JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 01, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

BLOCKCHAIN-BASED PATIENT HEALTH DATA MANAGEMENT AND SMART CONTRACT ACCESSING

Sandeep Kaur[1], Gurpreet Singh[2], Amandeep Kaur[3], Hardeep Singh[4], Satveer Kaur[5]

[1,2,3,4,5] *Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, India*

Email: [1]sandeepkaurcse@gmail.com, [2]gurpreetsinghgndu@gmail.com, [3]aman.cheema.2k12gmail.com, [4]hardeep.cet@gndu.ac.in, [5]satveer.dcet@gndu.ac.in

1. Introduction

Blockchain technology has recently gained popularity in many fields, including the healthcare industry.Blockchain technology provides a secure, and distributed database that does not require the intervention of an administrator or central authority. Additionally, blockchain technology has generated interest as a means of enhancing the transparency and authenticity of healthcare data [1].Patients are considered the primary entities and centers of a blockchain-based healthcare ecosystem. It can make significant improvements in terms of security, reliability, and interoperability of health data. This means that blockchain technology offers the potential to transform the healthcare industry. Thus, blockchain suggests a convenient, reliable, and protected model for the conversation of electronic health records (EHRs) and electronic medical records (EMRs) between patients and their healthcare providers. Most of the current limitations of the healthcare system are resolved by allowing them to centralize and improve their effectiveness and safety by using blockchain.The fundamentals of blockchain have been described here along with current and future blockchain applications in the healthcare industry [2].

1.1. Blockchain

Blockchain is an incorruptible record of transactions contained in a distributed ledger that ensures dispersed and secure transactions. Each transaction is grouped into a block which is then connected to the chain. The term blockchain technology refers to a synthesis of three techniquesthat are already in existence: distributed ledgers, consensus protocols, and cryptography [3]. Blockchain is a widely dispersed, peer-to-peer system that is used to create an uninterrupted record that is being added to an ever-growing database known as blocks which are then combined to form a digital ledger. Afterward, the network automatically validates each transaction which is represented as a cryptographically signed block on the network's server. It is important to note that these technological solutions are not new, but how they are implemented makes blockchain a modern technology[4].

1.1.1. Different Blockchain Models

Blockchain can be divided into a few distinct groups which have their characteristics, and directly reflect the network behavior. Figure 1 depicts the types of blockchain can be classified asgiven below [5].

Submitted: 08/03/2022 **Accepted**: 30/03/2022

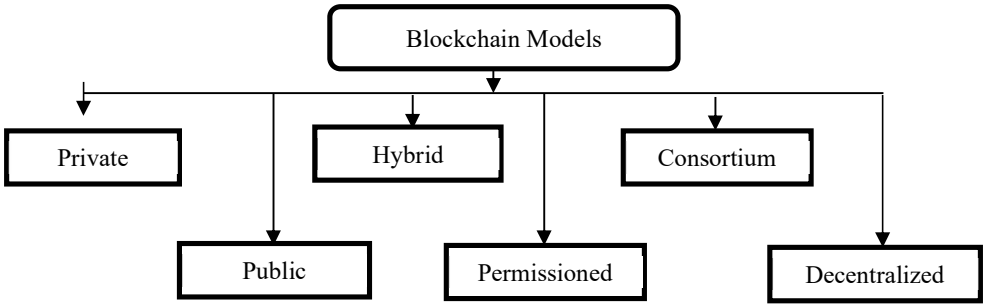

Figure 1: Blockchain models.

- **Private Blockchain**

A private blockchain is a type of distributed ledger that works as a private and safe place to store information and it is based on cryptographic principles to function as such.

- **Public Blockchain**

A public blockchain makes it possible for anyone to take part. It is in fact, a distributed ledger platform that is non-restrictive and does not require any permission.

- **Hybrid Blockchain**

A hybrid blockchain combines the features of a private blockchain with those of a public blockchain allowing users to create networks with or without public consent.

- **Permissioned Blockchain**

The permissioned model is useful for financial institutions, businesses, and organizations that are confident in their ability to comply with the majority of the restrictions while also being concerned about keeping an eye on the records at all times.

- **Consortium Blockchain**

Multiple companies share control of the blockchain network in a consortium blockchain which is based on a semi-decentralized model.

