ACCSCIENCE PUBLISHING

Artificial Intelligence in Health

REVIEW ARTICLE

Enhancing health-care security: The role of blockchain and consensus mechanisms

Asmaul Hosna[1], Nujhat Tabassum Rahman[1], Supriya Dewanjee[1], Zulfikar Alom[1], Elmustafa Sayed Ali[2,3]*, Mohammad Abdul Azim[1], and Rashid A. Saeed[4]

[1]Department of Computer Science, Asian University for Women, Chattogram, Bangladesh

[2]Department of Electrical and Electronic Engineering, Faculty of Engineering, Red Sea University, Port Sudan, Sudan

[3]Department of Electronics Engineering, Faculty of Engineering, Sudan University of Science and Technology, Khartoum, Sudan

[4]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia

Abstract

Blockchain technology has gained prominence recently by virtue of its strong security features for clinical data. Automation of blockchain transactions enables data transactions and records, providing decentralized, secure, and dependable access. Through intelligence-sharing agreements, it can also manage member relationships without the need for a middleman or other third party. Researchers in the health-care industry using blockchain algorithms to safeguard security of data, which is properly stored, are on the rise. In addition, this technology is patient adaptive. Patients and other health-care users can now trust the technology because it prevents any third party from accessing the medical data. Many platforms intended for use in the health-care domain are emerging, including Gem Health Network and MedRec. Using blockchain in health-care protects user data and grants them full authority over their data. However, blockchain technology is also confronting challenges and limitations regarding data privacy and storage capacity. This paper explores the implementation of blockchain within health-care sector while providing an overview of this technology and the different consensus algorithms used in blockchain technology.

Keywords: Blockchain; Health-care security; Electronic health records; COVID-19 pandemic; Genetic algorithm; Consensus mechanisms

***Corresponding author:**
Elmustafa Sayed Ali
(elmustafasayed@gmail.com)

Citation: Hosna A, Rahman NT, Dewanjee S, *et al*. Enhancing health-care security: The role of blockchain and consensus mechanisms. *Artif Intell Health.* 2024;1(2): 29-47. doi: 10.36922/aih.2580

Received: December 29, 2023

Accepted: February 26, 2024

Published Online: April 16, 2024

1. Introduction

Blockchain is an arrangement of a central node of control that connects distinct nodes. A peer-to-peer distribution database communication allows for safe data storage, verification, and transduction within the network. The growing utilization of blockchain technology has led to a compassionate project coordinated by the United Nations to help refugees who have lost their identity papers such as qualification documents and also to track pharmaceutical manufacturers that supply products in particular hospitals.[1] In the UK, health-care applications and validation were initialized to develop a digitized

health-care system through the help of government and policy. However, the health-care applications cannot securely share data through the application with data resources.[2] Personal health-care record (PHR) technology has been introduced to safeguard and store the patients' medical records, which the patients control.

The PHR secured some confidential governance. A previous study[2] has highlighted the harmful impact of poor record sharing on patient treatment, suggesting that the patients become part of the health-care platform that requires advanced tools and capabilities. Al Mamun *et al.*[3] asserted that patients should control their medical data through electronic medical records. Since electronic medical records consist of confidential and sensitive information, the robust security system should be transparent. Blockchain ensures safe transduction and transparent medical history records – an important attribute that helps build patients' trust. For instance, based on the medical records of HIV patients, cancer patients have to endure long-duration treatment.[4] The electronic medical record services with integrated blockchain technology make the process of data storing and securing incredibly easier by storing the results of laboratory test reports, post-treatment reports, *etc.*

The Commonwealth Health Alliance took the initiative to secure the patients' electronic health records (EHRs) efficiently. Medical and health-care services are becoming increasingly important in the present environment, and they must be supplied on time, securely, and safely.[5] Disease identification has become a crucial responsibility for medical practitioners. Many viral and cardiovascular disorders, including COVID-19 and diabetes, should be diagnosed in the early phase for optimal treatment. Given its rapid dissemination, detecting coronavirus has become a critical endeavor. However, deep learning holds significant value for detecting diseases by analyzing large volumes of image data, with blockchain allowing for decentralized and secure data access.[6]

Researchers are continuously struggling to improve disease detection models. To achieve this, hospitals, testing laboratories, research centers, and other organizations can share their data and work together to improve the learning model. As the security of personal information held in hospital databases is of paramount importance concern, every party needs to commit to protecting data privacy.[7] However, accurate and efficient learning models are still required for various applications. Due to ethical and regulatory concerns about medical data privacy, data sharing among organizations are limited.

Many applications have been deployed in the battle against the COVID-19 pandemic. For example, companies such as Apple and Google have developed contact tracing applications to track COVID-19 patients.[8] However, these applications are not decentralized, so patients' data can be easily accessed, resulting in a breach of data privacy. Data in a centralized system are prone to fraud, deletion, and modifications, undermining the data integrity of these systems. Blockchain technology can assist in lowering the impacts of the COVID-19 pandemic while providing high security and ensuring that a failed attack does not occur. This is due to the decentralized feature of blockchain, and all the data and records of transactions stored in blockchain are transparent to all the network members.[1,9] Therefore, data are more reliable and trustworthy.

To make data immutable, hashing or cryptographic algorithms are applied in the blockchain, linking one block to another.[10,11] Smart contracts are also used by blockchain technology to automate business processes and resolve health-care collaborators' disputes. Blockchain technology employing intelligent contracts can be applied to the logistic supply management of COVID-19 polymerase chain reaction testing kits.[12] This can help track supplies of these kits, recognize faulty or fake kits, monitor the condition of testing kits while shipping, and allow government officials to analyze the supply and demand of testing kits in specific locations. The paper will discuss the algorithms used for blockchain security and technology in health-care sector in the aspect of protecting medical records.[13] The main contributions of this paper are illustrated as follows:

(i) *Comprehensive overview:* To provide a summary of blockchain technology and discuss its various uses and implications for the health-care industry.
(ii) *Security concerns in health care:* To outline how blockchain technology resolves important security issues in the medical field and promote it as a dependable means of protecting clinical data.
(iii) *Blockchain security algorithms:* To provide a useful insight into the technical aspects of using blockchain technology to secure medical records by discussing the algorithms used for blockchain security.

The rest of this paper is organized as follows: Section 2 summarizes related works and motivations, and section 3 introduces the background of blockchain technology. The blockchain based on consensus algorithms in health-care sector is reviewed in section 4. Section 5 encapsulates a blockchain-based EHR system for Healthcare 4.0 Applications. The taxonomy of blockchain technology in health care is discussed in section 6. In section 7, the strength of blockchain technology in the health-care sector is reviewed. Section 8 discusses blockchain technology and applications in health care. The research gap and technical limitations of blockchain in health care, and the

relevant future directions, are given in sections 9 and 10, respectively. The paper is concluded in section 11.

2. Related works and motivations

Multiple studies on blockchain utilization in health-care sector have been conducted. One of the papers[14] narrates the history of blockchain development, with a focus on the technology of intelligent health-care management for assisting patients. Krishnamurthi and Shree[15] discussed several blockchain census algorithms and comparatively analyzed the algorithms. Another published study[16] presented a model to solve a confidentiality issue inherent in wearable medical devices used to monitor and care for patients, circumventing privacy intrusion and security concerns stemming from the transfer and recording of medical data. A new framework has been proposed for modified blockchain models for internet of things devices and other privacy and security features.

Yazdinejad *et al.*[17] proposed a new decentralized authentication of patients in a distributed hospital network, by leveraging the blockchain. This proposed model protects health-care networks for patients and allied health professionals. After the analysis, the results of the simulations showed that they demonstrated a high performance in ensuring confidentiality of the proposed structure among a distributed affiliated hospital network. Another study[18] expounded the different types of blockchain, such as public, private, and consortium blockchain, with elaborations on the uses of different algorithms in the health-care sector and the security purposes. Sharma *et al.*[21] proposed a framework for community interaction and developed a smartphone application to encrypt messages between researchers and research groups.

A survey conducted by Nguyen *et al.*[20] illustrated the contribution of blockchain and artificial intelligence (AI) in the health-care sector to combating COVID-19. Table 1 summarizes the most important features and contributions of the previous studies. These studies highlight the huge dependence of the next-generation health-care networks and applications on the use of the blockchain for security and user privacy.[22] Accordingly, this paper aims to comprehensively discuss the theoretical concept about the most critical blockchain issues related to the health-care sector, in addition to the impact of blockchain approaches and consensus algorithms in health-care application.

3. Blockchain technology

Blockchain is one of the most hyped disruptive innovations in recent years. It has garnered growing attention as a horizontal technology used in various sectors.[23] It is a distributed, immutable, open-source, public digital ledger distributed among network peers. It is a ledger made up of a chain of blocks. This ledger keeps a permanent record of all transactions and interactions among participants on the distributed and decentralized blockchain network. In addition, blockchain can be highly cost-effective in removing the requirement for a centralized authority to control and verify interactions and transactions between multiple users.[24] Every transaction in the blockchain is cryptographically signed and validated by all mining nodes, which keep a copy of the whole ledger made up of chained blocks of all transactions.[25] This provides unchangeable, secure, synchronized, and shareable time-stamped documents.

