Proceedings of the 16th International
Scientific and Practical Conference
«Scientific Research in XXI Century»

(September 16-18, 2024).
Ottawa, Canada

No
216

INFORMATION AND WEB TECHNOLOGIES

Blockchain technology - current status and future research in healthcare technology

Shmatko Oleksandr[1], Gamayun Igor[2], Dorohyi Mykola[3]

[1] PhD, Associate Professor;
Technical University «Metinvest Polytechnic» LLC; Ukraine

[2] doctor of Technical Science, Professor;
National Technical University «Kharkiv Polytechnic Institute»; Ukraine

[3] Masters Student
National Technical University «Kharkiv Polytechnic Institute»; Ukraine

Abstract. Modern society is facing a growing need for safe, efficient, and transparent exchange of patients' personal data in healthcare. Protecting the confidentiality and integrity of medical information is a priority for ensuring high-quality and effective medical care. Blockchain technologies provide a promising tool for solving this problem, allowing you to create a decentralised and secure system for sharing personal patient data. The aim of this work is to ensure a high level of security and confidentiality of medical data, as well as to increase the efficiency of processes in the healthcare sector by developing software components of the patient personal data exchange system based on blockchain technologies. The study's goal is to investigate the system for exchanging patients' personal data in the healthcare sector. The study's subject is software components based on blockchain technologies, designed to ensure the safety, transparency, and efficiency of medical information exchange. Results. This paper proposes an architectural model for a safe and efficient medical data exchange system, suitable for widespread implementation in the healthcare sector. conclusion. The introduction of a secure personal data exchange system based on blockchain technology in healthcare will help improve the quality of medical care and provide medical personnel with faster access to important data. The theoretical significance lies in expanding knowledge about the application of blockchain technologies in healthcare, as well as issues of medical information security and confidentiality. This study can serve as a foundation for further research in this area and contribute to the development of new methods and approaches to medical data exchange.
Keywords: *blockchain, personal patient data, IoTM, smart contracts, Ethereum, Medical Data Exchange System Model.*

Introduction. Medical data contains a large number of patient data records that are important for future treatment and research. However, we must securely store and share data to ensure its confidentiality. Medical data management widely uses blockchain due to its decentralised functions and protection against unauthorised access. Medical data is

INFORMATION AND WEB TECHNOLOGIES

relevant for everyone. They capture physical information about our bodies. This is important for the diagnosis and treatment of diseases [1]. With the rapid development of artificial intelligence, medical data has become a big asset. This can aid in the creation of diagnostic models using artificial intelligence, thereby assisting doctors in their diagnostic processes. Despite the evolution of medical information from initial paper records to electronic medical records (EMR), which offer greater convenience for accessing and storing data, it is crucial to prioritize the protection of data privacy [2]. To prevent sensitive data leaks, numerous hospitals and institutions have curtailed data transmission and exchange, resulting in the fragmentation of medical data across various health facilities [3].The privacy and security of medical data also lead to other problems. For instance, a new hospital should conduct a re-examination of patients for safety reasons. This behaviour leads to a waste of energy and money. The confidentiality of patients prevents the transfer of medical data to scientific institutions, impeding the advancement of medicine. This prompted the search for secure methods of data storage and transmission, and blockchain is widely used, due to its decentralised nature, protected from unauthorised access, for the exchange of medical data [4]. Modern society is facing a growing need for safe, reliable, and transparent sharing of patients' personal data in the healthcare sector. Protecting the confidentiality and integrity of medical information is a priority for ensuring high-quality and effective medical care. Blockchain technologies provide a promising tool for solving this problem, allowing you to create a decentralised and secure system for sharing personal patient data.The study's goal is to investigate the system for exchanging patients' personal data in the healthcare sector. The study's subject is software components based on blockchain technologies, designed to ensure the safety, transparency, and efficiency of medical information exchange.The aim of this work is to ensure a high level of security and confidentiality for medical patients, as well as to increase the efficiency of processes in the healthcare sector by developing software components of the patient personal data exchange system based on blockchain technologies.Main partIn the growing world of technology, things around us are getting smarter than we think. The latest technology is also revolutionizing fields like healthcare. As technology advances, the healthcare industry's quality and

