BC, any node can initiate a transaction and broadcast it to any node on the network [35]. A block contains a block header and a transaction list. The metadata in the block header includes the hash value of the immediately previous block and the transaction root hash value. A Merkle tree model/structure is used to organize all transactions. The root of the Merkle tree verifies every transaction.
2. Chain: A chain is a set of blocks arranged in a specific order.
3. Network: The network handles information propagation and verification, as well as node discovery (see Fig. 4).

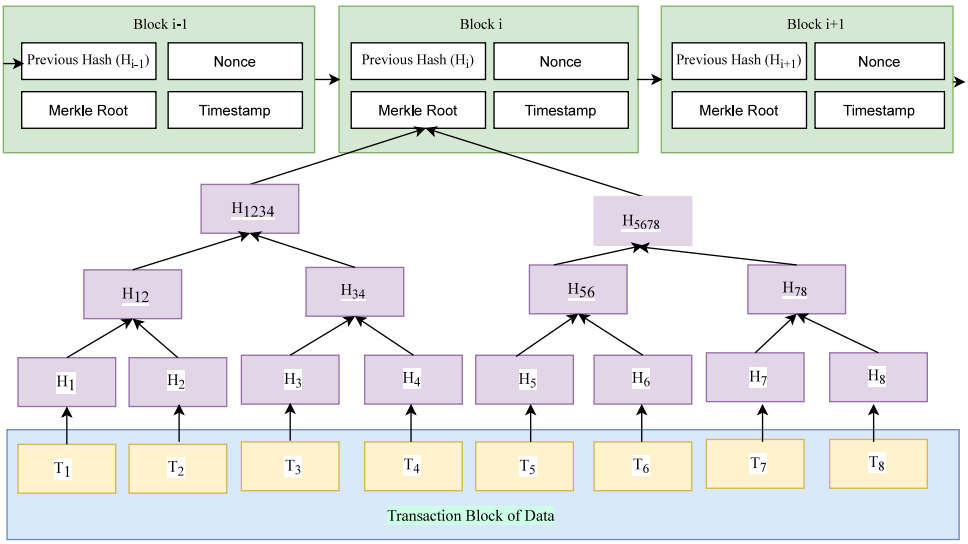

Fig. 3. Blockchain structure.

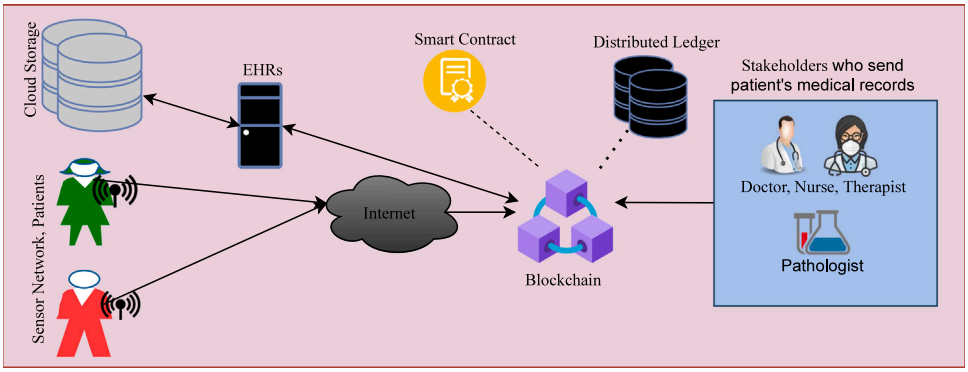

Fig. 4. The generic diagram of BC based eHealth system.

2.4. Cryptographic primitives in BC technology

In a conventional system, cryptography prevents third parties from accessing private data. Cryptography also provides security, reliability, and privacy for transactions in a BC. The following cryptographic approaches are utilized in most BCs, such as Bitcoin or Ethereum:

1. Public-Key Cryptography: Public-Key Cryptography (or asymmetric cryptography) utilizes a pair of keys, a public key, and a private key, to authenticate the user and get access to the data or message [36].
2. Hash Functions: a cryptographic hash, known as a digest, is a signature for a document or a data file. For example, the SHA-256 cryptographic hash algorithm associated with the BC technology generates hashes for verifying documents and ensuring message integrity while exchanging transactions [37].
3. Merkle Tree: the Merkle tree in BC technology is configured for packing transactions in a block [38]. The hash value of each transaction is included in the block header in the form of the root of the Merkle tree, where the Merkle tree is a binary tree or Patricia trie.

3. BC-IoT based healthcare applications

BC technology is redefining data modeling and governance used in many healthcare applications. This has been possible because of BC's agility and unparalleled capacity to separate, safeguard, and transmit medical data and resources [70]. BC technology might be a backbone for many recent advancements in the medical field. Blockchain-based medical care systems can advance security and privacy in managing healthcare data, applications, and stakeholders. Recently, many healthcare frameworks presented in Table 3

Table 3
Summary of existing BC-based IoT-enabled eHealth applications.