- **Decentralized Blockchain**

Decentralized applications (DApps) are software applications or systems that are independent of any single authority or influence.

1.2. Security and Privacy Issues in Healthcare System

A large amount of information is generated, accessed, and disseminated on an ongoing basis in the healthcare industry which is considered a data-intensive clinical domain. Storing and disseminating such a massive amount of data is critical but extremely difficult due to the data sensitivity and constraints such as confidentiality and protection. A broad range of software, hardware, and networking technologies have contributed to the century-long

advancement of health - care data management. All of which seek to enhance disease tracing and identification, medical treatment, the quality of drugs and medical care, and the creation of worldwide chronic disease impediment plans. The use of big data in healthcare has raised new questions about patients' privacy and security [6].

1.3. Blockchain technology in health care

The healthcare challenges in many countries are growing rapidly but access to primary doctors or practitioners is becoming more difficult for patients. A closer look at the word blockchain reveals that this technology is not only noteworthy but also incredibly useful in the era of the Internet. Blockchain technology has a diverse variety of applications and uses in the healthcare industry. Patient medical records are transferred securely using ledger technology, which also manages the drug supply chain and aids healthcare researchers in their efforts to decode the genetic code.Health care institutions might use blockchain technology to keep medical records securely and confidentially, updating patient data across different facilities and locations in real-time and with security [7].

1.3.1. A generalized workflow of blockchain

Blockchain is a peer-to-peer network as well as a public database that functions without the use of a central server. A public database contains information about each exchange between users that takes place on the network [8].

A blockchain can be thought of as a distributed ledger or decentralized database that keeps track of all electronic transactions and exchanges that have taken place between the users (patients).A blockchain contains irrefutable and verifiable records of every transaction ever made. A transaction can be carried out in a decentralized manner by employing blockchain technology[9].A person who is a member of the network is responsible for verifying each new transaction that is made. A blockchain becomes increasingly irreversible as each transaction in a block is validated by all of the nodes connected to the network [10]. Figure 1 given below depicts the blockchain process flow [11]:

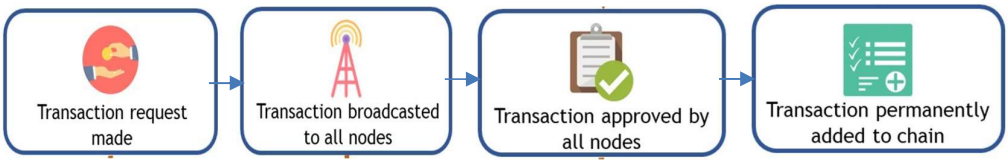

Figure 1: A general workflow of blockchain [11].

Blockchain eliminates the need for a central database server that acts as an intermediary between the peers in a distributed network. The server is the only cause that can lead to the failure of the entire network. The whole network would be down if the server goes down. The server's network bandwidth consumption must also be high to accommodate high network traffic volumes. Furthermore, the use of a centralized approach with a server raises security issues as the server includes all the sensitive data about the participants in the network [11].

1.4. Applications of blockchain in healthcare

Applications of blockchain in the healthcare system are discussed below:

- The original purpose of blockchain technology (BCT) was to be used in the fields such as cryptocurrencies and economics and but now it is growing in many other areas such as the biomedical field [12].
- Blockchain technology has a lot of potential in the medical field by stabilizing and protecting the data set that users can interact with one another [12].
- It is used in telemedicine, genomics, electronichealthrecord, telemonitoring, neuroscience, and personalized health applications [13].
- Blockchain technology is a viable choice for personal electronic health record (EHR) management [14].
- Blockchain is also used for Personal Health Record (PHR) Data Management [14].

2. Literature Review

A brief review of already done work in the field of the blockchain-based healthcare system is discussed below:

Dash, et al., (2022) [15]explained blockchain as an emerging technology with a decentralized electronic cash system. Barnes and Noble (BN) Publishing, and distributed technology used by third trusted parties (TTP) to secure, and resolve cyberattacks. The scope of PalCom middleware was evaluated to enable graphical user interface(GUI) development and to maintain massive data values by employing blockchain. The PalCom directives made use of a limited version of the commands/parameters to reach patients online. It intended to provide a compiled version of the blockchain's functionality to maintain safe and secure digital relationships through the use of authentication and private key cryptography. Health care record integrity and patient privacy were at risk due to data fragmentation and smart contract security. The authentication algorithm and Hyperledger were utilized to secure the patient data. Research demonstrated the advantage and outcomes of using cryptography algorithms in conjunction with strict adherence to data regulations and industry standards to provide solutions for data-intensive domains such as the healthcare system.