INFORMATION AND WEB TECHNOLOGIES

efficiency also grow rapidly. Both doctors and patients benefit from technological advances in healthcare. Now we receive laboratory reports, MRIs, and CT scans in less time, which is more efficient and accurate than before. Digital X-rays are a revolutionary way to look at bone fractures and tumors, and digital storage of medical records opens up a new way to care for patients using deep learning and artificial intelligence technologies. Furthermore, thanks to technological advances, it is possible to continuously monitor patients remotely, collect data from patients in real time using IOT sensors, and perform analysis without delays [1].Now we can more accurately predict serious diseases (such as cancer) and prescribe medications at a very early stage. While storing medical data digitally provides many advantages, it also opens the door to security threats and data loss. As we know, medical data is critical; it consists of confidential and sensitive information related to patients.Therefore, we need a reliable mechanism to confirm the integrity and confidentiality of safe medical data. Integrating blockchain technology with the healthcare industry can solve Da's integrity and security problems. We can now share health-related patient data with doctors and healthcare providers more efficiently and securely.The healthcare system was initially known as Healthcare 1.0 in the 1970s. In healthcare, there was an acute shortage of resources, and the ability to interact with digital systems was limited. During this period, when medical companies transitioned to paper prescriptions and reports, the absence of integrated biomedical sensors led to an increase in costs and time. The concept of healthcare systems emerged from 1991 to 2005 with healthcare 2.0. During this phase, doctors utilized digital tracking to study the patient's health status using imaging equipment. With the introduction of the online platform, healthcare providers began to create online communities and use cloud servers to store patient information, which provided widespread access for both the patient and the practitioner. Healthcare 3.0 introduced the concept of customizing patients' medical records. New user interfaces provide a personalised and optimised experience. Besides these achievements, the implementation of medical documentation systems enables real-time and universal tracking of patients' medical data. Similarly, the integration of EHR systems like HL7 to store patient information led to the emergence of autonomous non-network

INFORMATION AND WEB TECHNOLOGIES

systems like social media channels. This has reduced the exchange of medical data, whether online or between clinicians using HL7. These techniques also improved the ability to interact and communicate with the patient. The era of healthcare 4.0 began in 2016 and continues to this day [3]. During this time, a number of different technologies have been applied, including fog computing, frontier computing, cloud computing, the Internet of Things, advanced analytics, artificial intelligence and machine learning, and blockchain, to transform it into an intelligent healthcare system, or Healthcare Industry 4.0. The main focus was on wearable health sensors.Innoplexus combines artificial intelligence and blockchain to provide continuous scanning of global life science data [5]. The system collects data for research institutes and pharmaceutical companies. BlockRx is a platform that has been successfully used in real-world documents [6]. The platform combines blockchain technology and advanced isolated digital ledger technology. The platform combines medical data from biomedical and research institutes. The implementation of BlockRx has resulted in significant progress.

Blockchain-based models have been the subject of several published summaries. Jin et al. conduct an analysis of the confidentiality of medical data exchange, utilizing the model's type of blockchain [7]. The review divides blockchains into two categories: without permissions and with authorised access. The analysis then focuses on the advantages and disadvantages specific to each type of blockchain. Leili et al. analysed a number of papers published between 2016 and 2020 [8]. This article focuses on healthcare application situations rather than comparing and generalizing models. Sakha et al. summarised some blockchain-based healthcare approaches, but did not compare them [9]. Israel et al. analysed the model from a unique point of view, considering both the benefits and threats that the technology poses to patients [10]. Hasselgren et al. performed a statistical analysis of the published papers. However, the review did not provide a summary of the methods used [11]. Xu et al. mainly analyse the use of blockchain in medical cancer data, such as drug traceability and cancer data sharing [12]. Blockchain is a decentralised distributed technology (DDT) [16]. A distributed system of computing nodes in a single-rank network develops and manages a blockchain, a collection of records that block the exchange or transfer of valuables and digital