3.1. Types of blockchain

The three basic blockchain types are public permissionless, consortium public permission, and private blockchains.[26] They differ in terms of who has access to, writes to, and reads the data on the blockchain. Anyone can see the data in a public chain, and anyone can join and contribute to both consensus and make changes to the core software in principle. The public blockchain is commonly utilized in cryptocurrencies, and the two most popular cryptocurrencies, Bitcoin and Ethereum as the main chain, are public permissionless blockchains. Only a few specified groups of companies can monitor and participate in the consensus procedure on a consortium blockchain, which can be considered semi-centralized.[27] The private blockchain network is distributed yet often centralized. Only specific nodes can join the network, and a central authority frequently manages them.

3.2. How blockchain empowers secure data sharing in health-care system

The technologies blockchain with deep learning can improve health-care systems.[28] Utilization of blockchain technology in health-care domains helps secure data sharing and train deep learning models for diagnosing and predicting diseases. Other problems include data privacy concerns and compromised security in data flow between businesses. Therefore, the information was shared across the organization based on external and internal policies.[29] In addition, some fascinating research focuses on safe health-care data brain stimulation and biomedical and e-health data exchange for the central database built on the private blockchain by authorized users. In addition, to minimize risk, the remote patient monitoring system uses the Ethereum protocol.[30] Likewise, other authors recommended using encryption to store data from publicly accessible organizations. Several writers created a blockchain-based framework for sharing data on cloud

Table 1. Summary of related works on blockchain for securing medical data

Study	Blockchain in COVID-19 pandemic	Blockchain strength	Algorithms in health care	Taxonomy	Remarks
Mettler (2016)[14]	No	No	No	No	Describing the history of blockchain development from bitcoin and intelligent health-care management for patient guidance.
Krishnamurthi and Shree (2019)[15]	No	No	Yes	No	Presenting a comparative analysis of the algorithm, a brief overview of blockchain and challenges using algorithms.
Dwivedi *et al.* (2019)[16]	No	Yes	Yes	No	Demonstrating a blockchain-based IoT model for the security and privacy of any IoT-based remote monitoring system to protect business security.
Yazdinejad *et al.* (2020)[17]	No	No	Yes	No	Presenting a designed model for the safe data recording in a geographically diverse hospital network based on a blockchain-based approach.
Sharma *et al.* (2021)[18]	No	No	Yes	No	Proposing a cryptographic framework to create a blockchain-based secure community.
Saranya and Murugan *et al.* (2021)[19]	No	No	Yes	No	Explaining the blockchain types and uses of different algorithms in the health-care sector.
Nguyen *et al.* (2021)[20]	Yes	No	Yes	No	Combining blockchain and artificial intelligence for emergency health-care services used in the COVID-19 pandemic.

Abbreviation: IOT: Internet of things.

storage without the need for a third party.[31] Recent research has focused on real-time health-care systems' diagnosis and treatment of patient conditions.

4. Blockchain based on consensus algorithms in health-care sector

Several lists of algorithms are used in blockchain networks such as proof of work (POW), proof of stake (POS), practical byzantine fault tolerance (PBFT), recovery algorithm for fast tracking (RAFT), and delegated POS (DPOS). These algorithms are discussed in the following.

4.1. POW

POW technique required mining nodes for solving complex mathematical puzzles. After solving puzzles and node validation, the block is added to the blockchain network. The rest of the mining nodes approve the authenticity of the blocks.[32] When the miners confirm that the block is authorized, the block is attached to the blockchain by recompensing submitter mining nodes. There is lesser chance to get a false reward unless the attackers accommodate more than 50% of the mining nodes. The consensus processes-based POW provides data integrity, immutability, and reliability on the blockchain, improving the security of health-care applications.[33] Consensus techniques ensure that all participants have an accurate representation of the data by assisting in reaching an agreement on the current state of distributed database.

The POW algorithm is used in the health-care transaction. The work has traversed different consensus approaches in blockchain technology and is principally recommended for health care.[34] The sensors connect with intelligent devices and distribute the data for all possible events. Since automatic intelligent contracts are executed, the data are reliable. For instance, a sensor is connected to the human body so that the master device gathers data from the sensor to telecast it to the blockchain. Once medical data are stored on the blockchain, the POW technology guarantees that it is safe and unalterable. Since the POW is known to be decentralized. The network is more resistant to attacks because of its decentralization which offers fail-safe mechanism to protect itself against a single point of failure.[29,35] This can improve the system's overall security and dependability in the health-care industry by guarding against unauthorized access and guaranteeing the ongoing availability of vital patient data.

4.2. POS

With POS consensus mechanisms, miners are selected based on the quantity of cryptocurrency they own and are prepared to stake as collateral, thereby replacing the conventional POW mining method's intricate computational puzzle approach. In health-care applications, the medical chain is a systematic scheme of data sharing that can be executed for health-care systems using blockchain technology.[34] The incidence of attack against POS-based blockchain is lesser than that against POW-based blockchain. In POS, it is very difficult for an attacker to obtain the majority of

the blockchain supply. This protects patient data integrity and increases the resilience of PoS-based health-care blockchains against threats. For health-care applications based on blockchain, switching from complicated computational problems to POS results in lower energy consumption and enables randomized validator selection, node participation incentives, performance-based rewards, and continuous work to resolve distribution issues.[36] The security, effectiveness, and dependability of health-care blockchain applications are all improved by these contributions taken together.

Moreover, using the POS consensus mechanism in the context of an EHR system indicates that health-care applications built on blockchain technology are more secure and efficient in terms of making smart decisions. Real-time modifications to patient records can be made easier with POS, which has advantages including faster transactions and less energy usage. In addition, the tasks of verifying patient records are carried out by trusted health care providers who use health care networks to ensure reliability and efficiency.[37] POS is a good option for applications where timely access to patient data is crucial and environmental concerns are present since it combines the benefits of decentralization with a fast and streamlined consensus process, which enhances the system's overall security.

4.3. DPOS

DPOS is a decentralized model with high efficiency but low consumption. There is an option to vote for creating a panel with restricted trusted parties known as witnesses.[33,38] Some users act in the reputation system. It can create blocks and add them to the blockchain. The DPOS census is cost-efficient and time-saving. Since few nodes are eligible for DPOS to be centralized, the central node can easily monitor the election process. DPOS cannot maintain all the nodes effectively, undercutting the trustworthiness in security. Nowadays, the health-care domain is undergoing advancements through the incorporation of blockchain.[34,39] The implementation of the DPOS algorithm ensures the privacy of EHRs through secure transactions. With this technology, the patients maintain control of their EHRs. The patients may share their medical records with different institutions.

Blockchain technology can ensure the privacy and security of shared data. Once a doctor updates the EHR, it is encrypted by the SHA256 hashing algorithm, and then, it is stored in a different block.[35,40] The doctor receives a unique key from the patients through mail for accessing the medical data. The DPOS algorithm secures the patient data with a trustworthy guarantee and lowers the computational time and minimizes the entire cost of processing EHRs.

4.4. PBFT

PBFT can solve the byzantine problem, as presented in a published paper.[30] A byzantine fault is a defective algorithm. Byzantine fault tolerance can ensure the safety and efficiency of the system so that hardly [(n-1)/3 duplicate data are defective over the system in a lifetime. In medical science, PBFT algorithms create an efficient impact because several nodes are being shared and maintained by several nodes.[36,40] The fact that they hinder medical data from being disclosed or accessed by attackers significantly enhances the trustworthiness of PBFT.

4.5. RAFT

RAFT has five server nodes with three states, namely leader, follower, and candidate. Modified RAFT nodes work in a category accepting the same transitions. For instance, if a person is selected from a category assigned as a leader, he must accept clients' requests.[37,41] The leader must replicate the log to other servers and the data flow from the leader to the server. The leader's task is divided into three subtasks: leader election, leader log replication, and safety. A new leader is elected when the assigned leader fails to monitor the works. In log replication, the leader can guide and command the followers to execute changes made by the leader.[34,41] Finally, RAFT uses different commands for the same log index when the server changes the state of machine for safety concerns. Figure 1 shows the process of cluster algorithm of RAFT.

By comparing these five consensus algorithms, as shown in Figure 2, the POW algorithm stands outs as the most efficient for the health-care sector because it has a robust security system, which is the primary goal of initiating blockchain algorithms in health-care sectors. The summary of compared algorithms is shown in Table 2.

A previous study[29] provides a framework for implementing the algorithms discussed previously, where a number of computers with the same specifications were used to act as nodes for the blockchain.[38] By considering the typical framework with a computers of core I7, with the specifications of 16 GB memory size, and Window 10 operating system, the experimented POW, POS, DPOS, and PBFT algorithms with data size of 100 M/times can deliver performance depicted in Figure 3. An extended period of time is required to implement the proposed model in the system, as per empirical experiences, to compensate for the random delay between nodes.