Authors	Year	Objective	Transaction data	Platform	Used smart contract?
Electronic Health Records (EHR)					
Huang et al. [39]	2021	eHealth system named BCES to achieve integrity of EHR	Medical Record	Private Blockchain	No
Zhuang et al. [40]	2020	EHR model to protect data security and patients' privacy.	SEER [41]	Ethereum	Yes
Guo et al. [42]	2020	Hybrid BC approach for EHR Management based on attributes.	EHR Data	Hyperledger Fabric, Hyperledger Ursa	Yes
Kim et al. [43]	2020	cloud-Assisted EHR system using ECC with cloud computing.	EHR data	Hyperledger fabric.	Yes
Chenthara et al. [44]	2020	A privacy-preserving architecture for securing data storage and providing efficient access control	Queried Dataset	Hyperledger	Yes
Chen et al. [45]	2019	Proposed searchable encryption approach for EHR.	Nursery dataset [46]	Ethereum	Yes
Tang et al. [47]	2019	Authenticated EHRs paradigm.	Medical related Data	JPBC	No
Bhattacharya et al. [48]	2019	An applications named BinDaaS based on BC and Deep-Learning.	EHR Dataset	Python+ Keras [49]+ TensorFlow	No
Vora et al. [50]	2018	Framework for efficient storage and maintenance of EHR.	Medical Data	Ethereum	Yes
Clinical Research (CR)					
Miyachi et al. [51]	2021	A hybrid framework for establishing privacy-preserving BC solution.	Healthcare data	Consortium Blockchain	Yes
Hardin et al. [52]	2021	A prototype implementation of Amanuensis capable of information provenance for health-data systems.	mHealth Data and Provenance Metadata	VeChain Thor [53]	Yes
Venkatesan et al. [54]	2021	eHealth record management system to secure and efficiently share healthcare data.	eHealth Records	Cloud/IPFS	Yes
Khatoon et al. [55]	2020	Proposed BC-based approach in healthcare ecosystem for data management.	Medical data.	Ethereum	Yes
Albanese et al. [56]	2020	A BC-based approach for trusted and decentralized management of clinical trials.	Medical Data	Hyperledger, web technology	Yes
Omar et al. [57]	2020	Suggested BC-based model for clinical trial data management system.	Clinical Data	Ethereum	Yes
Wong et al. [58]	2019	BC-based approach for collecting data in the clinical trial process.	Clinical Trial Dataset	Python, Django	Yes
Zhang et al. [59]	2018	Architecture designed to securely and scalably share clinical data.	HapiFHIR [60]	Ethereum	Yes
Medical Fraud Detection					
Saldamli et al. [61]	2020	Prototype for health insurance fraud detection.	Healthcare records and EDI 835 payments data	Ethereum	Yes
Mackey et al. [62]	2020	Framework and prototype to help prevent and detect healthcare fraud and abuse.	Healthcare Records	Ethereum	Yes
Kuo et al. [63]	2020	Framework for identifying and preventing healthcare fraud and abuse.	Healthcare claims and transaction data	Ethereum	Yes
Wei Liu et al. [64]	2019	Architecture for anti-fraud of healthcare insurance.	Healthcare insurance data	Cross-Cloud	No

(*continued on next page*)

Table 3 (*continued*).

Authors	Year	Objective	Transaction data	Platform	Used smart contract?
Pharmaceutical Industry					
Saxena et al. [65]	2020	"PharmaCrypt" solution for counterfeit drugs.	Healthcare Records	Ethereum	Yes
Clohessy et al. [66]	2020	Emergent multi-layer PBVIS model that can combat counterfeit medications.	Pharmaceutical Data	Ethereum	Yes
Pandey et al. [67]	2020	Reliable medicine authentication system to handle counterfeit medicines.	Medicinal Data Records	Ethereum	Yes
Raj et al. [68]	2019	Secure the immutable and traceable supply chain for pharmaceuticals to prevent drug counterfeiting.	Pharmaceutical Data	Hyperledger Fabric	Yes
Bryatov et al. [69]	2019	Control system for pharmaceutical drug turnover.	Healthcare Records	Hyperledger Fabric	Yes

have been proposed to implement BC and IoT technology in healthcare systems. The full form of the acronym used in Table 3 is presented in Table 4.

Huang et al. [39] proposed a BC-based eHealth system that would allow users to audit health data and detect data manipulation. Hospitals, consumers, and healthcare professionals record all types of operations on health data on the BC to track data alteration. In addition, they used attributes-based proxy re-encryption to ensure fine-grained access control of medical data.

Security, privacy, data inconsistency, and quick access to health records are issues the current healthcare system faces. To solve these issues, Zhuang et al. [40] developed a BC-based health system that uses smart contracts to handle data storage and access management. By personalizing data segmentation and constructing an "approved list" for clinicians to access their data, this strategy achieves patient-centric HIE.

Gathering and processing IoT data in a traditional centralized system threaten availability, integrity, and privacy. Makhdoom et al. [71] proposed "PrivySharing" as a way for smart cities to share health data. To protect health data privacy, they advised data segmentation and different channels. A reward system was also developed for sharing users' data with stakeholders/third parties.

To govern electronic health records (EHRs) data access, Guo et al. [42] proposed a hybrid architecture that includes both BC and edge nodes. Identification and access control regulations are administered by a BC-based controller, which also maintains an account of access events. Furthermore, off-chain edge nodes store EHR data and employ ALFA policies with BC-based access control logs to enable attribute-based access control on EHR data.

BC technology to transmit EHRs among healthcare providers has grown increasingly common in recent years. EHR data cannot be stored on a BC because of their size and the associated expense. This problem can be solved via cloud computing. Storage and scalability are the advantages of cloud computing. However, cloud-based EHR systems are vulnerable to multiple attacks if sensitive data is sent over a public channel.

For cloud-based EHR, the authors [43] recommended a safe BC system. Data integrity and access control are ensured by transaction logging, while patient EHRs are stored and administered on a cloud server. In order to protect cloud health data, they used elliptic curve cryptosystems (ECCs). In [44], authors have represented a BC technology-based framework called "Healthchain" on privacy protection of EHRs. This framework can preserve the integrity, privacy, security, and scalability of healthcare data. To construct this "Healthchain" framework, authors utilize the InterPlanetary File System (IPFS) and Hyperledger, composer. Furthermore, a novel cryptographic public-key encryption algorithm is used to store encrypted data on the IPFS; as a result, robustness is achieved in the healthcare data.

Patient privacy is jeopardized when EHR data are leaked. BC might be used to make data exchange easier and to ensure that health data are not tampered with. In [45], the authors presented a BC-based EHR encryption system that uses complex logic expressions to allow users to search the data using a particular set of indexes stored on the BC. This method ensures the index's integrity, anti-tampering, and traceability.

Tang et al. [47] presented an authentication scheme for a BC-based EHR system named MA-IBS. This method uses efficient signature and validation algorithms that can withstand collision attacks. Bhattacharya et al. suggested a platform called BinDaaS [48] that uses BC and deep learning to transmit healthcare records among many healthcare customers. Vora et al. [50] presented a BC-based architecture for the effective storage and management of EHRs for the benefit of patients, stakeholders, and third parties.