INFORMATION AND WEB TECHNOLOGIES

assets, such as transactions, goods, and services. Bitcoin, a distributed database with ever-growing records treated as a block, is the source of blockchain technology [19]. The main idea of the blockchain is to stabilise the integrity, traceability, and accountability of shared data. Distribute-to-book restricts methods, such as storage and authentication, to a network of interacting nodes. These nodes implement audit software that matches the image of a shared ledger between a peer-to-peer network of shareholders, presenting all accountable actions using digital fingerprints or hash codes. When writing data, we classify a workbook as distributed. In the blockchain, each node participant has its own shared ledger. It generates a transparent, non-variable record [20]. Blockchain logs provide accuracy for receiving messages in the health IT environment, and audit logs offer accuracy for further requests for such permissions and performance of access models. Based on this functionality, the framework works as a consistent description of electronic health information access authorisation (EHI). Over the past decade, researchers have implemented several blockchain-based healthcare management systems to achieve various security goals [21, 22]. Malicious attacks cannot tamper with the data, and the blockchain verifies various aspects of the data's origin [23]. This technology uses cryptographic methods, and the blockchain network's distributed environment ensures the distribution of the entire information, providing a visible, trustworthy digital fingerprint and verifiable paths [24]. There are two main types of blockchains: perpetual and permissive. We also refer to a public blockchain as a blockchain without access rights. Bitcoin was the first blockchain to be invented without access rights. Without permissions, the blockchain is easily accessible and open for read and write actions by all system participants [25]. This means that anyone can participate in the system with Alias identification. The system identifies the user as part of the consensus mechanism and allows them to read or broadcast information [26, 27]. Ethereum also uses blockchain without permissions, so anyone can develop and combine smart contracts over the network without any restrictions on the part of developers. We also call an authorized blockchain a private blockchain. A separate organisation uses the authorised blockchain [28]. A blockchain with permissions design ensures that network participants are pre-defined for read/write actions and permanently identified within the system, unlike

INFORMATION AND WEB TECHNOLOGIES

a blockchain without permissions. So the main difference between a blockchain without access rights and a blockchain with permissions is how the user can access the network. In a permissive blockchain network, implement Byzantine Fault Tolerance (BFT) [29]. The Hyperledger framework aims to safeguard shared registry technology and enhance the capabilities of authorized users. Hyperledger Fabric is a type of permitted blockchain technology that runs on an open-source blockchain enterprise supported by the Linux Foundation [30]. Hyperledger is an ever-expanding collective or private blockchain that attempts to improve blockchain technology through industry-specific applications. Typically, a Hyperledger Fabric is a peer-to-peer distributed network where each peer-to-peer node has a replicated, consistent copy of the blockchain's data structure, specifically a transaction chain index describing the call and execution of chain codes. Hyperledger Fabric makes it possible to expand the range of applications of blockchain technology beyond cryptocurrency transactions, which distinguish between different areas of application of distribution databases, including medical information management [31]. The Linux Foundation supported Hyper-ledger Fabric projects, one such example being Hyperledger Composer. The Hyperledger Fabric blockchain inherits the Business Network Archive (BNA), a functional development of Hyperledger Composer [15]. Participants in the business network combine based on their identification and the assets generated in the system, with transactions defining the exchange of these assets. These rules facilitate the execution of smart contracts, which ultimately store all transactions in the ledger. Figure 1 illustrates the overall Hyperledger composer architecture. The model file contains three main components: participants, assets, and transactions. Participants are end users of the system, able to deal with assets and interact with others through transactions. Assets are usually stored on the network as changes. System targets call transactions to update settings. The Business Network script file defines many transaction functions in the system. It consists of JavaScript (JS) and deals with business logic that determines what standards apply to users and what types of resources are common. The Access Control List (ACL) describes the various access ranges that participants in the network have. The ACL file records the participants' goals, which determines their effectiveness in creating, reading, updating, or deleting

INFORMATION AND WEB TECHNOLOGIES

resources. The request file explains the system's request composition and usage. They remain fixed to extrapolate the transaction log, which contains records of all previous transactions on the network. The archive record specifies a registry that contains the history of system transactions and events. The system updates the log entry during transaction processing, preserving a history of all transactions within the business network. Participants send transactions using their identifiable data, and composer requests can extract log entry resources to request specific records. Depending on the method of participation, we can divide the blockchain into three categories: public, private, and consortium chains [15]. The public network, as the name suggests, is completely public and accessible to everyone. Since data in the chain cannot be changed, public chains are considered completely decentralized. Only authorised participants can participate in the consortium chain, and the Al-Yansu rules formulate read and write permissions as well as permissions to participate in the blockchain. Only private organisations use the private chain, and they formulate read and write permissions to the blockchain, as well as permissions to participate in accounting, according to their own rules. There are few participating nodes, and they are strictly limited [16]. In the table. The table compares various types of blockchains. Nodes receive transactions in a different order as a decentralized peer-to-peer system [17]. Therefore, nodes require consistent algorithms to coordinate transactions. Proof of work (POW) is the first successful decentralised blockchain consensus algorithm. To solve the Byzantine problem, a practical algorithm called Byzantine Fault Tolerance (PBFT) was proposed [18]. This ensures that the BLO-kchain can still function normally with some faulty or malicious nodes.