Balaji, et al., (2021) [16]suggested that knowing one's health status was a crucial task for any human being. However, it was difficult to find a person's health problems at different times. Security was very important in the above case because it has a person's private information in it. Blockchain technology played an important role in protecting the system and preventing data from being leaked. Blockchain was used to keep data safe and keep it from being changed. There was a lot of information about hospitals, like prescriptions, bills, medical records, claims, and so on. The Ethereum blockchain was used to gain access to the entire database. Patients had to be monitored regularly and the data had to be saved for later

access. As a result, the goal was to have highly secured electronic health record maintenance (EHRM).

Cáceres, et al., (2021) [17]suggested that health information systems were spread out and connected to other data sources and systems. Sufficient security measures were required to ensure the authenticity of data thereby escaping unnecessary damage to patients due to the use of erroneous, corrupt, or altered data. Decentralization, record modification and integrity issues, and quick and effective verification operations were evaded in these systems to ensure that human lives were not put in jeopardy by security mechanisms. Blockchain technology was used to create a decentralized registry system for healthcare environments. Register provided the same level of protection as transaction registers in distributed databases, but because it was a decentralized system, allowed for load balancing thereby facilitated fast and efficient operations, and included blockchain technology to preserve the integrity of the validation register.

Gu, et al., (2021) [18]studied that cryptocurrencies had gained financial and public attention since the invention of blockchain technology. Consequently, a lot of research had been performed on the time series forecasting of cryptocurrency. Nevertheless, the majority of these findings focused on forecasting the costs of different cryptocurrencies with little emphasis placed on predicting the number of transactions. Cryptocurrency exchangesserved as trading platforms for cryptocurrencies which were important players in the cryptocurrency market. The transaction data was collected from 15 different Ethereum exchange addresses, which was a public blockchain platform with open-source smart contracts.functionality at the time. Experiments based on deep learning have been used to make predictions about transaction value by modeling the problem as one of time series forecasting. Deep learning was more accurate at forecasting transaction values than traditional methods, according to experimental results.

Pooranam, et al., (2021) [19]explained that in today's world, keeping track of one's health was a necessary part of one's daily routine to live a prosperous life. Automation was used to keep the process running smoothly and to make it more interesting. Blockchain served as a safe and secure system for transactional data. Some techniques were followed to make the process of documenting each patient's test results a little more efficient and updated. The suggested technique aided in the reduction of duplications and the avoidance of confusion in the course of the process. In general, the blockchain technique increased the security of different transactions which resulted in a reduction in the number of duplicates. Smart contracts enabled documents to be shared in a decentralized manner through the use of a decentralized system. However, each process might be efficient in terms of clinical outcomes to achieve better results. Implemented blockchain techniques and algorithms that deal with an intelligent system and an analysis would be performed on a specific dataset that would be focused primarily on the healthcare system, as described above.

Vijayalakshmi, et al., (2021) [20]studied that it was extremely difficult for a healthcare organization to keep up with increasing challenges and costs while still providing high-

quality care. Clinical decision support systems (CDSS) were an essential tool for improving the treatment process and advancing healthcare services. Doctors could work together more effectively to enhance patient care using aCDSS. Collaborative treatment services shared the patient's medical records with a variety of healthcare professionals. An electronic health records system was used to store all of the patients' health information. Sharing electronic health records was a very difficult task because it contained sensitive and confidential information about the patient, which made it difficult to do. Patients, doctors, radiologists, hospitals, and insurance companies had also expressed concerns about confidentiality and trust in collaborative treatment. Health care providers could take advantage of distributed ledger technology (DLT), also known as the blockchain, because of its secure architecture framework. As a way to assist healthcare providers in addressing the most pressing problems and obstacles, blockchain and artificial intelligence hold great promise. The healthcare industry could benefit from the combination of artificial intelligence and blockchain.