The research and study of health, wellness, and illness using BC technology with privacy issues are accelerating. Miyachi et al. [51] presented a hybrid privacy-preserving paradigm based on BC technology. The system facilitates the interaction between on-chain and off-chain storage in a secure, scalable, and patient-centric manner and explores performance tradeoffs concerning critical healthcare datasets. To address the challenges associated with developing a trusted and secure data sharing ecosystem for mobile health devices, Hardin et al. [52] proposed a new approach called *amanuensis*, which leverages BC and Trusted Execution Environment (TEE) technologies to acquire data provenance for mHealth with limited scope for privacy-preserving BC techniques. Venkatesan et al. [54] proposed an eHealth record management system to rescue the data from miscellaneous attacks. The IPFS, or cloud, stores the encrypted eHealth records. The integrity, confidentiality, and availability of the data are ensured by storing the meta-data on the blockchain. In addition, the proposed model can provide flexible entry reports for audits and regulatory obedience

Table 4
Explanation of notations.

Notations	Definition
EHR	Electronic Health Records
ACL	Access Control Lists
ALFA	Abbreviated Language For Authorization
MA-IBS	Identity-Based Signature Scheme with Multiple Authorities
BinDaas	Blockchain-Based Deep Learning as-a-Service
DL	Distributed Ledger
CP	Consensus Protocols
IPFS	Inter Planetary File System
HIPAA	Health Insurance Portability and Accountability Act of 1996
JPBC	Java Pairing-Based Cryptography Library.
ECC	Elliptic Curve Cryptosystems.
PBVIS	Pharmaceutical Blockchain Vigilant Information System
IS	Information System
GDPR	General Data Protection Regulation

and remove the redundancy of the patient account. Khatoon et al. [55] demonstrated the usage of the Ethereum BC platform to manage and access a large amount of medical data via a BC-based medical smart contract system. This is reasonable and feasible in realistic scenarios involving low-cost healthcare data management systems.

Albanese et al. [56] developed a BC-based consent management system for clinical trials called SCoDES. Here, BC keeps all consent records with trust assurances while avoiding the necessity for an ad-hoc third party. The authors produced a superior technique for addressing consent with confidentiality and employed the REDCap software to store medical data.

Omar et al. [57] utilized Ethereum smart contracts to manage documents & workflow among stakeholders in Clinical Trials (CTs). The authors used Remix IDE to create the Ethereum smart contract and depicted algorithms needed to capture distinct phases of CT data handling. A decentralized warehousing system was also developed to store CT records instead of directly storing them on the BC.

CTs in the current complex settings are getting increasingly challenging. Wong et al. [58] presented a BC-based prototype to provide a balanced service for all members within the CT environment in order to make the CT process irreversible, traceable, and trustworthy. They collected genuine CT data and simulated a proof of concept to conduct the experiment on the proposed approach. However, this system does not address the issue of public data sharing. For integrated clinical decision-making, secure and scalable data sharing is essential.

Zhang et al. [59] introduced the FHIRChain BC-based architecture to facilitate effective healthcare and clinical data sharing. In addition, they developed a decentralized software that uses digital health self-identity to verify users to facilitate collaborative decision-making. As a result, FHIRChain can securely share users' health data with different stakeholders.

With today's widespread diffusion of Internet technology, healthcare data have become more appealing to cybercriminals. As a result, experts devised protocols and structures to protect healthcare data from cyber-hackers and attackers and deter them. Saldamli et al. [61] developed a BC-based conceptual model or prototype for detecting healthcare insurance fraud, as well as preventing fraud by adhering to HIPAA requirements. Mackey et al. [62] developed a BC-based framework and prototype to aid the detection and prevention of healthcare fraud and abuse. The authors used BC application layers to create their prototype and framework, including smart contracts, governance based on digital identification on the Ethereum foundation, token consensus techniques, and essential BC technologies. Kuo et al. [63] pioneered the use of BC technology to automate health care and biomedical applications and also provided a framework for mitigating healthcare fraud and abuse. As ModelChain uses authorized BC networks, malicious nodes cannot join the network, reducing the possibility of a 51% attack. Liu et al. [64] developed an architecture that includes an application layer, a core layer, a network layer, a cloud platform layer, and an interface layer. This architecture makes health insurance data secure against fraud. In addition, the authors discussed a strategy for data sharing between chains and the preservation of data privacy.

Drug counterfeiting is a serious and widespread problem that jeopardizes the health of customers and the wider public. As a result, the illegal medication industry generates billions of dollars each year. Saxena et al. [65] investigated the problem of counterfeit medications and offered the "PharmaCrypt" solution based on BC technology. This BC-based application is used to trace and track medications as they move through the pharmaceutical supply chain, uploading the information to a distributed BC ledger to ensure security, safety, and authenticity. In addition, the authors developed a "PharmaCrypt" prototype using the Amazon Web Services BC platform.

Clohessy et al. [66] studied pharmaceutical BC technology using an inductive grounded theory method and developed a Pharmaceutical Blockchain Vigilant Information System (PBVIS) multi-layer observe–orient–decide–act (OODA) theoretical model. This model implemented a BC-aware information system and provided a comprehensive view of supply chain control in the pharmaceutical domain. Pandey et al. [67] used BC to model trustworthy and secure e-health distribution networks against counterfeit medicine invasion. This system can detect counterfeit pharmaceuticals promptly and stop marketing the counterfeit medicines. They simulated the entire system using the Hyperledger Fabric platform. Raj et al. [68] demonstrated the use of BC technology to provide evidence of ownership throughout the pharmaceutical supply chain, thereby preventing drug counterfeiting. This system can be traced back to guarantee that a legitimate business produced the medicine because the ledger is irreversible. The

Table 5
State-of-the-art literature addressing the problems of conventional healthcare system.