The introduction of EMR has brought convenience, as well as privacy concerns. Security concerns prevent the free transfer of medical data. There have been several proposals for blockchain-based models [22]. Rahul et al. [23] proposed the blockchain-based "medichain" model. This model uses the blockchain as a database to collect complete information about the patient's case in the block. To ensure data security and prevent forgery, we hash transaction records and store the resulting hash values in the Merkle tree, thereby reducing errors in clinical decision-making. The proposed structure combines data from all fields into a single hyperspace to

INFORMATION AND WEB TECHNOLOGIES

address the challenge of diverse medical data structures and a wide range of source types. This method relies on chain storage. However, the blockchain is less scalable. Storing data online is also expensive. Wu implements a patient-centred access control model with confidentiality in the process of controlling access to private information in healthcare systems [24]. Wu then utilizes blockchain technology to establish a private information storage platform, while standard cryptographic algorithms facilitate the transfer of information. A file authorisation agreement safeguards confidential information in this process, thereby preventing the theft of confidential medical information. The model offers a detailed privacy-enabled access control method that grants users various privileges based on an assessment of their types. A third-party organisation that provides cloud services hosts a cloud database that stores EMR information. The cloud generates a hash of the data when it stores it. The blockchain then stores the hash. The chain's hash value compares tampered data in the cloud. In this model, the consensus algorithm is POW, which requires a large number of invalid node calculations. Liu et al. proposed a lightweight blockchain-based model for the exchange and protection of medical data [25]. To ensure data exchange between doctors in different hospitals, the model uses proxy re-encryption technology. The hash function used is difficult to match. Thus, stored medical information is almost impossible to obtain. We have improved the traditional delegated confirmation of interest to create a new consensus algorithm that is more secure and reliable. We have developed a mechanism for disease comparison, enabling patients with the same disease to communicate with each other. Patients can set session keys after mutual authentication. This mechanism can help patients share information about the disease. The PRI-Watt network is fast in terms of transactions, but less centralized. It is more suitable for applications within companies or institutions. This approach is not applicable in scenarios where there are numerous patients and hospitals. Yu et al. proposed a hybrid chain-based EHR sharing scheme to maintain the private part of electronic circulation in the federal chain, rather than the private part in the public chain [26]. Only licensed users can access the closed part, and scientific institutions can grant access to the closed part for medical development. The model employs offline storage, storing solely data hashes in the chain to thwart

INFORMATION AND WEB TECHNOLOGIES

data forgeries, while smart contracts autonomously oversee the EMR request, approval procedure, and utilization. The model employs a novel hybrid chain approach. However, the model uses rough access control and does not assign nodes any attributes. Zou et al. developed a new chain structure to avoid the branching problem and proposed a trust-based consensus mechanism to counter Byzantine attacks [27]. Through continuous mining, medical institutions can accumulate pre-faith points in exchange for EMR. The proposed reputation system is designed to accumulate reputation points in response to a significant number of incorrect calculations. Voting requires a significant amount of energy. Shahnaz et al. offer a blockchain-based, fine-grained access system that provides various access rights to patients, doctors, nurses, and administrators [28]. Access to electronic links is registered in the model proposed in [29], and a searchable encryption method is used to search for information without decrypting the chain's data. This method safeguards the privacy of data and guarantees the prompt execution of requests. This method also uses role-based access control. IOMT comprises a variety of medical devices that use computer networks to connect and determine patient symptom parameters. IOMT has many advantages for treating diseases, and detecting physical signs allows you to detect the disease as soon as possible and seek medical attention [30]. However, many IoMT products on the market lack uniform management standards, which can lead to information leaks [31]. Blockchain offers a solution for ensuring the security of medical IOMT [32]. Chen et al. developed an IoMT-based data collection system to ensure secure storage and exchange of medical data [33]. The system can simultaneously collect data from multiple medical devices, ensuring real-time collection of a patient's medical records during surgery. A cloud server and a re-encryption algorithm via a proxy serve as the foundation for the system's anonymous medical data exchange scheme. This approach increases the security of sharing private medical data. Hyperledger Fabric, a permitted blockchain architecture with a dual-channel deployment architecture and a medical chain code for data management and access control, serves as the foundation for the system's implementation. This method uses the Kafka consensus algorithm. This sequential algorithm can cause half of the nodes to fail, but it cannot allow malicious nodes. This makes the system more vulnerable to attacks. Jafar proposed a new