Shuaib, et al., (2021) [21] evaluated that a user's identity must be secure and reliable to accurately identify them and provide services. Traditional centralized identity systems suffered from several security flaws and did not allow for user control. User control and security have been provided by the use of the self-sovereign identity (SSI) technique. The ability of a healthcare information system to protect privacy and security for its users was critical.SSI solutions could also be used to protect patient information from security and privacy menaces in the healthcare industry. Advantages and requirements were examined using a blockchain-based SSI solution in healthcare.

Zarour, et al., (2020) [22] explained that when sharing private medical information with electronic healthcare record (EHR) systems, security and accessibility were very important factors to think about. Opinions of 56 people who worked in the field of healthcare management, were taken to evaluate different blockchain models. The fuzzy analytic analytical network process (F-ANP) technique was applied to figure out the weights of the criteria and the Fuzzy-Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method was used to figure out how different solutions would affect the criteria. Furthermore, the results of the study would be very important when it comes to choosing the best Blockchain model for keeping EHRs safe from breaches.

2.1. Comparative Analysis of literature review

Table 2 below contains the comparative analysis of the literature review:

Table-2: Comparative analysis of literature review

Author	Technique Used	Outcomes
Dash, et al., (2022) [15]	PalCom middleware	Findings demonstrated the advantage and efficiency of the cryptography algorithm, as well as

		the compliance with data regulations and standards.
Balaji, et al., (2021) [16]	Ethereum blockchain	Maintaining electronic health records with a high level of security.
Cáceres, et al., (2021) [17]	Decentralized registry system	Provided Blockchain mechanisms for ensuring the validation register's integrity.
Gu, et al., (2021) [18]	Ethereum blockchain	Deep learning is more effective at predicting transaction value than conventional techniques.
Pooranam, et al., (2021) [19]	Decentralized system	Improved the security among different transactions, which reduced duplications also.
Vijayalakshmi, et al., (2021) [20]	Distributed ledger using artificial intelligence	Helped the healthcare traders to tackle major healthcare issues and challenges.
Shuaib, et al., (2021) [21]	Self-sovereign identity (SSI)	Provided solutions to counter patient information privacy and security threats.
Zarour, et al., (2020) [22]	Fuzzy-Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)	Provided appropriate Blockchain model for maintaining breach-free EHRs.

3. Background Study

Wireless transmission and mobile computing have reached an advanced stage due to the rapid advancement of technology. These two technologies can be merged to enable medical data sharing on social media, but this requires secure data sharing betwixt pervasive social network (PSN) nodes. Earlier studies have shown that the majority of human sensors are incapable of supporting extremely high levels of calculation, as a result, the sensor node's computation must be reduced to a minimum. A hacker can steal shared data from a third party by intercepting a legitimate node resulting in security issues. A blockchain-based system for preserving medical records is formed by combining an authentication protocol for medical sensor areas with a data transfer protocol, considering the above security and performance considerations.The former protocol makes it possible for mobile devices to securely transfer data from human sensors to them using elliptic curve point multiplication. The latter protocol is used to store data that has been gathered and transferred by mobile phones and tablets. It has been demonstrated that the

methodsare secure against a variety of possible attacks and that it decreases the number of communication rounds lower than that of previous methods. Blockchain technology is used to store data in the social network information transfer protocol so that the owner of the data can permit the entry of pertinent clients. As a result, the new approach not only enhances computing efficiency but also enhances security [23].

4. Problem Formulation

Blockchain technology has gained popularity as a result of its ability to improve the security, trustworthiness, and robustness of distributed systemsamong other benefits. Several fields, including finance, remote sensing, data analysis, and healthcare have benefited from research based on blockchain technology in recent years. It is necessary but also extremely difficult to store and disseminate large amounts of patient data because of the sensitive nature of the data and the limitations imposed by issues like security and privacy. Conventional cloud-based and client-server healthcare data management systems are troubled by concerns such as data privacy, single point of failure, system vulnerability, and other things. The Ethereum blockchain technology is used to ensure the confidentiality, security, and availability of EHR data, as well as the control on a finer scale of who has access to it. The overall objective of implementing blockchain technology in healthcare is to enhance healthcare practices and consequently, patient outcomes. Blockchain is beneficial in a variety of waysincluding lowering transaction expenses, streamlining procedures, reducing administrative burdens, and eliminating the need for intermediaries. In this way, patients could share their medical records without fear of being compromised with doctors, hospitals, and research organizations.

