Blockchain in e-Health: Review

Rees Mangena, Nidhal Taferguennit, Samia Aitouche, Seyf El Islam Bousiouda, Fadhila Djouggane, Morri Farida
Laboratory of Automation and Manufacturing, Industrial Engineering Department, University Batna 2, Batna, Algeria
e-mail: mangenarees@gmail.com, nidhaltaferguennit@gmail.com, s.aitouche@univ-batna2.dz,
bousioudaseyfelislam@gmail.com, djougganefadhila@gmail.com, mourrisihame@gmail.com

Abstract— **Certain researchers consider the blockchain technology as an Industry 4.1 revolution, because it benefits from the Industry 4.0 revolution and its technologies, in a decentralized manner. It is a revolution in digital world. In this paper, authors addressed a review of the use of blockchain technology in electronic health (eHealth) because of its importance for the comfort of citizens and the promotion of a healthy society, especially after the pandemic experience of COVID-19, where the necessity and the importance of telework and, Information and Communications Technology (ICT) became more essential than ever before. The review begins by the essence of eHealth and the problems encountered in it. It responds to how blockchain can promote eHealth in terms of management of patient data, its privacy, gains in time and because of how it is a facility without a central authority. The decentralized management of the blockchain does not mean a mess or a loss of data; on the contrary, it means the accountability of all members and partners of the blockchain (patient, doctor, medical institution, etc.). This is guaranteed by the good choice of the consensus algorithms to minimize time, energy consumption and consequently minimize costs. Several algorithms and other issues are discussed in this review paper to help researchers and software developers to discover and use the opportunity of blockchain in eHealth. All the used rules consented by the partners of blockchain system for eHealth are automatically applied in the form of smart contracts. These latter allow the treatment of citizens by the same way, without subjectivity and favoritism.**

Keywords-blockchain; eHealth; e-Health; telemedecine; EHR; electronic health record.

I. INTRODUCTION

In 2008, the cryptocurrency Bitcoin [1] launched the blockchain technology, which has inherited properties such as decentralization, transparency, and anonymity. Bitcoin represents a good use-case for blockchain technology, with close to 400 million completed transactions as of March 19, 2019 [2]. As a result, there have been talks and suggestions that blockchain technology could be useful in a variety of other data-driven sectors, others as big as healthcare [3].

Healthcare has had a reputation for being a traditional business that is difficult to evaluate due to the realities of change and it’s resistance to new ideas. Healthcare issues (such as privacy, quality of care, and information security) have gotten a lot of attention in recent years all around the world. Blockchain technology is becoming more widely recognized as a means for addressing current information mismanagement difficulties. It has the potential to improve immediate healthcare practices, such as health service delivery and care support quality. The blockchain's immutability is a critical feature for healthcare data. It can protect health records, clinical trial outcomes, and regulatory compliance. Smart contracts are being utilized to show how blockchain can help with real- time patient monitoring and medical interventions [12]. Health Insurance Portability and Accountability Act (HIPAA) compliant solutions provide record protection while enabling access to patients and medical professionals.

Further blockchain applications include the pharmaceutical supply chain and the development of anti-counterfeiting mechanisms. While the development of new pharmaceuticals incurs significant expenditures connected to trials to evaluate the drug's safety and efficacy, the usage of smart contracts allows for a more efficient informed consent approach, as well as improved data management and quality [13]. Providing patients with access to manage their own identities allows the informed consent method to be integrated while preserving the privacy of individual health data. In the pharmaceutical industry, blockchain has the potential to assist the pharmaceutical business deal with the rising risks of counterfeit and unapproved pharmaceuticals. With integrated Global Positioning System (GPS) and chain-of-custody logging, smart contracts for pharmaceuticals can be formed and then identified, similar to device tracking.

Within clinical trials, blockchain can be used to address issues, such as falsified results and data removal that contradict the researcher's bias or the funding source's objective. Clinical studies will be more reliable as a result of this. It also enables for the creation of an irreversible log of trial subject consent. It is estimated that identifying a chain-of-custody in the supply chain may save the pharmaceutical sector $200 billion [7]. Many sectors of health insurance could benefit from a reliable record of events surrounding the patient pathway, such as improved incident reporting and automated underwriting operations. Contracts, such as automated payments for segments of the patient journey, could also be precisely stated and then implemented.