INFORMATION AND WEB TECHNOLOGIES

blockchain-based secure authentication technology to enhance the security of sensitive medical data transmitted between patients and hospitals [34]. Lamport Merkle digital signature (LMDS) generates and verifies signatures to ensure the secure transfer of sensitive medical data to cloud-based IoT medical networks. Smart contracts allow participating parties (i.e., patients and doctors) to set conditions and automate operations through a cloud server, reducing the work of third parties. Smart contracts also have different addresses and accounts on the blockchain, so that each IoT device can view and execute its own instructions, thereby reducing communication overhead. Al-Karalle et al. present a new model of secure image transmission and diagnostics using deep learning and blockchain for IoMT [35]. The proposed model includes several processes, including data collection, secure transactions, hash value encryption, and data classification. Initially, we collect patient data using Internet of Things tools and then encrypt it using the GO-FFO algorithm. Additionally, NIS-BWT technology encrypts and compresses hashes in the blockchain. Alternatively, the DBN model executes the classification process. The improved encryption algorithm, while more secure, takes longer to encrypt and decrypt than other algorithms. Suyel [36] proposes a system that offers an API interface. This interface generates and maintains health data between the healthcare professional and the patient. Additionally, a pro-protected system fully utilizes smart contracts to establish secure rules, thereby preventing malicious behavior. This method uses only simple authentication. We can assign detailed properties to nodes. This could make the model more advanced. Hu et al. suggest that the current focus of much blockchain-based IoMT research is on verifying cryptographic algorithms. From time to time, you should pay more attention to invalid signatures to reduce the likelihood of verification failure. Smart contracts on the blockchain play an important role in IOMT. Smart contracts do not require the participation of third parties and can automatically perform assigned tasks if the conditions are met. Typically, the model uses cryptographic algorithms to improve security. The confidentiality of medical data hinders the operation of data-based machine learning. Federated learning is a new artificial intelligence method that protects data privacy while building artificial intelligence models. Federated learning enables multiple nodes to collaboratively learn the model in public, transmitting only gradients and

INFORMATION AND WEB TECHNOLOGIES

losses, not the actual data, thereby ensuring robust data protection. For the next calculation, however, nodes must transmit data to a central institution. Blockchain can serve as a viable substitute for a central institution, thereby mitigating the potential for dishonesty within the central structure.

Conclusions. The analysis of the current state and prospects of using blockchain technologies in the healthcare sector allows us to draw the following conclusions: Blockchain technology demonstrates significant potential for solving key problems in the field of medical data management, particularly in ensuring the secure exchange and storage of personal patient information. A study of existing blockchain-based models and approaches reveals the significant benefits of this technology in improving the level of security, privacy, and efficiency of medical information processing. The main advantages of implementing blockchain in the healthcare system include: strengthening protection against unauthorised access to medical data; improving interoperability between different medical institutions and information systems; improving mechanisms for controlling access to data by patients; and creating conditions for secure data exchange for scientific purposes without violating confidentiality. Simultaneously, we've identified a number of challenges that necessitate further research and solutions. These include: ensuring scalability of blockchain-based systems; optimising consensus algorithms to reduce power consumption; and developing more advanced access control and cryptographic data protection mechanisms. The integration of blockchain technologies with other innovative solutions, such as the Internet of Medical Things (IoMT) and federated learning, opens up new prospects for creating more reliable and efficient healthcare systems. Researchers should focus their efforts on enhancing current models, formulating fresh strategies for safeguarding data confidentiality and security, and putting blockchain-based systems into practical use and testing within the operational environment of healthcare institutions. Thus, the introduction of blockchain technologies in the healthcare sector has the potential to significantly improve the quality of medical care, protect patients' rights, and promote the development of medical science while ensuring a high level of data security and confidentiality. Realising this potential requires further interdisciplinary research and development, as well as close

collaboration between specialists in information technology, medicine, and law.