Literature	Elimination of third parties' intervention	Preserving privacy (Access Control)	Enforcing security	Rapid access	Cost effective access	Real prototype design
Zhuang et al. [40]	The authors introduced and developed a private Ethereum blockchain technique with numerous smart-contract functions to eliminate the need for third parties to supervise health data	User data privacy and security were guaranteed using a P2P network technique	User data is stored in the smart contract to enforce higher security	"Allowed List" was implemented in the smart contract to access data rapidly	An incentive technique was used to encourage patients, and healthcare specialists to use and join these models	Prototype was developed
Guo et al. [42]	The authors implemented a hybrid architecture using BC technology and stored encrypted EHR data on the edge node to eliminate the involvement of third parties' intervention	Privacy of User's data was ensured using an EHR access activities control mechanism	Encrypted EHR data stored on the edge node to enforce higher security	ACL (Access Control List) mechanism was used for faster access	ABMS (Attribute-Based Multi-Signature) & ABE (Attribute-Based Encryption) scheme is used to increase the throughput of the architecture	Prototype was applied in a practical situation (Used Hyperledger Fabric & Hyperledger Ursa)
Chenthara et al. [44]	The authors developed a distributed healthcare framework by utilizing BC & patient-centric interoperability to avoid the involvement of third parties' intervention	Privacy of User's data was ensured using a hash-based access control mechanism	Actual EHR is stored in InterPlanetary File System (IPFS) after encryption (off-chain framework), and the only hash value is stored on-chain to enforce the higher security	Hyperledger Composer & ACL mechanism is used for faster access	An incentive technique was used to encourage patients, healthcare specialists, and business process applications to use and join these models	Prototype was applied in a practical situation
Tang et al. [47]	The authors introduced and implemented an authentication scheme for a BC-based EHR system named MA-IBS to eliminate the involvement of third parties' intervention	User's data privacy was ensured using an identity-based signature scheme	Efficient signature scheme, verification algorithms and random oracle model was used to enforce higher security	EHR was stored at multiple levels, including IoT devices and Cloud networks, to faster access data	A decentralized consensus mechanism was developed to minimize signing, communication, & verification costs and increase throughput by resisting collusion attacks	Prototype was not applied in practical situation
Bhattacharya et al. [48]	The authors designed a decentralized healthcare system by using BC-deep learning as-a-service to avoid the involvement of third parties' intervention	EHR records of patients' Privacy was ensured using a lattice-based key & signature scheme	EHR that is effective for medical purposes is stored in the blockchain, and random oracle model is used to enforce higher security	Patients record was stored at multiple levels for faster access	A decentralized consensus mechanism was implemented to minimize mining time, computation and communication cost	Prototype was applied in a practical situation

(*continued on next page*)

proposed authorized BC technology can provide the pharmaceutical supply chain system safety, security, visibility, and traceability. Bryatov et al. [69] developed and implemented a BC-based pharmaceutical turnover control system based on Hyperledger Fabric to combat counterfeit medical products and pharmaceuticals. The proposed technique detects only the direction of drugs within official supply channels. However, the system cannot trace and track counterfeit medicines that circulate outside official supply chains.

The breakdown of the state-of-the-art blockchain works that address the challenges and problems of the conventional healthcare system is presented in Table 5.

Table 5 (*continued*).

Literature	Elimination of third parties' intervention	Preserving privacy (Access Control)	Enforcing security	Rapid access	Cost effective access	Real prototype design
Vora et al. [50]	The authors represented a decentralized BC-based framework named BHEEM to eliminate the involvement of third parties' intervention	Privacy of patients' private data was ensured using encryption schemes	Patients data that is effective for medical purposes is stored in the blockchain to enforce higher security	Hash based access control mechanism was used for faster access	A decentralized consensus mechanism was implemented to minimize storage, mining, and communication cost	Prototype was not implemented
Uddin et al. [72]	The authors designed a decentralized health system by using blockchain and distributed patient-centric agent to avoid the involvement of third parties' intervention	Data privacy was maintained using ring signature	Data is stored and processed at multiple levels including IoT devices, Edge network, and Cloud network	Data was stored at multiple levels for faster access	A decentralized consensus mechanism was developed to minimize power consumption and increase throughput	Prototype was not applied in practical situation
Uddin et al. [73]	The authors introduced a decentralized patient-centric agent to eliminate the need for third parties to supervise health data	Privacy of User's data was ensured using a lightweight hash-based access control mechanism	Data that is significant for medical purpose is stored in the blockchain to enforce higher security	Tri tree was implemented for faster-accessing data	An incentive mechanism was introduced to motivate patients and healthcare professional to use the system	Prototype was not developed

Table 6
Research challenges in BC-based healthcare systems.

Application area	Target research challenge	Explanation
Healthcare data access control	Managing access control	This provides a more secure method of accessing patient's medical records.
Research and clinical data share	Accessibility of protected data	This safeguards medical records, facilitates data sharing among stakeholders, and ensures traceability for critical research.
Global data sharing	Secure collection and sharing of global data	Secure access to healthcare data should be available from everywhere.
Control of drug supply chain	Combat counterfeiting and pilfering of supply chain process	Managing and tracking the sequence of operations on supplies in healthcare facilities.
Billing/Payers	Latency/Fraud in paying bills	Providing healthcare payment options based on BC which are going to be faster, less complicated and more secure.

4. Research challenges

A BC-enabled IoT system is prone to errors and brings some research and design concerns. The primary challenges of a BC-enabled IoT approach in healthcare data management systems are presented in this section. Fig. 5 depicts the current research challenges in healthcare industries. We describe the underlining reasons for these claims and suggestions for new researchers approaching this domain. Table 6 shows the workflow of research challenges in BC-based healthcare systems.

4.1. Scalability

Scalability is one of the key challenges of BC technology that hinders widely adopting BC in the healthcare sector — as well as in other application domains [74]. Scalability is a major barrier to meeting the increasing demand from various industries and government agencies [7,75].

4.2. Privacy leakage

In eHealthcare systems, privacy-related mechanisms enable consumers to select who can view their sensitive information. However, in BC, a user can have multiple addresses and information is open to all. BC cannot secure transactional privacy since the values of all transactions and balances for each public key are publicly visible [76,77].