The analysis also showed that the POW algorithm takes longer time compared to DPOS and POS algorithms. Furthermore, the PBFT consensus algorithm requires shorter time compared to other algorithms. The performance

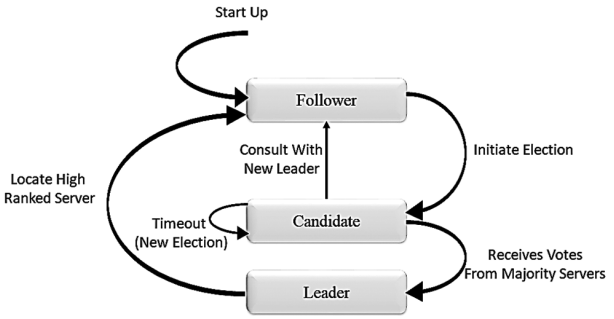

Figure 1. Recovery algorithm for fast tracking algorithm cluster diagram. Source: Schematic created by the authors.

of the PBFT algorithm is significantly different because the blockchain nodes are shared and maintained by multiple nodes, complicating the process of detecting medical data and protecting them from potential attackers.[29]

In general, the performance of these algorithms directly affects the utilization of medical data systems based on blockchain frameworks. However, depending on the kind of health-care application, the time delay during these algorithms processing will negatively impact the performance and utilization the blockchain-based health-care systems.

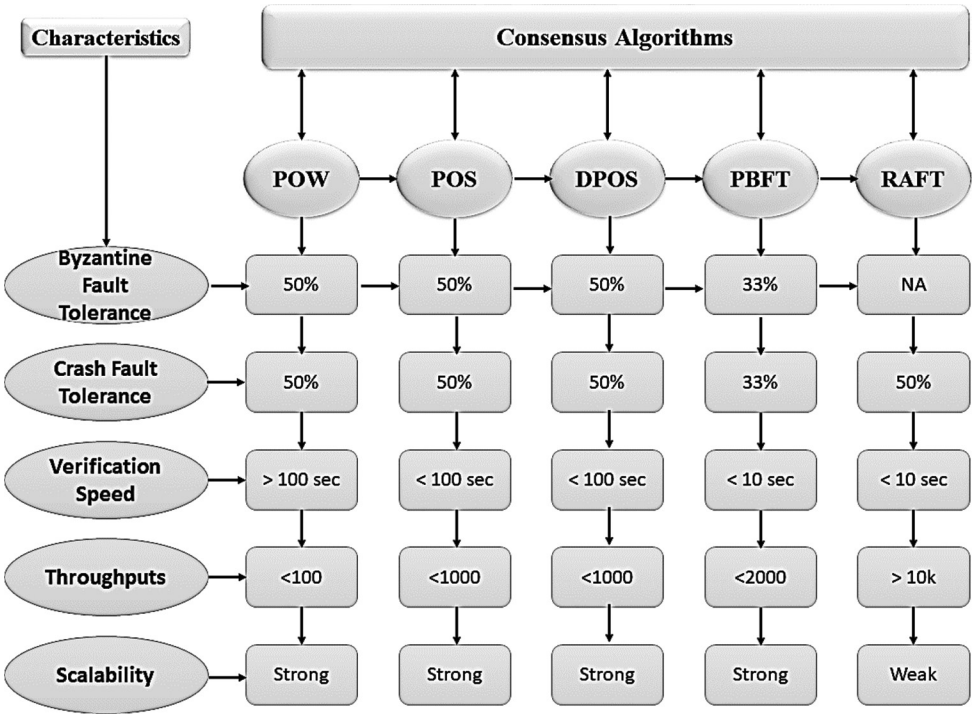

Figure 2. Performance analysis of consensus algorithms. Source: Schematic created by the authors.

Table 2. Comparative analysis of blockchain algorithm properties

Issues	Algorithms				
	POW	**POS**	**DPOS**	**PBFT**	**RAFT**
Developer	Markus Jakobsson		Developer	Markus Jakobsson	
Energy efficiency	Not enough	Limited	Limited	Yes	Efficient
Languages	C++, LLL	Michaleson	Improvised	Java	Haskell programming language
Advantages	Secure network, extensive and decentralized control over the network	Advantages	Secure network, extensive and decentralized control over the network	Advantages	Secure network, extensive and decentralized control over the network
Limitations	High consumption of electricity, not concordant with small networks			Limitations	High consumption of electricity, not concordant with small networks

Abbreviations: POW: Proof of work; POS: Proof of stake; PBFT: Practical byzantine fault tolerance; RAFT: Recovery algorithm for fast tracking; DPOS: Delegated proof of stake.

5. Blockchain-based EHR system for healthcare 4.0 applications

EHRs are medical records that can be managed and secured by a blockchain system supported by genetic algorithm and discrete wavelet transform.[32,41] The scope of a blockchain platform for industrial health care gives a new vision and future opportunities for Healthcare 4.0 Applications. The state-of-the-art focusing on the uses of blockchain with EHR in the health-care sector is summarized in Table 3.

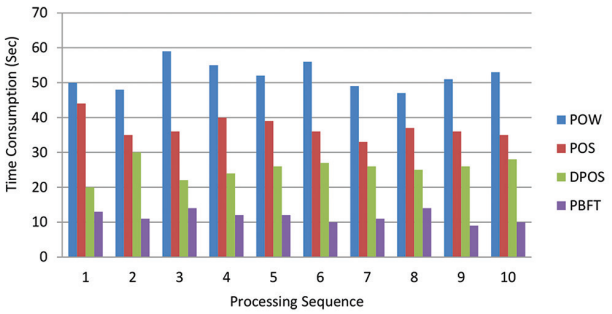

Figure 3. Consensus algorithm performance in blockchain framework. Source: Diagram created by the authors.

A study reported that EHRs of medical data consist of sensitive information and patients are permitted to share this information with health-care centers, doctors, and consultants.[15,41] EHRs are favorable for patients because they simplify the storage of laboratory reports and medicine lists and ease the appointments with attending doctors and the clinical consultations, especially for patients requiring treatment for diseases with an extended data history, such as cardiovascular disease, cancer, HIV, *etc.*[38,42] For patients who often visit different medical institutions, organizing and securing their medical history reports in the EHRs with the help of blockchain technology proves to be convenient for them. Through the data sharing features, medical research institute may collaborate with different health-care organizations under a regulated and secure data sharing environment.

Blockchain is known as a cryptographic protocol for conserving shared information records through a collection of computer networks where complete trust is not mandatory among the nodes. The implementation of blockchain in the health-care sector ensures data security for both patients and providers.[21,43] As a decentralized

Table 3. State of the art of blockchain use in health-care domain

References	Category	Components	Merits
Tanwar *et al.* (2020)[48]	Electronic health records	• Advantageous blockchain for health-care scenario • Securing and storing health-care clinical data • Data authentication for decentralized network	• A description of EHR work is presented • Transaction process in blockchain is explained • Blockchain in the health-care ecosystem is overviewed
Farouk *et al.* (2020)[24]	Electronic health records	• A brief description on the blockchain with EHR to share patients' information with the health-care centers and doctors	• Secure data sharing through excellent regulation
Hussein *et al.* (2018)[27]	Security and management of clinical records	• A brief description of blockchain networking system • Discrete wavelet transform for creating distinctive hash decrypted key • Genetic algorithm for enhancing data reliability	• Proposed method on managing and securing clinical data • Restriction on the access to the data using discrete wavelet transform algorithm • Enhancing data reliability using genetic algorithm
Wang *et al.* (2019) [46]	The SecNet	• Al-based algorithms to protect computing platforms • Smart contract algorithm i • Implementation of SecNet in medical data sharing	• Two aspects of SecNet are evaluated • Vulnerability of architecture and revenue for contributors is considered • An alternative storage model of the SecNet is proposed
Alqaralleh *et al.* (2021)[4]	Health-care diagnosis model	• An effective model for secure blockchain-enabled intelligent IoT • New health-care diagnosis model	• A data-gathering method is carried out to collect patient information using IoT devices • The GO-FFO (grasshopper with the fruit fly optimization) algorithm with elliptic curve cryptography is utilized for confidential image transmission for starters • NIS-BWT (neighborhood indexing sequence with burrow wheeler transform) approach is used to encrypt hash value • Deep belief network model is applied for diagnosing disease

Abbreviation: IOT: Internet of things.

system, the involvement of third parties is not allowed in blockchain. Thus, health-care service maintained by blockchain technology can only permit sharing of data contained within the blockchain architecture. The patients who use blockchain technology are facilitated with cost-efficient data distribution.[39,44] Moreover, the patients are privileged with an extensive network for secure health-care systems, medical data exchange through blockchain, health-care data protection, EHR facilities with attribute-based cryptosystem, and facilities for monitoring clinical emergencies. There are four stages of securing clinical data in the health-care industry:

(i) First step: At first, various health-care data, including patient's personal information and ID, are sent to the blockchain network through application programming interface (API). The current health IT system tracks and stores all the data.[43]
(ii) Second step: Blockchain technology has an internal transaction process through a smart contract. Entire transactions attached in the blockchain contain only patients' public ID rather than their personal information.
(iii) Third step: A permanent ledger is connected with the block. Thus, all sections become distinctly identifiable. The API processes queries from the health provider in a reverse manner. The database of blocks stores anonymous patient data, *e.g.*, gender, age, and illness.
(iv) Fourth step: The patient will have a private key. The health-care provider can only access the patient's information after the patient shares the private key. The data stand is restricted to people who do not have a private key.

Hussein *et al.*[27] proposed an extensive and prosperous system for handling the clinical record and information using blockchain technology. The method implements a different cryptographic technique for strong security management of sensitive clinical data and adaptability of the patients to simplified data access.[44] Discrete wavelet transform using hash function generation process was employed to boost the strength and restrict the access of data users. Moreover, genetic algorithms lower the time of transaction nodes to enhance data reliability and designate the data requests.