References:

[1] Häyrinen Kristiina, Saranto K, Nykänen Pirkko. Definition, structure, content, use and impacts of electronic health records: a review of the research literature. Int J Med Inform. 2008 May;77(5):291-304. doi: 10.1016/j.ijmedinf.2007.09.001.S1386-5056(07)00168-2

[2] Hripcsak G, Albers DJ. Next-generation phenotyping of electronic health records. J Am Med Inform Assoc. 2013 Jan 01;20(1):117-21. doi: 10.1136/amiajnl-2012-001145. http://europepmc.org/abstract/MED/22955496 .amiajnl-2012-001145

[3] Ludwick DA, Doucette J. Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries. Int J Med Inform. 2009 Jan;78(1):22-31. doi: 10.1016/j.ijmedinf.2008.06.005.S1386-5056(08)00092-0

[4] Zahabi M, Kaber DB, Swangnetr M. Usability and Safety in Electronic Medical Records Interface Design: A Review of Recent Literature and Guideline Formulation. Hum Factors. 2015 Aug;57(5):805-34. doi: 10.1177/0018720815576827.0018720815576827

[5] Mikkelsen G, Aasly J. Concordance of information in parallel electronic and paper based patient records. International Journal of Medical Informatics. 2001 Oct;63(3):123-131. doi: 10.1016/s1386-5056(01)00152-6

[6] Thiru K, Hassey A, Sullivan F. Systematic review of scope and quality of electronic patient record data in primary care. BMJ. 2003 May 17;326(7398):1070. doi: 10.1136/bmj.326.7398.1070. http://europepmc.org/abstract/MED/12750210 .326/7398/1070

[7] Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. J Am Med Inform Assoc. 2006;13(2):121-6. doi: 10.1197/jamia.M2025. http://europepmc.org/abstract/MED/16357345 .M2025

[8] Archer N, Fevrier-Thomas U, Lokker C, McKibbon KA, Straus SE. Personal health records: a scoping review. J Am Med Inform Assoc. 2011;18(4):515-22. doi: 10.1136/amiajnl-2011-000105. http://europepmc.org/abstract/MED/21672914 .amiajnl-2011-000105

[9] Roehrs A, da Costa Cristiano André, Righi RDR, de Oliveira Kleinner Silva Farias. Personal Health Records: A Systematic Literature Review. J Med Internet Res. 2017 Jan 06;19(1):e13. doi: 10.2196/jmir.5876.

[10] Rudin RS, Motala A, Goldzweig CL, Shekelle PG. Usage and Effect of Health Information Exchange. Ann Intern Med. 2014 Dec 02;161(11):803. doi: 10.7326/m14-0877

[11] Williams C, Mostashari F, Mertz K, Hogin E, Atwal P. From the Office of the National Coordinator: the strategy for advancing the exchange of health information. Health Aff (Millwood) 2012 Mar;31(3):527-36. doi: 10.1377/hlthaff.2011.1314.31/3/527

[12] Cimino JJ, Frisse ME, Halamka J, Sweeney L, Yasnoff W. Consumer-mediated health information exchanges: the 2012 ACMI debate. J Biomed

INFORMATION AND WEB TECHNOLOGIES

Inform. 2014 Apr;48:5-15. doi: 10.1016/j.jbi.2014.02.009. https://linkinghub.elsevier.com/retrieve/pii/S1532-0464(14)00046-X. S1532-0464(14)00046-X

[13] Zhuang Y, Sheets LR, Chen Y, Shae Z, Tsai JJ, Shyu C. A Patient-Centric Health Information Exchange Framework Using Blockchain Technology. IEEE J. Biomed. Health Inform. 2020 Aug;24(8):2169-2176. doi: 10.1109/jbhi.2020.2993072.

[14] Gordon WJ, Catalini C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Comput Struct Biotechnol J. 2018;16:224-230. doi: 10.1016/j.csbj.2018.06.003. https://linkinghub.elsevier.com/retrieve/pii/S2001-0370(18)30028-X .S2001-0370(18)30028-X

[15] Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Comput Struct Biotechnol J. 2018;16:267-278. doi: 10.1016/j.csbj.2018.07.004. https://linkinghub.elsevier.com/retrieve/pii/S2001-0370(18)30037-0 .S2001-0370(18)30037-0

[16] Murphy DR, Satterly T, Rogith D, Sittig DF, Singh H. Barriers and facilitators impacting reliability of the electronic health record-facilitated total testing process. Int J Med Inform. 2019 Jul;127:102-108. doi: 10.1016/j.ijmedinf.2019.04.004.S1386-5056(18)31386-8

[17] Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications. 2020 Feb;50:102407. doi: 10.1016/j.jisa.2019.102407

[18] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society. 2018 May;39:283-297. doi: 10.1016/j.scs.2018.02.014.