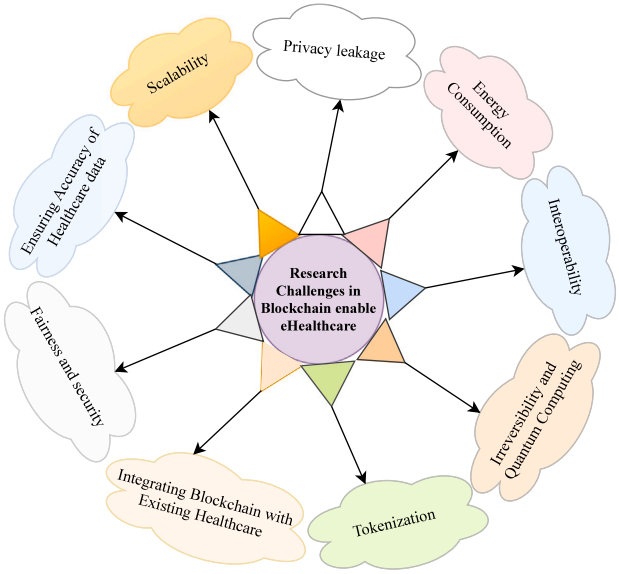

Fig. 5. Research challenges in BC-enabled eHealthcare.

4.3. Energy consumption

Energy consumption is an essential dimension to recognize when interpreting a blockchain-based IoT solution. Blockchains consume a massive amount of energy because of their provided algorithms. As a result, energy consumption is exorbitant in academia, business, and society; frequently, generalizations used for blockchain enable IoT [78,79]. For example, Proof-of-Work consumes more energy than Proof-of-Stake.

4.4. Interoperability and traceability

Interoperability between BCs is one of the primary impediments to widespread adoption of BC applications. Madine et al. [80] presented a solution for BC interoperability based on decentralized applications.

Future researchers might encounter a significant challenge in developing standards to facilitate interoperability among BC-based systems. Interoperability is a critical prerequisite for BC-based healthcare systems' long-term viability, and management [81]. In addition, interoperability can be leveraged to standardize and optimize healthcare quality, as there is a need to maintain many communication protocols for interacting with medical equipment, including sensors and BC aid.

To accomplish traceability, traditional methods rely on a central authority to modify data without informing other stakeholders. However, this does not provide transparency and may result in a performance bottleneck and a single point of failure [82].

4.5. Irreversibility and quantum computing

Ensuring the irreversibility of health data has not been possible in today's centralized healthcare systems because they are subject to hackers and data privacy breaches—irreversibility of data guarantees that sensitive data is not tampered with. Irreversibility is achieved by combining standard cryptography and the BC hashing process. However, research towards reducing the immutability of BC in order to ensure security is still in its infancy [83,84].

4.6. Tokenization

The tokenization of real-world tradable assets has sparked much interest in recent years. Tokenizing assets as a commodity overcomes the lack of audibility in BC and smart contracts [85]. Tokenization in BC technology dramatically increases efficiency by lowering transaction costs, diminishing transaction time, advancing infrastructure liquidity, and enhancing clarity.

4.7. Integrating blockchain with existing healthcare systems

BC enables secure transactions among stakeholders and centralized data sources in healthcare industries. BC technology can modify, restructure, and rebuild the behavior of data used in healthcare applications [11]. Healthcare systems collect data from a wide range of devices, resulting in a massive amount of data records. Researchers need to overcome significant obstacles to integrate BC technology into healthcare applications to preserve the integrity of health data.

4.8. Fairness and security

The widespread adoption of a BC-based healthcare framework will allow it to store and transfer application data in a transparent, secure, and decentralized manner without needing a central control point. With the growing number of interconnected devices and online transactions, processing a large volume of transactions from many heterogeneous devices and preserving data security and fairness are now research challenges.

Cybercriminals target sensitive data of healthcare industries because health data are always lucrative to hackers. Therefore, securing health data is the top priority for healthcare providers [86].

4.9. Ensuring accuracy of healthcare data

Data in the healthcare industry is used for analysis, research, management, and patient supervision. A healthcare system collects vast amounts of physiological and medical data, making the system more useful than ever [87]. Having accurate healthcare data increases participants' confidence and speeds up patient monitoring and medication. In BC technology, different users record health data from the diverse platform. Therefore, ensuring accurate data from diverse stakeholders is challenging in BC-based healthcare systems.

4.10. GDPR compliance

GDPR regulates the accumulation, processing, and securing of personal data responsibly and transparently to give back control of data to its owner [88]. Using GDPR is to make it more manageable and more inexpensive for companies to comply with data protection laws. GDPR and HIPAA are used mainly to contribute to mitigating the threat of privacy violations in healthcare data [89]. It preserves the right to restrict the processing of healthcare data.

4.11. Security and smart contract vulnerabilities

Non-repudiation, integrity, confidentiality, authentication, and authorization are key security requirements. Man-in-the-Middle (MITM) attacks and replay attacks are frequently encountered in a communication system. Therefore, producing smart contract code which is bug-free and immune to security attacks is of paramount importance.

However, guaranteeing smart contract code is safe from risk, attack, or vulnerability is not always possible due to inherent design issues. As a result, massive financial losses might result from security attacks [90].

A hard fork and 3.6 million Ethers of the Ethereum network were lost as a result of the decentralized autonomous organization (DAO) [91]. Indeed, this type of attack occurs when a hacker calls a function recursively in the smart contract code before completing the first call. Consequently, reentrancy is possible in the smart contract code. To eliminate vulnerabilities, this must be tested periodically using security analysis tools, such as Oyente [92,93].