There are separate blocks in the blockchain network that is shaped by establishing chain events from the current block to the original block. After obtaining event details, the block broadcasts into a network.[45] Once the chain forms, the block is locked and cannot be reformed, updated, and deleted. Any exploitation of data handling policies by users in the group will prompt data tracking by data forensics team so as to secure and manage clinical records.

SecNet is an architecture proposed by Wang *et al.*,[46] combining actual big data with AI to enhance the robustness of cyber security. A large-scale Internet setting offers safe data storage, computation, and sharing. It primarily consists of three components. Blockchain-based data sharing with ownership guarantees allows trusted data exchange to create massive data in a large-scale context. In addition, AI-based safe computing systems come with more intelligent security rules, which aid in the creation of more trustworthy cyberspace. Moreover, they purchase security services through trust value exchange, a method for participants to receive financial rewards for sharing their data or service, promoting data sharing, and improving AI performance.[47] Furthermore, the authors describe a scenario of using conventional SecNet and its potentially alternative deployment method and evaluate its network security and economic revenue.

Alqaralleh *et al.*[4] developed a deep learning model for safe image transmission and diagnosis on the Internet of Medical Things environment. Data gathering, secure transactions, hash value encryption, and data classification are among the procedures included in the model.[49] The elliptic curve cryptography (ECC) is used primarily, and the hybridization of the grasshopper with the fruit fly optimization technique is used to generate the best ECC keys. The hash values are encrypted using the neighborhood indexing sequence (NIS) with burrow wheeler transform (BWT) (NIS-BWT). Finally, a deep belief network is used in the categorization process to diagnose the presence of disease. To identify the analysis of the optimal results of the proposed model, substantial experimental validation is performed, and the results are examined from many perspectives.

6. Taxonomy of blockchain technology in health care

Blockchain technology utilizes network technology with tamper-resistant data. In blockchain technology, current transactions cannot be changed. Instead, the transactions can be updated using hash values. The taxonomy of blockchain technologies in health care is illustrated in Figure 4. Different features make blockchain technology distinctive from others:

(i) *Distributed ledger:* In a distributed system, transactions are added to retrieve the system by removing failure points.
(ii) *Census mechanism:* If every verified user of the network grants a permission transaction, the transaction can be updated.
(iii) *Provenance:* The entire data history is obtainable on the blockchain network.

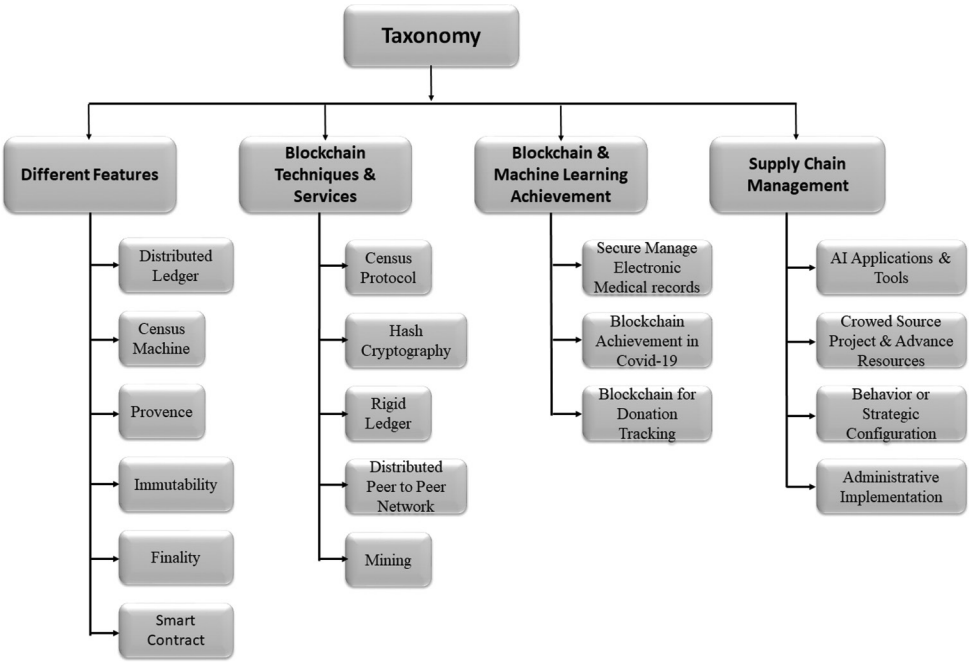

Figure 4. Taxonomy of blockchain. Source: Schematic made by the authors.

(iv) *Immutability:* Since all data are secure and trustworthy, not even a single record cannot be changed or redesigned.
(v) *Finality:* After completing the transaction, no one can change any data.
(vi) *Smart contract:* The codes are automatically executed within a specific time limit. The codes generated in the blockchain network and nodes are activated after executions. Consequently, blockchain hinders third parties from accessing the transaction, thus promising data security.[17]

6.1. Blockchain techniques and services

Blockchain incorporates various techniques and services such as Census Protocol, Hash Cryptography, Rigid Ledger, Distributed Peer-to-Peer Networking, and Mining, which are briefly explained in the following:[45,49]

(i) Census Protocol: There is a substantial restriction in allowing transactions. Through the Census Protocol, only specific users have access to the network assigned to grant permissions for transactions.
(ii) Hash Cryptography: The NSA has developed the SHA256 hash with 64 characters to add transactions used by blockchain. Hash algorithms have several uses, such as one-way cryptography, quick computation, avalanche effect, and inevitable combat impact.
(iii) Rigid Ledger: It is not possible to delete or modify because the blockchain network is stored and recorded.
(iv) Distributed peer-to-peer network: The data are updated and distributed through the network and distributed to different users.
(v) Mining: Miner helps attain the hash values in the network. The hash values can be easily computed for acquiring the award.

6.2. Blockchain and machine learning achievements

Blockchain has become a hot research topic since its inception. The concept of blockchain was first exemplified in digital currency, for example, Bitcoin in 2008. It has brought tremendous changes in health-care sector owing to its data obscurity, stability, and propagation features.

6.2.1. Safe management of electronic medical records

The accessibility and management of medical data in electronic medical records are not completely protected from any risks. The security and confidentiality of patients' confidential information, such as disease reports, medical history, and personal information, are not guaranteed. The solution to this hurdle is combining the interplanetary file system framework for electronic medical records in the health-care industry.[40,50] Inter Planetary file system (IPFS) allocates a peer-to-peer storage structure for reserving and accessing the encrypted huge volume of electronic medical records while needed. If any file needs to be deleted from version-control history, IPFS accumulates files with content address hash from a distributed hash table. IPFS uploads the hash value of the data as an alternative to keeping all

medical data. IPFS makes a distinctive content address for storing and retrieving the data.[3,50]

6.2.2. Blockchain achievements during COVID-19 pandemic

Blockchain ensures that all databases are synchronized, secure, and verified. Nowadays, researchers and health-care professionals leverage blockchain technology to curb the spread of COVID-19 pandemic and create alerts about future pandemics. There are several blockchain-based practices applied in realm of health care during the COVID-19 pandemic, including tracking of infectious disease outbreaks. By virtue of its ability in safeguarding data security, blockchain can also efficiently keep track of the public health data regarding infectious disease such as COVID-19.[41] Blockchain also assists with the accurate delivery of responses and helps with treatment decision-making soon after the early detection of symptoms so as to curb the spread of pandemic. Moreover, it guides health administration to keep track of the viral activity and suspected COVID-19 cases.[51]

6.2.3. Donation tracking

Blockchain technology can be applied to track donations. It notifies the donors of any exigencies requiring an urgent inflow of funds and, most importantly, the receipt of their monetary contributions.

6.3. Management of medical supply chains

With the help of blockchain technology, medical supply chains in different industries can be properly managed, through a series of procedures involving records collection, demands tracking, and product supply during the pandemic. It also keeps track of the usage of tools and instruments by doctors and patients in a bid to prevent the inadvertent use of contaminated items.[42,51] Proper guidelines governed by several AI sectors pertaining to data security have been introduced to fight against COVID-19 and any other pandemics in future. These categories are given in Table 4**,** which describes the AI technologies used in medical supply chain management.

7. Strength of blockchain technology in health-care sector

The intrinsic properties of blockchain technology are highly compatible with applications in the health-care sector. The strength of blockchain technology contributes to various applications in the health-care sector, as shown in Figure 5. There are clear parallels between blockchain technology and the essential requirements of the current health-care infrastructure.[41,52] Table 5 encapsulates some characteristics of blockchain technologies that can facilitate resolution of certain hurdles facing the current health IT environment.