This paper is organized as follows; Section 2 gives a view on the meaning of eHealth and some problems encountered in it. Section 3 clarifies the need of blockchain in eHealth to solve some of these problems. Some types of used blockchains in eHealth are given in Section 4. Section 5 points the more adapted and benefic consensus or algorithms to eHealth. Section 6 highlights the use of smart contracts in eHealth. The methods of accessing and storing data are presented in Section 7. Section 8 inspects the benefits of IOT in eHealth and blockchain. Section 9 is devoted to Electronic Health Records. Section 10 analyses blockchain eHealth’s respect of General Data Protection Regulation (GDPR) rules. Then we finished by general remarks in a conclusion Section.

II. Problems In e-Health

The use of the Internet and other technologies in the health-care industry is referred to as eHealth [8]. eHealth is an evolving field at the intersection of medical informatics, public health, and business. It refers to health services and information distributed or enhanced through the Internet and associated technologies. According to the World Health Organization (WHO), eHealth is "the cost-effective and secure use of information and communication technologies in support of health and health-related fields, such as health-care services, health surveillance, health literature, and health education, knowledge, and research."

Many government health institutions have developed frameworks to ensure a high level of security and privacy. For example, the United States (US) Congress proposed the Health Insurance Portability and Accountability Act (HIPAA) in 1996 as a federal law that applies to the US healthcare industry. For effective use of eHealth, a set of valuable security and privacy requirements must be put in place in accordance with HIPAA guidelines [32].

- **Accessing and Sharing Health Data:** Data must be transferred between healthcare providers, third parties, insurers, and patients while adhering to data protection regulations in the healthcare sector.
- **Nationwide Interoperability:** Having a single standard for patient data exchange facilitates data exchange between healthcare providers, which legacy systems frequently do not provide.
- **Medical Device Tracking:** Medical device tracking from the supply chain to decommissioning enables quick retrieval of devices, avoidance of unnecessary repurchasing, and fraud analytics.
- **Drug Tracking:** Blockchain like medical devices, allows for the tracking of the chain of custody from the supply chain to the patient, allowing for frictionless recalls and the prevention of counterfeit drugs.

Furthermore, blockchain based health care systems face additional challenges, such as system evolution, privacy leakage, energy consumption, and communication scalability, due to the complexities associated with healthcare engagement and laws [28].

III. The Use of Blockchain Technology in e-Health

There are many problems in today’s healthcare that may be solved using blockchain. Two of the major focuses that must be addressed are: Data security and Data ownership. Others include health data interchange, nationwide operability, Medical Device tracking, Drug Tracking, Clinical trials and Health Insurance. Currently, sensitive medical records lack a secure structure, resulting in data breaches with serious consequences. For example, in 2018, the Office for Civil Rights (OCR) at the Department of Health and Human Services (DHHS) received notification of numerous data breaches that exposed 13 million total healthcare records.

The second source of concern is that patients are currently unable to fully own their own medical data, a concept that is becoming more relevant with the rise of personalized medicine and wearables. Both of these issues have significant moral ramifications that must be addressed. Blockchain technology could be the answer to both these problems.

Another key challenge as tagging medical equipment with a usable ID and integrating trust in device identification and tracking. When a device, such as an infusion pump, is shown to have malfunctioned, tracking the device can reveal the source of the problem and prevent unnecessary repurchasing in the case of lost devices. These threats are likely to be reduced by a strong trust infrastructure based on medical device identification. According to the report, only 20% to 30% of medical devices are connected within hospitals due to security and privacy concerns.

Blockchain can also assist the pharmaceutical industry in overcoming the growing risks associated with counterfeit and unapproved drugs. As with device tracking, smart contracts for drugs can be defined and then pill containers identified using integrated (GPS) and chain-of-custody logging.

Another use of blockchain in healthcare could be in clinical trials to overcome problems such as fraudulent results and the removal of data that does not support the researcher's bias or the funding source's intention. This will enforce clinical trial integrity. Furthermore, it allows for the keeping of an immutable log of trial subject consent. The pharmaceutical industry is expected to save $200 billion by defining a chain-of-custody in the supply chain. Health insurance could also benefit from a trusted record of events surrounding the patient pathway, such as improved incident reporting and automating underwriting activities. Contracts, such as automated payments for parts of the patient pathway, could also be clearly defined and then implemented [11].

Table 1 [25] shows the benefits of blockchain to the eHealth systems, relative to the traditional system. Privacy, security, transparency and reliability are guaranteed in the blockchain system.