1. **Non-repudiation:** The initiator calls are logged and cannot be tampered with because the off-chain transaction on the Ethereum BC and the instances are all tamper-proof logs signed by the smart contract. As a result, everyone has to accept their activities and actions because all activities are already documented in the log file. In addition, if attackers attempt to copy or alter the user token or Ethereum Address (EA) and public key, they will be unable to do so because the correct private key to sign it is not available [93,94].
2. **Integrity:** On the Ethereum BC, all messages exchanged between two users are tamper-proof and cannot be changed [93]. Furthermore, the off-chain transaction between the users and server is protected with timestamps, an authentic user token, or a private key already communicated in the chain. The whole system is secured against MITM and replay attacks, achieving integrity security requirements [94].
3. **Confidentiality:** Confidentiality can be achieved by preventing unauthorized access to IoT devices and users' data. Furthermore, confidentiality can be ensured by using encryption and decryption techniques through secure SSL sessions upon successful user authentication [93,94]. BC technology offers a powerful feature that allows each user or IoT device to be allocated a unique 20-byte EA instantaneously and with almost no collisions [95]. EA asymmetric public key pairs are used to establish the SSL session for communication between the IoT devices and the authenticated user [96].
4. **Authentication and Authorization:** Only some authorized entities have full access to the smart contract's functions. For example, if any unauthorized access is detected, all states will be restored, generating an error. Furthermore, off-chain contact between the file server and clients is dependent on an effectual handshake for authentication, which permits the content to be downloaded via a secure SSL link. As a result, the transmission is protected against DDoS (Distributed Denial of Service) attacks [80,93,94].

5. Conclusion

This article investigated the IoT-enabled application with blockchain and research issues in the healthcare system. We also pointed out the research challenges of blockchain in healthcare. Furthermore, blockchain-based health care systems face additional challenges, such as system evolution, privacy leakage, energy consumption, and communication scalability, due to the complexities associated with healthcare engagement and laws. This review summarizes the state-of-the-art works on blockchain in the healthcare sector. Future research might consider incorporating more technological characteristics to improve feasibility evaluation and narrow the gap between ideas and implementations, propelling healthcare technology. Moreover, the additional study should also address how blockchain and IoT-enabled accomplishments can concur with existing healthcare data rules, integrity, and standards. Although the ledger is updated based on the latest transaction, the miners need to use more energy to maintain synchronization among nodes. Furthermore, blockchain-based applications rely on nodes to function correctly with a lack of Distributed Computing approach. Our future work involves combining the study of energy consumption and consensus algorithms to identify and analyze their functions to improve the scalability of blockchain in various domains.

Declaration of competing interest

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

Acknowledgments

We would like to thank the anonymous reviewers for their rigorous and constructive comments. We believe that they have helped us to improve and finalize the manuscript, for which we are grateful.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, Ieee Access 6 (2018) 32979–33001.
[2] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, Comput. Commun. 136 (2019) 10–29.
[3] L. Bell, W.J. Buchanan, J. Cameron, O. Lo, Applications of blockchain within healthcare, Blockchain Healthcare Today 1 (8) (2018).
[4] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, M. Ylianttila, Blockchain utilization in healthcare: Key requirements and challenges, in: 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom), IEEE, 2018, pp. 1–7.
[5] Y. Lu, The blockchain: State-of-the-art and research challenges, J. Ind. Inform. Integr. 15 (2019) 80–90.
[6] T. McGhin, K.-K.R. Choo, C.Z. Liu, D. He, Blockchain in healthcare applications: Research challenges and opportunities, J. Netw. Comput. Appl. 135 (2019) 62–75.
[7] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A survey on the adoption of blockchain in IoT: Challenges and solutions, Blockchain Res. Appl. (2021) 100006.
[8] G.J. Katuwal, S. Pandey, M. Hennessey, B. Lamichhane, Applications of blockchain in healthcare: current landscape & challenges, 2018, arXiv preprint arXiv:1812.02776.
[9] K. Jaiswal, V. Anand, A survey on IoT-based healthcare system: Potential applications, issues, and challenges, in: Advances in Biomedical Engineering and Technology, Springer, 2020, pp. 459–471.
[10] L. Soltanisehat, R. Alizadeh, H. Hao, K.-K.R. Choo, Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review, IEEE Trans. Eng. Manage. (2020).
[11] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations, Neural Comput. Appl. (2021) 1–16.
[12] B. Houtan, A.S. Hafid, D. Makrakis, A survey on blockchain-based self-sovereign patient identity in healthcare, IEEE Access 8 (2020) 90478–90494.
[13] E.J. De Aguiar, B.S. Faiçal, B. Krishnamachari, J. Ueyama, A survey of blockchain-based strategies for healthcare, ACM Comput. Surv. 53 (2) (2020) 1–27.
[14] P.J. Taylor, T. Dargahi, A. Dehghantanha, R.M. Parizi, K.-K.R. Choo, A systematic literature review of blockchain cyber security, Digit. Commun. Netw. 6 (2) (2020) 147–156.
[15] A.Z. Ourad, B. Belgacem, K. Salah, Using blockchain for IOT access control and authentication management, in: International Conference on Internet of Things, Springer, 2018, pp. 150–164.
[16] H. Hasan, E. AlHadhrami, A. AlDhaheri, K. Salah, R. Jayaraman, Smart contract-based approach for efficient shipment management, Comput. Ind. Eng. 136 (2019) 149–159.
[17] T.A. Butt, R. Iqbal, K. Salah, M. Aloqaily, Y. Jararweh, Privacy management in social internet of vehicles: review, challenges and blockchain based solutions, IEEE Access 7 (2019) 79694–79713.
[18] R. Iqbal, T.A. Butt, M. Afzaal, K. Salah, Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions, Int. J. Distrib. Sens. Netw. 15 (1) (2019) 1550147719825820.
[19] M. Hölbl, M. Kompara, A. Kamišalić, L. Nemec Zlatolas, A systematic review of the use of blockchain in healthcare, Symmetry 10 (10) (2018) 470.
[20] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Bus. Inform. Syst. Eng. 59 (3) (2017) 183–187.
[21] J. Al-Jaroodi, N. Mohamed, Blockchain in industries: A survey, IEEE Access 7 (2019) 36500–36515.
[22] Z. Li, A.V. Barenji, G.Q. Huang, Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, Robot. Comput.-Integr. Manuf. 54 (2018) 133–144.
[23] B. Singhal, G. Dhameja, P.S. Panda, How blockchain works, in: Beginning Blockchain, Springer, 2018, pp. 31–148.
[24] L. Ismail, H. Materwala, S. Zeadally, Lightweight blockchain for healthcare, IEEE Access 7 (2019) 149935–149951.
[25] C. Pirtle, J. Ehrenfeld, Blockchain for healthcare: The next generation of medical records? 2018.