8. Blockchain technology and applications in health-care sector

In 2016, the National Coordinator for Health Information Technology Office requested proposals on blockchain applications in health-care sector, with a focus on data validation, auditing, and authorization. Such a move is driven by the potential obstacles laid ahead of the incorporation of blockchain technology in health-care domain, such as privacy concerns, compliance with regulatory requirements, and technical issues with data storage and distribution, even though this technology enables storage of complete health-care records of an individual as a blockchain use case.[42,52] Blockchain technology offers numerous opportunities in health-care sector for the secure sharing and storage of patients' data and medical records, and coupled with consensus methods, provides effective schemes in solving security issues in the health-care industry in recent real-world applications. Leveraging medical chain is one prominent example of using blockchain technology to protect EHRs and give people control over their personal health information. The emphasis on decentralization is consistent with maintaining the confidentiality and integrity of patient records, even though the precise consensus procedure is not usually mentioned.[44,52]

Several security companies like Hashed Health in the USA are committed to using blockchain technology to

Table 4. Management of medical supply chain with the aid of AI technology

Issues	Sector 1	Sector 2	Sector 3	Sector 4
Description	Application of AI with AI tools	Crowd source project	Description	Application of AI with AI tools
AI contribution	Develop systems for drugs and vaccines against COVID-19; enhance diagnosis and improve public health	Ensure data security (pandemic situations)	AI contribution	Develop systems for drugs and vaccines against COVID-19; enhance diagnosis and improve public health
Implementation examples	Quick diagnosis of COVID-19 using medical images (Mexico, Singapore)	Cognitive impact of COVID-19 (USA); COVID-19 symptom study (UK)	IEEE declaration for ethical implementation of AI system	Implementation examples

Table 5. List of the characteristics of blockchain technology and their descriptions

Characteristics	Description
Decentralization	• Blockchain technology is a serialized data structure used to establish a decentralized ledger. • Decentralization allows parties to transact data in the health-care sector without involving a third party, reducing financial bias and fraud.
Trustlessness	Payments are made only when the balance is available on the blockchain, a feature that is essential to secure financial balances.
User-centricity	• The user-centricity attribute of blockchain technology ensures patients in control of their personal financial data. • Blockchain allows the patient to become the key mediator in distributing his or her medical data. • Patient or family member must expressly grant the provider access to the patient's medical record governed by the patient's private key signature for every new medical interaction. • Every access to patient's data is recorded in the immutable transaction history of the blockchain, providing a clear record of who has accessed and edited the patient's record.
Transparency	• Every transaction data in the blockchain is publicly viewable.
Immutability	• Blockchain is impervious to data manipulation. • The immutability of the blockchain ledger means that transactions cannot be changed or removed once they have been recorded. • Blockchains serve as a data timekeeping system, allowing easy data history reporting.
Speed	• Blockchain technology helps enhance the efficiency of verification for health-care sector transactions between financial institutions.
Cost	• Blockchain technology obviates the need to pay transaction fees by removing intermediaries from the health-care transaction.

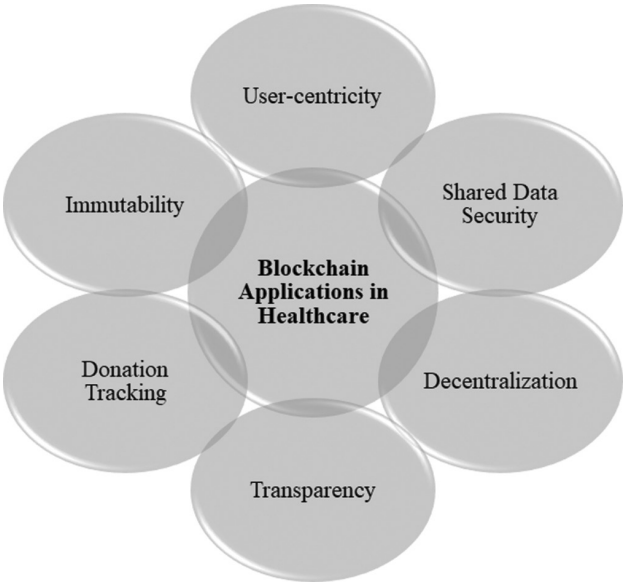

Figure 5. Summary of how blockchain technology is applied in health-care sector. Source: Schematic made by the authors.

expedite health-care transactions and minimize fraud, while enhancing operational security and efficiency. Keyless Signature Infrastructure (KSI) is utilized by other applications, including the ones developed by the Estonian E-Health Foundation, to assure the immutability of health records, prevent unauthorized adjustments, and improve overall security.[18,36] In addition, a different health-care facility uses blockchain technology to improve the security, traceability, and transparency of medical payments in an effort to lower fraud and errors in the system. According to these real-life examples, it is clear that blockchain technology can significantly add value to health-care applications.[18,44] There are other applications that have used blockchain technology in the field of health care, which are explained in the following subsections.

8.1. Blockchain for health-care management

Blockchain technology carves out a revolutionary niche in the health management sector due to the advances and benefits it brings to cloud storage of EHR data, privacy protection, *etc.*, as shown in Figure 6. With blockchain, we can improve data sharing, management, and storage. Data can then be easily shared with health-care providers. The steps of how blockchain could be used in health-care domain summarized by Khezr *et al.*[32] are given in the following:

(i) *Step 1:* While interacting with the doctors, the recent information about the patient are integrated into the medical records, serving as the primary data.
(ii) *Step 2:* EHR of the patient is shaped using the primary data collected.
(iii) *Step 3*: The control over and access to the contents embodied in EHR is granted to the EHR's owner only. Permission of the EHR's owner must be obtained for others to access EHR data.
(iv) *Steps 4, 5, and 6:* These three steps form the central part of database and cloud storage (for storing patient records) as well as data security conferred by the blockchain technology.
(v) *Step 7:* This is where health-care providers and other parties like the hospitals and care centers, collectively known as the end-users, who request access to patients' data. Records of patients' health data will be available wherever they are as they are stored and validated in the blockchain's distributed ledgers.

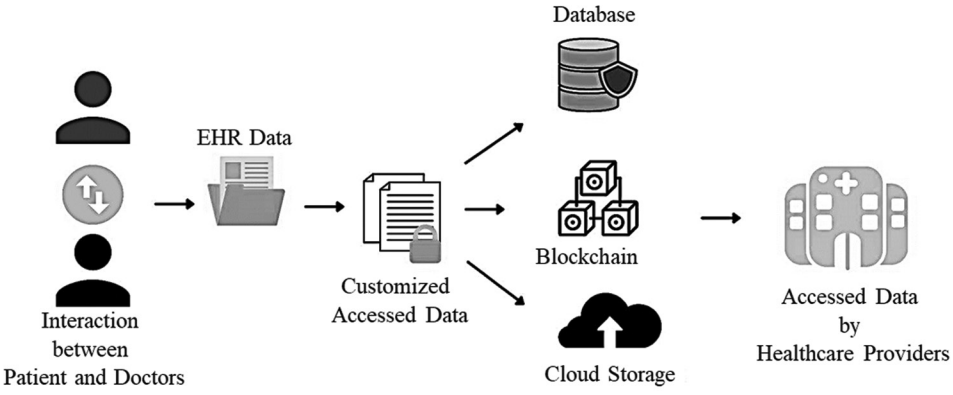

Figure 6. Health-care management using blockchain. Source: Schematic made by the authors.

8.2. Blockchain platforms used in health-care domain

Gem Health Network, Guard-time, Med-Rec, and Health-bank are some of the blockchain platforms developed for use in health-care domain. These platforms enable secure sharing of medical information with different health-care providers.

8.2.1. Gem health network

Gem Health Network is a blockchain platform developed based on the Ethereum Blockchain Framework that can allow the sharing of medical data supplied by health-care specialists. Gem Health Network merges businesses, specialists, and patients to enhance patient-centered care. This network allows medical stakeholders to have transparent access to any latest information.[44] On this platform, outdated information can be removed, thereby reducing the risk of medical negligence starting from the early stage of treatment. Medical experts can also track all the interactions between patients and their doctors.

8.2.2. Guard-time

Guard-time, a blockchain-powered data security platform based in the Netherlands, is used in Estonia to operate public health infrastructure, especially in patient identity validation. Estonian citizens are given smartcard that link their EHR data with their corresponding blockchain-based profiles. Citizens of Estonia, health-care providers, and insurance companies can acquire information about medical treatments done in Estonia through Guard-time. Updates made to the EHR are assigned with a hash and registered in the blockchain network. Thus, patients' records are immutable and are protected from malicious modifications.[45] Along with that, health-care database information, such as time and date of appointments, are also signed cryptographically in a block.

8.2.3. Med-rec

Med-Rec, built from a collaborative project between MIT Media Lab and Beth Israel Deaconess Medical Center, is a blockchain-based platform deals particularly with EHRs.[46] The non-seamless design of EHRs in managing multi-institutional and lifelong records is the prime reason for data loss as patients' data may become scattered as they move from one organization to another.[13] Med-Rec can provide its users with all of their records, which are credible, easily accessible, and most importantly, immutable. It also allows management permissions, authorization, and data sharing among health-care providers and systems using a decentralized approach.

Blockchain in the Med-Rec platform grants patients the power to authorize individuals who can access their health records. This project is tested as a proof of concept with medication data. Med-Rec was further enhanced in terms of data types as well as number of data contributors and users.[47]

8.2.4. Health-bank

Blockchain can also be applied in the area of patient-generated data. Built by a Switzerland-based digital health startup, Health-bank stands as a great example of this application. Users can store and manage their personal health-care information secured on the Health-bank platform. All the users have full control over their own data.[49] User data in Health-bank are also made available for medical research. In addition, users will be financially compensated for share their data. Blockchain implemented in health-bank allows for tracking personal patient-generated health data, which researchers can use, by means of timestamp. Users who have contributed to medical research can also be identified using blockchain.