All pharmacists will potentially be impacted by this technology and therefore should have a strong interest in it. Pharmacists could have prescriptions that cannot be forged. Pharmacists in research laboratories could use this technology to prove the progress of their research without disclosing it. Finally, industrial pharmacists will be able to ensure the authenticity of medicines throughout their journey [26].

TABLE I. Comparison Of Traditional, Centralized,And Blockchain Supported eHealth

criterion	Traditional Healthcare System	Centralized Telemedicine System	Blockchain Supported Telemedicine
Cost	High	Low	Low
Patient Waiting Time	Very High	Low	Low
Fault Tolerence	No	No	Yes
Requirement for In-	Yes	No	No

Person Visiting			
Data Provenance	No	No	Yes
Health Record Manipulation	Yes	Yes	No
Documentation	Yes	Yes	No
System Administration	Centralized	Centralized	Decentralized
Audit Trials	No	No	Yes
Data Privacy & Security	Hard	Hard	Easy
Transparency	No	No	Yes
Reliability & Integrity	Low	Low	High

Blockchain Supported telemedecine is better for the comfort of patients and healthcare personel.

IV. eHealth Types of Blockchains

Blockchains are classified into three types: public (permissionless), consortium (public permissioned), and private. They differ in terms of who has access to, writes to, and reads data on the blockchain [30]. Everyone can see the data in a public chain, and anyone can join and contribute to both consensus (in theory) and changes to the core software. The public blockchain is widely used in cryptocurrencies, and the two most popular cryptocurrencies, Bitcoin and Ethereum (the main chain), are public permissionless chains. A consortium blockchain is partially centralized in the sense that only a select group of entities has access to view and participate in the consensus protocol. The network in a private blockchain is distributed but frequently centralized [31]. Only selected nodes can participate in the network, which is frequently managed by a single central authority. The debate over the definition and categorization of the various types of blockchains presented here is still ongoing. There is currently no broad agreement on which distributing characteristics and consensus mechanisms are required to label a technology as "blockchain".

V. Algorithms (Consensus) Used In eHealth Systems

The way data entries are accepted onto the distributed ledger by a distributed consensus protocol validating the data entries is a critical component of blockchains. There are several proposed and used consensus protocols, the three most commonly used being Proof-of-Work (PoW), Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) [34].

Because of its integration in Bitcoin, Proof-of-Work (PoW) is the consensus protocol most strongly associated with blockchain. When the PoW protocol is used, so-called miners compete to solve a computationally difficult puzzle. Miners use brute force to try to find a hash of the proposed block that is less than a predetermined value. The miner who computes this hash value first validates the transactions (or other entries) in the block and receives a reward. When used on a large blockchain, the PoW protocol consumes a significant amount of energy. This is demonstrated by the fact that the current electricity used for Bitcoin mining is comparable to the needs of a smaller country [33].

The selection of an approving node in Proof of Stake (PoS) is determined by the stake each node has in the blockchain. The stake in crypto-currencies is represented by the balance of a given currency. This, however, may give the "richest" node an unfair advantage. To account for this, several hybrid PoS versions have been proposed, in which the stake is combined with some randomization to choose the approving node. Ethereum, the second largest cryptocurrency, intends to switch from PoW to PoS [35]. A Byzantine agreement protocol underpins Practical Byzantine Fault Tolerance (PBFT). Because all nodes in PBFT must be known to the network, this consensus protocol can only be used in a public blockchain. The PBFT consensus process can be divided into three stages: pre-prepared, prepared, and commit. To progress through the three phases, each node must receive two-thirds of the votes cast by all nodes. Hyperledger Fabric currently employs PBFT [36].

Due to the high cost of PoW algorithm in terms of hardware and energy, there was a need for an efficient but low-cost protocol. A promising candidate is the proof of elapsed time protocol made by INTEL which is secure and fast in processing and approving transactions, and low in energy consumption considering the huge number of blocks needed to be created and data to be stored in the health industry. However, this algorithm lacks decentralization, which is the main philosophy of the blockchain technology because this protocol depends only on INTEL hardware. A hybrid protocol with the same properties but independent of INTEL will have promising results [37].

There is one other candidate that can be used which is the proof of weight protocol that has the speed and security needed to store and approve medical data and is low in terms of energy consumption. But the only down side for this algorithm is that it doesn’t reward miners. However, finding an alternative way of paying them will make this protocol an optimal choice for the health industry [19].