5. Research Methodology

This section contains the architecture of research methodology for patient health data management by Ethereum based blockchain technique. In this methodology the patient dataset is taken based on the medical records. Then this dataset is clustered in the form of time span. An Ethereum based blockchain is used to stored and encrypt the data. Blockchain technology is designed, which can have all the conditions from managing different permission to accessing the data as shown in Figure 2.

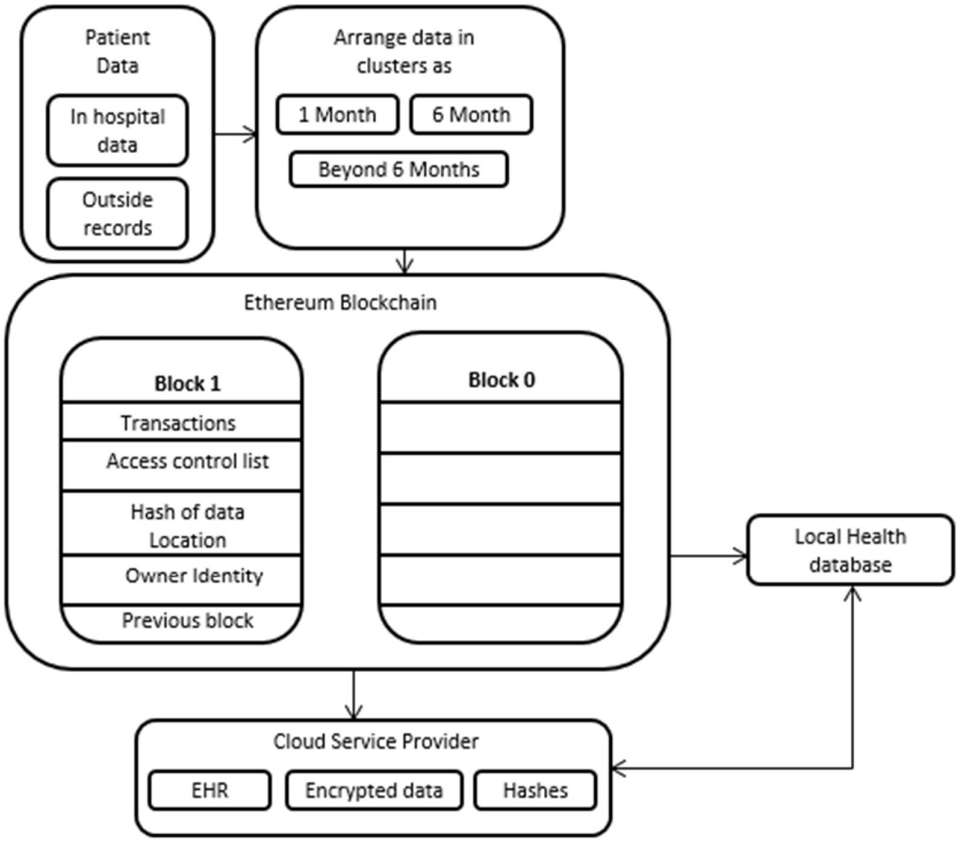

Figure 2: Architecture of research methodology.

5.1. Technique Used

The Ethereum blockchain technique has been used to design and implement a medical workflow that includes accessing and managing a large volume of medical data.

5.1.1. Ethereum Blockchain

The Ethereum blockchain is a safe place to store any type of confidential data, including that of patients. Ethereum is a specific blockchain-based software platform that makes it possible to store and securely protect data. Ethereum represents a blockchain that has a built-in programming language that can be used throughout the whole development process. Everyone may establish their own rules for ownership, transaction formats, and state transition functions since it is implemented as an abstract layer that everyone can access [16].

In the context of research methodology design framework has been discussed step by step as given below.

Step-1: Collection of Patient Data

In this step, patient data is collected by two resources for further processing. Data collected from the patients are divided into two categories: Firstly, data is taken from hospital itself and considered as secondary data. Next data can also be gathered directly from patients and this data is considered primary data.

Step-2: Data Arrangement

After collecting the data either from the hospital or directly from patients is arranged in the form of clusters according to the time. Clustering is the process of grouping the population of data points to make it easier to compare data points in the same group with those from different groups. Data is arranged as a one-month cluster, six-month cluster, or beyond six months clusters.