8.3. Benefits of using blockchain technology in fighting COVID-19 pandemic

Blockchain technology offers distributed, encrypted, and secure digital transaction loggings. Blockchain technology can be employed to track the spread of coronavirus infections by tracking citizens on a global scale while maintaining patients' personal information, tracking drug trials, and tracking and maintaining records of fundraising activities and donations.[44,48] There were cases of blockchain technology used to curb the COVID-19 pandemic. Specifically, the distributed blockchain ledger technology was utilized in logging and data visualization of the coronavirus outbreaks with data derived from the Centers for Disease Control and Prevention (CDC) and the World Health Organziation.[50]

Public health blockchain consortium is another blockchain-based platform that could pinpoint communities and workplaces that have yet to be affected by coronavirus outbreaks and other pathogens before corresponding protective measures are imposed on them in a bid to prevent further spread of infectious diseases. This technology can also verify and track uninfected individuals and restrict their movements if they have visited areas affected by outbreaks.[45,51] Another example is Hyper-chain, a blockchain-based platform used in China, which facilitates donation tracking and flags the needs of COVID-19 patients to the health-care organizations and the government.

8.4. Blockchain in combating COVID-19 pandemic

Blockchain is an essential tool in the fight against COVID-19. The indispensability of the blockchain technology can be accounted for by its ability in tracking and tracing personal protective equipment (PPE).[52] During the pandemic, most countries were facing a shortage of PPEs, which are essential to prevent and control the COVID-19 infection, due to the lack of reliable and correct data about their demand and supply. A lack of transparency in the logistic supply chain management was also contributing to the prevalence of low-quality PPEs on the market. The utilization of blockchain technology can help facilitate the supply chain operations, secure PPE certificates, prevent compliance violations, and identify faulty PPEs,[18] creating an healthy atmosphere in which committers of compliance violations will be penalized, and reliable and trustworthy manufacturers will be recognized for their high-quality products.

Transactions or COVID-19 data can be recorded and made available to health-care organizations. These records of transactions will be rendered immutable, preventing alterations by any entities. Blockchain can also help with enhancing the reliability of COVID-19 analytics, reducing the incidence of fatal consequences such as COVID-19 misdiagnosis attributed to incorrect data.[43]

8.5. Blockchain for ensuring patient data privacy

Consensus procedures combined with blockchain technology offer a strong framework for protecting patient data privacy in health-care domain, resolving a number of issues commonly seen with conventional centralized methods. Ensuring the stability of patient data records by making them tamper-resistant and immutable is one of the most crucial steps in applying blockchain technology. This capability of blockchain permits the generation of an accurate and visible record of activity that documents all data transactions in the past[53] Thus, by improving data integrity and security, any unauthorized attempts to access or alter patient information can be promptly identified. Consensus techniques, which are addressed in section 4, are essential for verifying the authenticity of data supplied to the blockchain and for confirming transactions. These measures reduce the possibility of fraudulent activity and unauthorized changes to patient records by demanding network consensus. The network's trust is built through the consensus process, which improves the overall patient data security.

Blockchain networks leverage strong cryptographic algorithms to secure patient data in terms of data encryption. An extra layer of security is added by encryption, which guarantees that even in the event of illegal access, the data cannot be read without the right decryption keys. The privacy and confidentiality of patients are greatly improved by this function. By automating permissions and access controls, smart contracts self-executing algorithms with pre-established rules help protect patient privacy.[54] Patients may decide the usage and accessibility of their data through these contracts, which can be configured to manage and enforce detailed authorization procedures. Data handling in compliance with patient preferences and legal requirements is guaranteed by this automated method, which also lowers the possibility of human error.

Consensus mechanisms and blockchain technology together offer consistency, decentralization, robust encryption, access controls based on smart contracts, transparency, and improved consent management, all of which contribute to protecting patient data privacy in the health-care industry.[55] By addressing the ever-evolving issues of data security and privacy in the health-care industry, this all-encompassing strategy builds a foundation of confidence and dependability in the handling of sensitive patient data.

9. Research gap and technical limitations of blockchain in health-care sector

Blockchain technology has a positive impact on the health-care sector by facilitating the businesses of the health-care organizations. Moreover, this technology has a unique edge in securing and upgrading patient's data, in a cost-effective fashion. One of the census mechanisms, the POW, required plenty of energy to operate.[56] Due to the restriction in accessing sensitive information from the stored data, the public ledger system can be disrupted.[45] Despite its significant role in securing medical data, blockchain is fraught with limitations and challenges in technology, integration, cost, regulation, culture, energy consumption, and data privacy.

9.1. Limitations

A flood of software are currently employed in the health-care sector, but the functionalities of some of them have not fully matured and equivalent but enhanced software is constantly being created and added to this growing armada. In the aspect of integration, the blockchain technology to be applied must be compatible with the present financial technologies before their full integration.[57] Furthermore, institutions will be incurred higher initial costs due to the implementation of new technology. On a separate note, regulatory concerns surrounding blockchain technology have yet to be resolved by government agencies. One of the prominent concerns is that distributed access to the whole data set can be compromised even if the data have been encrypted and de-identified within the blockchain.[48]

The two main issues about blockchain data storage are confidentiality and scalability. Individuals who are linked on the same chain can access the data. As a result, data in the blockchain, which might contain sensitive information such as medical history and X-ray report, are vulnerable to breaches and not desirable in a decentralized platform. Storage capacity in blockchain will be highly impacted by the data breach vulnerability.[48,57] The summary of challenges facing blockchain and the guidelines to tackle each of them is shown in Table 6.

9.2. Open research issues

Several vital issues confronting the adoption of blockchain for medical applications require investigations tailored to solving security problems prevalent in the EHR systems. These open issues are iterated in four research questions:

(i) How to build servers for blockchain-based health-care systems that are amenable to blockchain protocol scalability.
(ii) How to determine the levels of authority in blockchain and safeguard the access to patient data without triggering system failure that could greatly affect access to EHR information.
(iii) How to design massive, blockchain-based globalized storage systems for large volumes of confidential health records without compromising the efficiency of the blockchain network.
(iv) When and how to integrate an approved and specialized standards formulated by global standardization institutions into blockchain-based health-care systems and into the mechanism responsible for data exchange in blockchain services.

Most recent studies present the concept of the use of blockchain in health-care domain, underscoring the important role of blockchain in transforming the health-care sector. However, one of the most important research problems surrounding the application of blockchain in health-care systems is the interoperability between different health systems following the adoption and integration of blockchain to improve security of data sharing, especially in the case of wearable devices. To investigate this aspect, Roehrs *et al.*[58] evaluated the productivity of the blockchain performance when implementing a prototype that integrates and performs medical records from different production databases.[59]

The measurement of response time, central processing unit usage, memory and disk occupation, and network usage were monitored. Figure 7 depicts the performance of blockchain in EHRs to query data and manipulate health records in a scenario containing data blocks running from 50 to 500 concurrent sessions in the network,[60] showing that there is an increase in the number of users who simultaneously access the network, measured in terms of the average load of records and the average response rate obtained.[61] These results indicate that the response time is almost equivalent despite the multiplicity and abundance of data, underlining the potential of merging open EHR standards and blockchain technologies to create an interoperable model for health data sharing with the aim of reducing the impact of various interoperability constraints.

10. Future directions

Several aspects concerning the future adoption of blockchain technology in the health-care sector should be taken into consideration:

10.1. Enhanced performance of blockchain

Platforms using blockchain technology should be technically enhanced in terms of scalability, resource consumption, network latency, throughput, *etc.* Increasing scalability and building more lightweight blockchain designs for health-care purposes are needed to make

Table 6. Challenges facing blockchain and guidelines to tackle them

Challenges	Causes	Guidelines
Security and privacy of data	• Blockchain technology is still in its early stages of development and refinement. • There is much ambiguity when it comes to designing the blockchain. • When old corporate systems and record systems are involved, integration issues arise.	• The type of data shared with and among participants must be determined since the beginning. • Prediction models that protect data privacy should be used. • It is necessary to choose a blockchain protocol – the framework that guides the structure of the blockchain and the development of applications – and use the appropriate authorization structures.
Managing storage capacity	• Storage capacity for a large amount of data is limited. • Limitations in throughput capacity and storage exist.	• A scalable and resilient blockchain solution is required. • Data storage requirements should be kept to a minimum.
Interoperability issues	• Creating blockchains from a variety of communication services is a challenge. • It is technically challenging to afford an effective interaction platform for users and for the operations of medical applications. • Gaps in communication and information sharing are obstacles.	• Evaluability should be maintained while reducing integration complicatedness. • The ease of integration should be taken into consideration with security concerns.
Decisions about blockchain governance	• Records' ownership • How is permission granted?	• New cybersecurity risks must be addressed before patients entrust a public blockchain with storing their data. • The blockchain's nodes, users, peers, and/or validators will need to be defined.
Standardization challenges	• Lack of uniformity and scalability • Lack of successful blockchain-based projects for reference	• International standardization authorities are required to formulate well-authenticated and approved standards. • The standards will be treated as guidelines for inspecting the exchanged data and as safety precautions.
Social challenges	• Concerns about blockchain adoption due to cultural and trust issues • Knowledge gap • Hesitant social adoption of technology	• Organizations are encouraged to adopt technology and join a shared network.
Inadequate universally defined standards	• No defined standards • Time- and effort-consuming implementation of standards in the health-care sector	• Universal standards will help blockchain become more adaptable. • Data format, size, and type in blockchain will be readily determined.