VI. Smart Contracts

Smart contracts are supported by some blockchain infrastructures, such as Ethereum. These are self-executing contractual agreements that formalize previously agreed-upon provisions in source code. Because smart contracts are automatically enforced based on these pre-agreed provisions, they operate without the involvement of a third party or intermediary. This function within a smart contract can be activated in a blockchain transaction, and its use appears to be appealing to the health domain [10]. In [4], authors design secure payment protocols by performing blockchain-based smart contract enabling the patients and hospital to reliably pay the diagnostic and storage service efficiently. In general, the smart contracts in eHealth can be involved in [27]:

- Health Record Creation Contact to generate digital health records.
- Health Record Storage Contract for secure storage and rapid access
- Update permission Contract that can provide access at emergency situations.
- Data sharing Permission Contract for exchange of health records between different stakeholders and

VII. Methods of Accessing and Storing Data

A. Using a blockchain tree

This is done by using a principal block on the main chain containing basic information of the patient and a sub block on the sub chain containing the medical record accessed only by using Proof Of Authority (POA) protocol to ensure the registration of any successful or unsuccessful attempts of access to the records, as illustrated in Figure 1 [20].

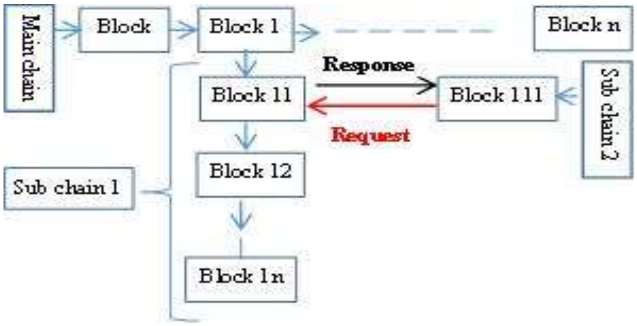

Figure 1. Blockchain tree structure

B. Practical Byzantine fault tolerance

Here, all nodes participate to the voting (2/3 must accept the transaction) which may cause a delay in the transaction processing and slow the whole operation.

Delegated byzantine fault tolerance

Not all nodes most vote which leads to a fast transaction acceptance but with a risk of centralization [21].

C. Adoptive leader election algorithm : (ALEA)

This algorithm is based on electing a leader via Leader Election Algorithm (LEA) to grant him permission to create, access, copy, move, edit and delete data. This type of algorithm is using bully leader election method to minimize energy consumption.

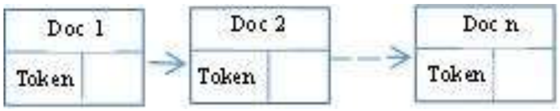

Figure 2. Leader election queue

These algorithms are characterized by:

- 0% failure: due to blockchain technology if a node fails others can do the work
- Ownership can't change if the owner dies or loses consciousness
- High and slow response using ALEA [22]

D. Using two types of chains

A private one that contains the real ID of the patient and a public one which has health data of the patient under a temporary ID, under the control of a hyper ledger fabric framework, noting that only the trusted nodes can access the private chain, as shown in Figure 3.

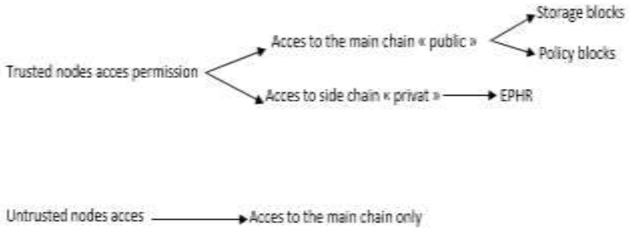
Storage blocks
Acces to the main chain « public »
Policy blocks
Trusted nodes acces permission
Acces to side chain « privat »
EPHR
Untrusted nodes acces
Acces to the main chain only

Figure 3. Types of permission for trusted and untrusted nodes

Storage block: The main chain is used to secure the data from modification as it creates storage blocks containing the temporary ID, patient digital signature approving the transaction, medical institution signature and information about the current block and the previous one.

Policy block: It contains a form of contract about the storing policies of the institution who store the data, signed by both it and the patient then approved by the trusted nodes and broadcasted on the main chain [23].