Step-3: Security provided by Ethereum Blockchain

This section contains the explanation of security provided to healthcare data by the Ethereum blockchain:

Ethereum is a decentralized open-source network that has a thriving community and is undoubtedly one of the biggest public blockchain networks. Ethereum is sometimes referred to as the world computer because it allows distributed applications (such as smart contracts) to run in a distributed manner. Ethereum blockchain contains a chain of the block as block1, block0, and so on. Each block's primary function is to record, verify, and distribute transactions to other blocks. Each block contains transactions of patient data, an access control list, the hash of data location, owner identity, and previous block. All these terms are defined below.

- **Transaction**

  In blockchain networks, a transaction group is combined into blocks of transactions that are connected in the chain by using the hash of the previous block's record which is stored in the blockchain. As a block progresses further down the chain (and thus becomes older), the more protection it provides against changes to the data contained within it.

- **Access Control List (ACL)**

  An access control list (ACL) is a set of rules in computing that specify which users or systems are allowed or denied access to a specific object or system resource. Network access control lists are put in routers and switches and typically are used to determine which traffic may and cannot transit across the network[24].

- **Hash of location data**

  As soon as an attacker attempts to change any of the keys, the local register will be rendered inoperable because of the completely different hash values that will be generated in the following blocks.

- **Owner Identity**

  Owner identification means the name, image, and likeness of the owner or patient which is

kept safe throughout the entire process.

- **Previous block**

Each block contains a collection of transactions that have been created and dispatched throughout the system. Also included are a timestamp, a link to the previous block, and a hash value that allows each block to be distinguished from the other blocks.

Step-4: Cloud Service Provider

After providing security to patient data by Ethereum blockchain data is stored in a cloud service provider which contains three values EHR, encrypted data, and hash value. A third-party company that provides cloud-based platforms, infrastructure, application, or storage services is known as a cloud service provider.

- **Electronic Health Record (EHR)**

  A digital version of a patient's paper chart is referred to as an electronic health record. Any patient information about treatment history should be recorded in the EHR. Electronic health records (EHRs) keep track of patient care in real-time and make that data instantly and securely available to those with the proper authorization.

- **Encrypted data**

  Encrypting data is the process of converting it from plaintext (unencrypted) to ciphertext (encrypted data). Users can access encrypted data with an encryption key and decryption keys to protect sensitive data.

- **Hash**

  A hash is a function that solves the encrypted demands of a blockchain computation. It is nearly impossible to guess the length of a hash if someone were trying to break the blockchain by guessing the hash's length.

Step-5: Local Database Storage

In this step, data is stored in a local database after processing bya cloud service provider.The medical record data is stored in local database storage to maintain the performance and economic viability of the system, and the hash data is the element of the block that has been committed to the chain of custody.

References

[1]. Angraal, Suveen, Harlan M. Krumholz, and Wade L. Schulz. "Blockchain technology: applications in health care." Circulation: Cardiovascular Quality and outcomes 10, no. 9 (2017): e003800.

[2]. Hussien, Hassan Mansur, Sharifah Md Yasin, S. N. I. Udzir, Aws Alaa Zaidan, and Bilal BahaaZaidan. "A systematic review for enabling of developing a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges,

recommendations, and future direction." Journal of medical systems 43, no. 10 (2019): 1-35.

[3]. Ito, Kenichi, KiichiTago, and QunJin. "i-Blockchain: A blockchain-empowered individual-centric framework for privacy-preserved use of personal health data." In 2018 9th International Conference on Information Technology in Medicine and Education (ITME), pp. 829-833. IEEE, 2018.

[4]. Authority, Financial Conduct. "Discussion Paper on distributed ledger technology." DP17/3 (April 2017)< https://www. fca. org. uk/publication/discussion/dp17-03. pdf (2017).

[5]. Morkunas, Vida J., Jeannette Paschen, and Edward Boon. "How blockchain technologies impact your business model." Business Horizons 62, no. 3 (2019): 295-306.

[6]. Griebel, Lena, Hans-Ulrich Prokosch, Felix Köpcke, Dennis Toddenroth, Jan Christoph, Ines Leb, Igor Engel, and Martin Sedlmayr. "A scoping review of cloud computing in healthcare." BMC medical informatics and decision making 15, no. 1 (2015): 1-16.