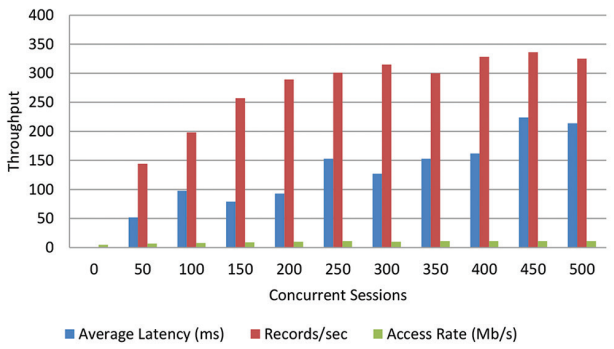

Figure 7. Interoperability performance of electronic health record systems powered by blockchain technology. Source: Graph made by the authors.

data verification and transmission of ultralow-latency information more optimized.[48,57]

10.2. Blockchain security issues

Despite the huge potential, security issues of blockchain technology that could undermine its adoption remain to be resolved. For instance, blockchain is still vulnerable to a compromise of mutual trust, by a degree of 51%, even though such a trust system is built upon with consensus mechanisms.[59] Data hackers can capitalize on this vulnerability to hijack the whole system developed with blockchain. For blockchains operating on POW mechanisms in particular, an attack with a probability of 51% may occur if one miner's hashing power is more than 50% of the hashing power in total. If a user's private key is lost, their entire blockchain will be vulnerable to tampering by other people. Since blockchain is decentralized and does not rely on third-party institutions for its operations,[54,62] it would be tough to track the whereabouts of a stolen private key and to retrieve back the stolen private key if it has been changed by the criminals. Therefore, solutions should be created to counteract the attacks and enhance blockchain security.

10.3. Reduction of resource consumption

Given the profound resource-consuming nature of POW consensus algorithm used in blockchain, a more efficient mechanism is urgently warranted. A prevailing idea of

improving the existing mechanism is to develop a hybrid mechanism system of POW and POS. Further research and experiments on creating better consensus mechanisms will significantly contribute to the development of blockchain systems.[63]

10.4. Data validation and cleanup

Not all data stored in the blockchain is verified, thereby prompting smart contracts to delete some codes, although the contract address will not be removed. Furthermore, smart contracts either have the same codes or no codes at all.[59,64] In addition, most smart contracts are not published after their execution. Therefore, data cleaning and disclosure strategies must be put in place to enhance the efficiency of blockchain systems.

10.5. Future regulations

In the context of applying blockchain technology in health-care domain while safeguarding data security, more efforts should be invested in navigating and resolving the issues in the ever-changing regulatory framework. Blockchain technologies that are adherent to the current laws and regulations, including Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) requirements, should be explored.[60] To ensure compliance of these innovations with jurisdiction-specific legislations, considerations should also be given to the legal recognition and enforcement of smart contracts in health-care agreements.[65]

11. Conclusion

The integration of blockchain technology will continue to promote multifaceted advancements in the health-care industry. By comparing the algorithms utilized in blockchain technology, we found that the POW algorithm outperforms the rest. At present, several blockchain-driven platforms are already in use to store patients' medical records. These data can then be shared with medical professionals for patient-centered care and overall improvement of treatments. Patients can store their data and have full authority over who can access their data. However, there are still many flaws and challenges inherent in this technology that needs to be addressed.

Acknowledgments

None.

Funding

None.

Conflict of interest

The authors declare that they have no conflicts of interest.

Author contributions

Conceptualization: Asmaul Hosna, Nujhat Tabassum Rahman, Supriya Dewanjee

Writing – original draft: Asmaul Hosna, Nujhat Tabassum Rahman, Supriya Dewanjee, Zulfikar Alom

Writing – review & editing: Elmustafa Sayed Ali, Mohammad Abdul Azim, Rashid A. Saeed

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Availability of data

Data are available from the corresponding author upon reasonable request.

References

1. Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M. Blockchain and COVID-19 pandemic: Applications and challenges. *Cluster Comput*. 2023;26:2383-2408.

   doi: 10.1007/s10586-023-04009-7

2. Ratwani R. Electronic health records and improved patient care: Opportunities for applied psychology. *Curr Dir Psychol Sci*. 2017;26(4):359-365.

   doi: 10.1177/0963721417700691

3. Al Mamun A, Jahangir MUF, Azam S, Kaiser MS, Karim A. A Combined Framework of Interplanetary File System and Blockchain to Securely Manage Electronic Medical Records. In: *Proceedings of International Conference on Trends in Computational and Cognitive Engineering*; 2021.

   doi: 10.1007/978-981-33-4673-4_40

4. Alqaralleh BA, Vaiyapuri T, Parvathy VS, Gupta D, Khanna A, Shankar K. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. *Pers Ubiquitous Comput*. 2024;28:17-27.

   doi: 10.1007/s00779-021-01543-2

5. Attaran M. Blockchain technology in healthcare: Challenges and opportunities. *Int J Healthc Manage*. 2022;15(1):70-83.

   doi: 10.1080/20479700.2020.1843887

6. Abernethy A, Adams L, Barrett M, *et al*. The promise of digital health: Then, now, and the future. *NAM Perspect*. 2022;6(22):1-24.

   doi: 10.31478/202206e

7. Brunese L, Mercaldo F, Reginelli A, Santone A. A blockchain based proposal for protecting healthcare systems through formal methods. *Procedia Comput Sci*. 2019;159:1787-1794.

doi: 10.1016/j.procs.2019.09.350

8. Brunese L, Mercaldo F, Reginelli A, Santone A. Lung Cancer Detection and Characterisation through Genomic and Radiomic Biomarkers. In: *2020 International Joint Conference on Neural Networks* (*IJCNN*); 2020.

   doi: 10.1109/IJCNN48605.2020.9206797

9. Ozair FF, Jamshed N, Sharma A, Aggarwal P. Ethical issues in electronic health records: A general overview. *Perspect Clin Res*. 2015;6:73-76.

   doi: 10.4103/2229-3485.153997

10. Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain Cities Soc*. 2018;39:283-297.

    doi: 10.1016/j.scs.2018.02.014

11. Sheth H, Dattani J. Overview of blockchain technology. *Asian J Converg Technol.* 2019;5(1):1-3.

12. Dubovitskaya A, Novotny P, Thiebes S, *et al*. Intelligent health care data management using blockchain: Current limitation and future research agenda. In: *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*. Berlin: Springer; 2019.

    doi: 10.1007/978-3-030-33752-0_20

13. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain. In: *AMIA Annual Symposium Proceedings*. Vol. 2017. Bethesda: American Medical Informatics Association; 2017:650-659.

14. Mettler M. Blockchain Technology in Healthcare: The Revolution Starts Here. In: *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services* (*Healthcom*); 2016:1-3.

    doi: 10.1109/HealthCom.2016.7749510

15. Krishnamurthi R, Shree T. A brief analysis of blockchain algorithms and its challenges. In: Information Resources Management Association, editor. *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government*. Hershey, PA: IGI Global; 2021:23-39.

    doi: 10.4018/978-1-7998-5351-0.ch002

16. Dwivedi AD, Srivastava G, Dhar S, Singh R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* (*Basel*). 2019;19(2):326.

    doi: 10.3390/s19020326

17. Yazdinejad A, Srivastava G, Parizi RM, Dehghantanha A, Choo KKR, Aledhari M. Decentralized authentication of distributed patients in hospital networks using blockchain. *IEEE J Biomed Health Inform*. 2020;24(8):2146-2156.

    doi: 10.1109/JBHI.2020.2969648

18. Sharma R, Wazid M, Gope P. A blockchain based secure communication framework for community interaction. *J Inf Secur Appl*. 2021;58:102790.

    doi: 10.1016/j.jisa.2021.102790

19. Saranya R, Murugan A. A systematic review of enabling blockchain in healthcare system: Analysis, current status, challenges and future direction. *Mater Today Proc*. 2023;80:3010-3015.

    doi: 10.1016/j.matpr.2021.07.105

20. Nguyen DC, Ding M, Pathirana PN, Seneviratne A. Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey. *IEEE Access*. 2021;9:95730-95753.

    doi: 10.1109/ACCESS.2021.3093633

21. Sharma A, Bahl S, Bagha AK, Javaid M, Shukla DK, Haleem A. Blockchain technology and its applications to combat COVID-19 pandemic. *Res Biomed Eng*. 2020;38:173-180.

    doi: 10.1007/s42600-020-00106-3

22. Ekblaw A, Azaria A, Halamka JD, Lippman A. A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data. In: *Proceedings of IEEE Open and Big Data Conference*; 2016.