[26] G. Greenspan, Multichain private blockchain-white paper, 2015, URl: http://www.multichain.com/download/multichain-white-paper.pdf.
[27] A. Hasselgren, K. Kralevska, D. Gligoroski, S.A. Pedersen, A. Faxvaag, Blockchain in healthcare and health sciences—A scoping review, Int. J. Med. Inform. 134 (2020) 104040.
[28] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, 2017, pp. 557–564.
[29] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F.-Y. Wang, Blockchain-enabled smart contracts: architecture, applications, and future trends, IEEE Trans. Syst. Man Cybern. Syst. 49 (11) (2019) 2266–2277.
[30] A.A. Siyal, A.Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, G. Soursou, Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives, Cryptography 3 (1) (2019) 3.
[31] C. Sullivan, E. Burger, E-residency and blockchain, Comput. Law Secur. Rev. 33 (4) (2017) 470–481.
[32] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, J.B. Othman, Blockchain for managing heterogeneous internet of things: A perspective architecture, IEEE Netw. 34 (1) (2020) 16–23.
[33] F. Tian, An agri-food supply chain traceability system for China based on RFID & blockchain technology, in: 2016 13th International Conference on Service Systems and Service Management (ICSSSM), IEEE, 2016, pp. 1–6.
[34] D.D.F. Maesa, P. Mori, Blockchain 3.0 applications survey, J. Parallel Distrib. Comput. 138 (2020) 99–114.
[35] B.K. Mohanta, D. Jena, S.S. Panda, S. Sobhanayak, Blockchain technology: A survey on applications and security privacy challenges, Internet Things 8 (2019) 100107.
[36] R. Karim, L.S. Rumi, M.A. Islam, A.A. Kobita, T. Tabassum, M.S. Hossen, Digital signature authentication for a bank using asymmetric key cryptography algorithm and token based encryption, in: Evolutionary Computing and Mobile Sustainable Networks, Springer, 2021, pp. 853–859.
[37] P. Velmurugadass, S. Dhanasekaran, S.S. Anand, V. Vasudevan, Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm, Materials Today: Proceedings 37 (2021) 2653–2659.
[38] C. Oham, R.A. Michelin, R. Jurdak, S.S. Kanhere, S. Jha, B-FERL: Blockchain based framework for securing smart vehicles, Inf. Process. Manage. 58 (1) (2021) 102426.
[39] H. Huang, X. Sun, F. Xiao, P. Zhu, W. Wang, Blockchain-based ehealth system for auditable EHRs manipulation in cloud environments, J. Parallel Distrib. Comput. 148 (2021) 46–57.
[40] Y. Zhuang, L.R. Sheets, Y.-W. Chen, Z.-Y. Shae, J.J. Tsai, C.-R. Shyu, A patient-centric health information exchange framework using blockchain technology, IEEE J. Biomed. Health Inf. 24 (8) (2020) 2169–2176.
[41] D. National Cancer Institute, S. R. program. surveillance, epidemiology, and end results (SEER) program, 2020, Data (1975-2016).
[42] H. Guo, W. Li, E. Meamari, C.-C. Shen, M. Nejad, Attribute-based multi-signature and encryption for EHR management: A blockchain-based solution, in: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2020, pp. 1–5.
[43] M. Kim, S. Yu, J. Lee, Y. Park, Y. Park, Design of secure protocol for cloud-assisted electronic health record system using blockchain, Sensors 20 (10) (2020) 2913.
[44] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, Z. Chen, Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology, Plos One 15 (12) (2020) e0243043.
[45] L. Chen, W.-K. Lee, C.-C. Chang, K.-K.R. Choo, N. Zhang, Blockchain based searchable encryption for electronic health record sharing, Future Gener. Comput. Syst. 95 (2019) 420–429.
[46] Nursery data set, University of California, Irvine, 1997, http://archive.ics.uci.edu/ml/datasets/Nursery.
[47] F. Tang, S. Ma, Y. Xiang, C. Lin, An efficient authentication scheme for blockchain-based electronic health records, IEEE Access 7 (2019) 41678–41689.
[48] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, N. Kumar, Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications, IEEE Trans. Netw. Sci. Eng. (2019).
[49] F. Chollet, et al., Keras: The python deep learning library, Astrophys. Source Code Lib. (2018) ascl–1806.
[50] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, J.J. Rodrigues, BHEEM: A blockchain-based framework for securing electronic health records, in: 2018 IEEE Globecom Workshops (GC Wkshps), IEEE, 2018, pp. 1–6.
[51] K. Miyachi, T.K. Mackey, HOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design, Inf. Process. Manage. 58 (3) (2021) 102535.
[52] T. Hardin, D. Kotz, Amanuensis: Information provenance for health-data systems, Inf. Process. Manage. 58 (2) (2021) 102460.
[53] VeChain Foundation, VeChain Whitepaper 2.0, Tech. Rep., VeChain Foundation, 2019, https://www.vechain.org/whitepaper/#bit_65sv8.
[54] S. Venkatesan, S. Sahai, S.K. Shukla, J. Singh, Secure and decentralized management of health records, in: Applications of Blockchain in Healthcare, Springer, 2021, pp. 115–139.
[55] A. Khatoon, A blockchain-based smart contract system for healthcare management, Electronics 9 (1) (2020) 94.
[56] G. Albanese, J.-P. Calbimonte, M. Schumacher, D. Calvaresi, Dynamic consent management for clinical trials via private blockchain technology, J. Ambient Intell. Humaniz. Comput. (2020) 1–18.
[57] I.A. Omar, R. Jayaraman, K. Salah, M.C.E. Simsekler, I. Yaqoob, S. Ellahham, Ensuring protocol compliance and data transparency in clinical trials using blockchain smart contracts, BMC Med. Res. Methodol. 20 (1) (2020) 1–17.
[58] D.R. Wong, S. Bhattacharya, A.J. Butte, Prototype of running clinical trials in an untrustworthy environment using blockchain, Nature Commun. 10 (1) (2019) 1–8.
[59] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom, FHIRChain: applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.
[60] Hapi-fhir, 2021, http://fhirtest.uhn.ca/, Accessed: 2021–04-06.
[61] G. Saldamli, V. Reddy, K.S. Bojja, M.K. Gururaja, Y. Doddaveerappa, L. Tawalbeh, Health care insurance fraud detection using blockchain, in: 2020 Seventh International Conference on Software Defined Systems (SDS), IEEE, 2020, pp. 145–152.
[62] T.K. Mackey, K. Miyachi, D. Fung, S. Qian, J. Short, Combating health care fraud and abuse: Conceptualization and prototyping study of a blockchain antifraud framework, J. Med. Internet Res. 22 (9) (2020) e18623.
[63] T.-T. Kuo, H.-E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, J. Amer. Med. Inform. Assoc. 24 (6) (2017) 1211–1220.
[64] W. Liu, Q. Yu, Z. Li, Z. Li, Y. Su, J. Zhou, A blockchain-based system for anti-fraud of healthcare insurance, in: 2019 IEEE 5th International Conference on Computer and Communications (ICCC), IEEE, 2019, pp. 1264–1268.
[65] N. Saxena, I. Thomas, P. Gope, P. Burnap, N. Kumar, PharmaCrypt: Blockchain for critical pharmaceutical industry to counterfeit drugs, Computer 53 (7) (2020) 29–44.
[66] T. Clohessy, S. Clohessy, What's in the box? Combating counterfeit medications in pharmaceutical supply chains with blockchain vigilant information systems, in: Blockchain and Distributed Ledger Technology Use Cases, Springer, 2020, pp. 51–68.
[67] P. Pandey, R. Litoriya, Securing e-health networks from counterfeit medicine penetration using blockchain, Wirel. Pers. Commun. (2020) 1–19.
[68] R. Raj, N. Rai, S. Agarwal, Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership, in: TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 1572–1577.