[19] Zhang A, Lin X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J Med Syst. 2018 Jun 28;42(8):140. doi: 10.1007/s10916-018-0995-5.10.1007/s10916-018-0995-5

[20] Cao S, Zhang G, Liu P, Zhang X, Neri F. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences. 2019 Jun;485:427-440. doi: 10.1016/j.ins.2019.02.038.

[21] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Bitcoin: Open Source P2P Money. 2008. [2021-04-23]. https://bitcoin.org/bitcoin.pdf .

[22] Ferdous MS, Chowdhury MJM, Hoque MA. A survey of consensus algorithms in public blockchain systems for crypto-currencies. Journal of Network and Computer Applications. 2021 May;182:103035. doi: 10.1016/j.jnca.2021.103035.

[23] Kuo T, Zavaleta Rojas H, Ohno-Machado L. Comparison of blockchain platforms: a systematic review and healthcare examples. J Am Med Inform Assoc. 2019 May 01;26(5):462-478. doi: 10.1093/jamia/ocy185. http://europepmc.org/abstract/MED/30907419 .5419321

[24] McGhin T, Choo KR, Liu CZ, He D. Blockchain in healthcare applications: Research challenges and opportunities. Journal of

INFORMATION AND WEB TECHNOLOGIES

Network and Computer Applications. 2019 Jun;135:62-75. doi: 10.1016/j.jnca.2019.02.027.
[25] Vazirani AA, O'Donoghue O, Brindley D, Meinert E. Implementing Blockchains for Efficient Health Care: Systematic Review. J Med Internet Res. 2019 Feb 12;21(2):e12439. doi: 10.2196/12439. https://www.jmir.org/2019/2/e12439/ v21i2e12439
[26] Hussien HM, Yasin SM, Udzir SNI, Zaidan AA, Zaidan BB. A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. J Med Syst. 2019 Sep 14;43(10):320. doi: 10.1007/s10916-019-1445-8.10.1007/s10916-019-1445-8 [PubMed: 31522262] [CrossRef: 10.1007/s10916-019-1445-8]
[27] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD); August 22-24; Vienna, Austria. 2016. pp. 25-30
[28] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst. 2016 Oct;40(10):218. doi: 10.1007/s10916-016-0574-6.10.1007/s10916-016-0574-6
[29] Roehrs A, da Costa Cristiano André, da Rosa Righi Rodrigo. OmniPHR: A distributed architecture model to integrate personal health records. J Biomed Inform. 2017 Jul;71:70-81. doi: 10.1016/j.jbi.2017.05.012.
[30] Ichikawa D, Kashiyama M, Ueno T. Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR Mhealth Uhealth. 2017 Jul 26;5(7):e111. doi: 10.2196/mhealth.7938. https://mhealth.jmir.org/2017/7/e111/ v5i7e111
[31] Mannaro K, Baralla G, Pinna A, Ibba S. A Blockchain Approach Applied to a Teledermatology Platform in the Sardinian Region (Italy) Information. 2018 Feb 23;9(2):44. doi: 10.3390/info9020044
[32] Ji Y, Zhang J, Ma J, Yang C, Yao X. BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. J Med Syst. 2018 Jun 30;42(8):147. doi: 10.1007/s10916-018-0998-2.10.1007/s10916-018-0998-2 [PubMed: 29961160] [CrossRef: 10.1007/s10916-018-0998-2]
[33] Kleinaki A, Mytis-Gkometh P, Drosatos G, Efraimidis PS, Kaldoudi E. A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. Comput Struct Biotechnol J. 2018;16:288-297. doi: 10.1016/j.csbj.2018.08.002. https://linkinghub.elsevier.com/retrieve/pii/S2001-0370(18)30040-0 .S2001-0370(18)30040-0
[34] Jamil F, Hang L, Kim K, Kim D. A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. Electronics. 2019 May 07;8(5):505. doi: 10.3390/electronics8050505.
[35] Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics J. 2019 Dec;25(4):1398-1411. doi: 10.1177/1460458218769699.
[36] Jamil F, Ahmad S, Iqbal N, Kim D. Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals. Sensors (Basel) 2020 Apr 13;20(8):2195. doi: 10.3390/s20082195. https://www.mdpi.com/resolver?pii=s20082195 .s2008215.