23. Ezzine I, Benhlima L. Technology against COVID-19 A Blockchain-based Framework for Data Quality. In: *6th IEEE Congress on Information Science and Technology* (*CiSt*); 2020:84-89.

    doi: 10.1109/CiSt49399.2021.9357200

24. Farouk A, Alahmadi A, Ghose S, Mashatan A. Blockchain platform for industrial healthcare: Vision and future opportunities. *Comput Commun*. 2020;154:223-235.

    doi: 10.1016/j.comcom.2020.02.058

25. Gourisetti SNG, Mylrea M, Patangia H. Evaluation and demonstration of blockchain applicability framework. *IEEE Trans Eng Manag*. 2019;67(4):1142-1156.

    doi: 10.1109/TEM.2019.2928280

26. Gupta R, Kumari A, Tanwar S. Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. *Trans Emerg Telecomm Technol*. 2021;32(1):1-20.

    doi: 10.1002/ett.4176

27. Hussein AF, ArunKumar N, Ramirez-Gonzalez G, Abdulhay E, Tavares JMR, de Albuquerque VHC. A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. *Cogn Syst Res*. 2018;52:1-11.

    doi: 10.1016/j.cogsys.2018.05.004

28. Ivan D. Moving toward a blockchain-based method for the secure storage of patient records. In: *ONC/NIST Use*

of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

29. Jayaram R, Prabakaran S. Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. *Egypt Inform J*. 2021;22:401-410.

doi: 10.1016/j.eij.2020.12.003

30. Jia Q. Research on medical system based on blockchain technology. *Medicine* (*Baltimore*). 2021;100(16):e25625.

doi: 10.1097/MD.0000000000025625

31. Khan FA, Asif M, Ahmad A, Alharbi M, Aljuaid H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustain Cities Soc*. 2020;55:102018.

doi: 10.1016/j.scs.2020.102018

32. Khezr S, Moniruzzaman M, Yassine A, Benlamri R. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Appl Sci*. 2019;9(9):1736.

doi: 10.3390/app9091736

33. Kim D, Doh I, Chae K. Improved Raft Algorithm Exploiting Federated Learning for Private Blockchain Performance Enhancement. In: *2021 International Conference on Information Networking* (*ICOIN*); 2021:828-832.

doi: 10.1109/ICOIN50884.2021.9333932

34. Kumar A, Kumar Sharma D, Nayyar A, Singh S, Yoon B. Lightweight proof of game (LPoG): A proof of work (pow)'s extended lightweight consensus algorithm for wearable kidneys. *Sensors* (*Basel*). 2020;20(10):2868.

doi: 10.3390/s20102868

35. Kumar R, Wang W, Kumar J, *et al*. An integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals. *Comput Med Imaging Graph*. 2021;87:101812.

doi: 10.1016/j.compmedimag.2020.101812

36. Leeming G, Cunningham J, Ainsworth J. A ledger of me: Personalizing healthcare using blockchain technology. *Front Med* (*Lausanne*). 2019;6:171.

doi: 10.3389/fmed.2019.00171

37. Lemieux VL. Blockchain recordkeeping: A swot analysis. *Inf Manag*. 2017;51(6):20-27.

38. Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. *Future Gener Comput Syst*. 2020;107:841-853.

doi: 10.1016/j.future.2017.08.020

39. Liu H, Crespo RG, Martínez OS. Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. *Healthcare* (*Basel*). 2020;8:243.

doi: 10.3390/healthcare8030243

40. Liu W, Li Y, Wang X, Peng Y, She W, Tian Z. A donation tracing blockchain model using improved DPoS consensus algorithm. *Peer-to-Peer Netw Appl*. 2021;14:2789-2800.

doi: 10.1007/s12083-021-01102-9

41. Lo SK, Xu X, Chiam YK, Lu Q. Evaluating Suitability of Applying Blockchain. In: *2017 22nd International Conference on Engineering of Complex Computer Systems* (*ICECCS*); 2017:158-161.

doi: 10.1109/ICECCS.2017.26

42. Mackey TK, Kuo TT, Gummadi B, *et al*. 'Fit-for-purpose? Challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Med*. 2019;17(1):68.

doi: 10.1186/s12916-019-1296-7

43. Nakagawa T, Hayashibara N. Energy efficient raft consensus algorithm. In *International Conference on Network-Based Information Systems*. Cham: Springer; 2017:719-727.

doi: 10.1007/978-3-319-65521-5_64

44. Shen M, Zhu L, Xu K. *Blockchain: Empowering Secure Data Sharing*. Singapore: Springer; 2020.

doi: 10.1007/978-981-15-5939-6

45. Quiané-Ruiz JA, Pinkel C, Schad J, Dittrich J. RAFTing MapReduce: Fast Recovery on the RAFT. In: *2011 IEEE 27th International Conference on Data Engineering*; 2011:589-600.

doi: 10.1109/ICDE.2011.5767877

46. Rahmadika S, Rhee KH. Blockchain technology for providing an architecture model of decentralized personal health information. *Int J Eng Bus Manage*. 2018;10:1-12.

doi: 10.1177/1847979018790589

47. Wang K, Dong J, Wang Y, Yin H. Securing data with blockchain and AI. *IEEE Access*. 2019;7:77981-77989.

doi: 10.1109/ACCESS.2019.2921555

48. Rajput DS, Sharma S, Tiwari SK, Upadhyay A, Mishra A. Medical data security using blockchain and machine learning in cloud computing. In: *Mathematical Modeling and Soft Computing in Epidemiology*. Boca Raton: CRC Press; 2020:347-374.

doi: 10.1201/9781003038399-18

49. Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J Inf Secur Appl*. 2020;50:102407.

doi: 10.1016/j.jisa.2019.102407

50. Rupa C, Midhunchakkaravarthy D. Preserve Security to Medical Evidences Using Blockchain Technology. In: *2020 4th International Conference on Intelligent Computing and Control Systems* (*ICICCS*). Madurai, India: IEEE;

2020:438-443.

doi: 10.1109/ICICCS48265.2020.9120948

51. Ahir S, Telavane D, Thomas R. The Impact of Artificial Intelligence, Blockchain, Big Data and Evolving Technologies in Coronavirus Disease-2019 (COVID-19) Curtailment. In: *2020 International Conference on Smart Electronics and Communication* (*ICOSEC*). Trichy, India: IEEE; 2020:113-120.

doi: 10.1109/ICOSEC49089.2020.9215294

52. Salah K, Rehman MHU, Nizamuddin N, Al-Fuqaha A. Blockchain for AI: Review and open research challenges. *IEEE Access*. 2019;7:10127-10149.

doi: 10.1109/ACCESS.2018.2890507

53. Sethy PK, Behera SK, Ratha PK, Biswas P. Detection of coronavirus Disease (COVID-19) based on Deep Features and Support Vector Machine. *Int J Math, Eng, Manag Sci*. 2020;5(4):643-651

doi: 10.33889/ijmems.2020.5.4.052

54. Reegu FA, Abas H, Gulzar Y, *et al*. Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*. 2023;15(8):6337.

doi: 10.3390/su15086337

55. Chinnasamy P, Albakri A, Khan M, Raja AA, Kiran A, Babu JC. Smart contract-enabled secure sharing of health data for a mobile cloud-based e-health system. *Appl Sci*. 2023;13(6):3970.

doi: 10.3390/app13063970

56. Singh M, Singh A, Kim S. Blockchain: A Game Changer for Securing IoT Data. In *2018 IEEE 4th World Forum on Internet of Things* (*WF-IoT*). Singapore: IEEE; 2018:51-55.

doi: 10.1109/WF-IoT.2018.8355182

57. Singh SK, Rathore S, Park JH. BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gener Comput Syst*. 2020;110:721-743.

doi: 10.1016/j.future.2019.09.002

58. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*. 2019;3(1):3.

doi: 10.3390/cryptography3010003

59. Roehrs A, da Costa CA, da Rosa Righi R, da Silva VF, Goldim JR, Schmidt DC. Analyzing the performance of a blockchain-based personal health record implementation. *J Biomed Inform*. 2019;92:103140.

doi: 10.1016/j.jbi.2019.103140

60. Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. In: *Advances in Computers*. Vol. 111. Amsterdam: Elsevier; 2018:1-41.

doi: 10.1016/bs.adcom.2018.03.006

61. Zhang R, Xue R, Liu L. Security and privacy on blockchain. *ACM Comput Surv*. 2019;52(3):1-34.

doi: 10.1145/3316481

62. Chinnasamy P, Vinothini C, Arun Kumar S, Allwyn Sundarraj A, Annlin Jeba SV, Praveena V. Blockchain technology in smart-cities. In: Panda SK, Jena AK, Swain SK, Satapathy SC, editors. *Blockchain Technology: Applications and Challenges*. *Intelligent Systems Reference Library*. Vol. 203. Cham: Springer; 2021:179-200.

doi: 10.1007/978-3-030-69395-4_11

63. Zubaydi HD, Chong YW, Ko K, Hanshi SM, Karuppayah S. A review on the role of blockchain technology in the healthcare domain. *Electronics*. 2019;8(6):679.

doi: 10.3390/electronics8060679

64. Zamri N, Mohamad Z, Nik WN, Mohamad AHZ. Smart secure telerehabilitation apps for personalized autism home intervention using blockchain system. In: *Blockchain for 5G-Enabled IoT*. Cham: Springer; 2021:377-398.

doi: 10.1007/978-3-030-67490-8_15

65. Wang F. *Building High-performance Distributed Systems with Synchronized Clocks*. PhD Thesis. Stanford University; 2019.