[7]. Gorodnichev, Mikhail, Alexandra Kukharenko, Elena Kukharenko, and Tatyana Salutina. "Methods of developing systems based on blockchain." In Conference of Open Innovations Association, FRUCT, no. 24, pp. 613-618. FRUCT Oy, 2019.

[8]. Koshechkin, K. A., G. S. Klimenko, I. V. Ryabkov, and P. B. Kozhin. "Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation." Procedia Computer Science 126 (2018): 1323-1328.

[9]. Nugent, Timothy, David Upton, and Mihai Cimpoesu. "Improving data transparency in clinical trials using blockchain smart contracts." F1000Research 5 (2016).

[10]. Zheng, Zibin, ShaoanXie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services 14, no. 4 (2018): 352-375.

[11]. Ismail, Leila, HunedMaterwala, and SheraliZeadally. "Lightweight blockchain for healthcare." IEEE Access 7 (2019): 149935-149951.

[12]. Kuo, Tsung-Ting, Hyeon-Eui Kim, and Lucila Ohno-Machado. "Blockchain distributed ledger technologies for biomedical and health care applications." Journal of the American Medical Informatics Association 24, no. 6 (2017): 1211-1220.

[13]. Swan, Melanie. "Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]." IEEE Technology and Society Magazine 34, no. 4 (2015): 41-52.

[14]. Dimitrov, Dimiter V. "Blockchain applications for healthcare data management." *Healthcare informatics research* 25, no. 1 (2019): 51-56.

[15]. Dash, Sonali S., V. Rajasekar, and Sam Goundar. "PalCom Middleware-Based Blockchain Challenges on Healthcare System." In Convergence of Internet of Things and Blockchain Technologies, pp. 109-124. Springer, Cham, 2022.

[16]. Balaji, V. R., and J. R. Dinesh Kumar. "Electronic Health Record Maintenance (EHRM) Using Blockchain Technology." In Internet of Things, Artificial Intelligence and Blockchain Technology, pp. 179-208. Springer, Cham, 2021.

[17]. Cáceres, Cinthia Paola Pascual, José Vicente Berná Martinez, Francisco Maciá Pérez, and Iren Lorenzo Fonseca. "Blockchain Validity Register for Healthcare Environments." In International Congress on Blockchain and Applications, pp. 64-73. Springer, Cham, 2021.

[18]. Gu, Zhuoming, Dan Lin, Jiatao Zheng, Jiajing Wu, and Chaoxin Hu. "Deep Learning-Based Transaction Prediction in Ethereum." In International Conference on Blockchain and Trustworthy Systems, pp. 30-43. Springer, Singapore, 2021.

[19]. Pooranam, N., G. IgnishaRajathi, R. Lakshmana Kumar, and T. Vignesh. "Decision Support Mechanism to Improve a Secured System for Clinical Process Using Blockchain Technique." In Internet of Things, Artificial Intelligence and Blockchain Technology, pp. 241-258. Springer, Cham, 2021.

[20]. Vijayalakshmi, S., S. P. Gayathri, and S. Janarthanan. "Blockchain Security for Artificial Intelligence-Based Clinical Decision Support Tool." In Internet of Things, Artificial Intelligence and Blockchain Technology, pp. 209-240. Springer, Cham, 2021.

[21]. Shuaib, Mohammed, Shadab Alam, Mohammad Shabbir Alam, and Mohammad Shahnawaz Nasir. "Self-sovereign identity for healthcare using blockchain." Materials Today: Proceedings (2021).

[22]. Zarour, Mohammad, Md Tarique Jamal Ansari, Mamdouh Alenezi, Amal Krishna Sarkar, MohdFaizan, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records." IEEE Access 8 (2020): 157959-157973.

[23]. Lee, Tian-Fu, Hong-Ze Li, and Yi-Pei Hsieh. "A blockchain-based medical data preservation scheme for telecare medical information systems." *International Journal of Information Security* 20, no. 4 (2021): 589-601.

[24]. Guo, Hao, Wanxin Li, Mark Nejad, and Chien-Chung Shen. "Access control for electronic health records with hybrid blockchain-edge architecture." In *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 44-51. IEEE, 2019.