[69] S. Bryatov, A. Borodinov, Blockchain technology in the pharmaceutical supply chain: Researching a business model based on Hyperledger Fabric, in: Proceedings of the International Conference on Information Technology and Nanotechnology (ITNT), Samara, Russia, 2019, pp. 21–24.
[70] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: A comprehensive review and directions for future research, Appl. Sci. 9 (9) (2019) 1736.
[71] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, W. Ni, PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities, Comput. Secur. 88 (2020) 101653.
[72] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Blockchain leveraged decentralized IoT ehealth framework, Internet Things 9 (2020) 100159, http://dx.doi.org/10.1016/j.iot.2020.100159, URL https://www.sciencedirect.com/science/article/pii/S2542660520300020.
[73] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Continuous patient monitoring with a patient centric agent: A block architecture, IEEE Access 6 (2018) 32700–32726, http://dx.doi.org/10.1109/ACCESS.2018.2846779.
[74] M.H. Nasir, J. Arshad, M.M. Khan, M. Fatima, K. Salah, R. Jayaraman, Scalable blockchains—A systematic review, Future Gener. Comput. Syst. (2021).
[75] A.A. Monrat, O. Schelén, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access 7 (2019) 117134–117151.
[76] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.
[77] Q. Feng, D. He, S. Zeadally, M.K. Khan, N. Kumar, A survey on privacy protection in blockchain system, J. Netw. Comput. Appl. 126 (2019) 45–58.
[78] J. Sedlmeir, H.U. Buhl, G. Fridgen, R. Keller, The energy consumption of blockchain technology: beyond myth, Bus. Inform. Syst. Eng. 62 (6) (2020) 599–608.
[79] J. Hu, M.J. Reed, M. Al-Naday, N. Thomos, Hybrid blockchain for IoT—Energy analysis and reward plan, Sensors 21 (1) (2021) 305.
[80] M. Madine, K. Salah, R. Jayaraman, Y. Al-Hammadi, J. Arshad, I. Yaqoob, AppXchain: Application-level interoperability for blockchain networks, IEEE Access 9 (2021) 87777–87791.
[81] S. Shi, D. He, L. Li, N. Kumar, M.K. Khan, K.-K.R. Choo, Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey, Comput. Secur. (2020) 101966.
[82] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, S. Ellahham, A blockchain-based approach for drug traceability in healthcare supply chain, IEEE Access 9 (2021) 9728–9743.
[83] H. Gamage, H. Weerasinghe, N. Dias, A survey on blockchain technology concepts, applications, and issues, SN Comput. Sci. 1 (2) (2020) 1–15.
[84] E. Politou, F. Casino, E. Alepis, C. Patsakis, Blockchain mutability: Challenges and proposed solutions, IEEE Trans. Emerg. Top. Comput. (2019).
[85] V. Davydov, Y. Yanovich, Optimal portfolio sold-out via blockchain tokenization, in: Proceedings of the 2020 2nd International Electronics Communication Conference, 2020, pp. 129–136.
[86] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2) (2019) 326.
[87] H.-T. Wu, C.-W. Tsai, Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing, IEEE Consumer Electron. Mag. 7 (4) (2018) 65–71.
[88] A.B. Haque, A.N. Islam, S. Hyrynsalmi, B. Naqvi, K. Smolander, GDPR compliant blockchains–a systematic literature review, IEEE Access (2021).
[89] A. Hasselgren, P.K. Wan, M. Horn, K. Kralevska, D. Gligoroski, A. Faxvaag, GDPR compliance for blockchain applications in healthcare, 2020, arXiv preprint arXiv:2009.12913.
[90] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, Springer, 2017, pp. 164–186.
[91] N. Bari, U. Qamar, A. Khalid, Efficient contact tracing for pandemics using blockchain, Inform. Med. Unlocked 26 (2021) 100742.
[92] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254–269.
[93] H.R. Hasan, K. Salah, Proof of delivery of digital assets using blockchain and smart contracts, IEEE Access 6 (2018) 65439–65448.
[94] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, K. Salah, A user authentication scheme of IoT devices using blockchain-enabled fog nodes, in: 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), IEEE, 2018, pp. 1–8.
[95] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.
[96] M. Al-Bassam, SCPKI: A smart contract-based PKI and identity system, in: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017, pp. 35–40.