VIII. Using Internet Of Things (IOT) in eHealth

In this section, we will try to see how can we introduce IOT and blockchain to the health care system, first we must refer to some existing platforms such as OmniPHR [38] which is a platform that allows the sharing of EPHR on a universal scale or GemOS which is used as an access platform to a medical chain owned by the patient and contains his EPHR. many researchers have developed BC-enabled IoT eHealth systems and explored the application of BC technology in diverse fields of eHealthcare. The general idea is to equip patients, post-hospitalization, with equipment easy to use that collect data for example "heart rate, blood pressure, etc. and puts them on the blockchain while having a well put web platform that offers the link for authorized persons (medical staff) to access the patients' data and monitoring his medical status leading to the lowering of the cost of post-hospitalization by roughly 113B$ just in the US (Fig. 4). Cybersecurity is a critical consideration for all users of EHRs, particularly for patients. With the advent of Healthcare 4.0, which is based on IOT and sensors, cyber resilience has become a key requirement in ensuring the protection of patient data across devices [6].

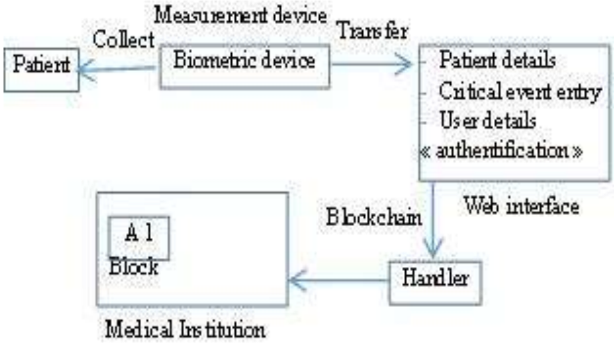

Figure 4. IOT and blockchain health platform

One of many developed methods of collecting patient data and storing them or delivering them in real time to medical institution to ensure the best performance of health care towards the patient is Wireless Body Area Network (WBAN) [18]. It is mainly a collection of wireless sensors placed on or in a human body and is used to exchange data from patient to remote stations (Fig. 5).

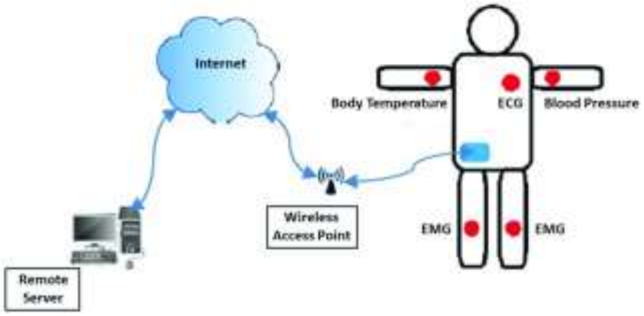

Figure 5. Wireless body area network scheme [29]

Afterwards, all these data are then transferred using blockchain technology to ensure proper security and confidentiality.

IX. Health Records And The Integration Of Blockchain Technology

In a general point of view, e-health is an integration of computing methods and systems to provide solutions to the industry of health care, such as managing patient files but due to the huge amount and diversity of files provided by medical institutions, it has become a challenge to share and store data without failing or breaking the rules of privacy [15]. These files are called EHRs, i.e., a digital format of a patient information such as medical history, current and past medication, etc., that are sourced to cloud but cloud based EHRs aren't secure enough and their current cryptographic methods aren't sufficient enough [18]. Thus, blockchain technology has emerged as a promising solution in terms of privacy and data security since it is independent of third parties such as governments or banks. However, this doesn't mean that it is an optimal solution since it is in its early years and needs more development in terms of performance, energy consumption and offering guaranteed confidentiality since in medical health care no one is allowed to read or see patient files without the proper permission [16].

X. Blockchain Technology and The GDPR Rules

After the rise of blockchain technology, all over the world, a tension was created between this technology and the GDPR. This tension was mainly because of two overarching factors. First, the GDPR is based on assuming that there is always someone who controls data thus adding more protection as commanded by data subjects; however, blockchain has a philosophy of decentralization, which means there is no more governance but many players who control these data, which can make accountability difficult.

Secondly, the GDPR requires the possibility to erase or modify data in certain circumstances but blockchains are designed for the exact opposite purpose where they make the modification or deletion data difficult or even impossible, which makes it hard to reconcile with GDPR requirements [17]. The crucial challenges that companies face to achieve compliance with GDPR, and specifically to i) let data owners full visibility and control on the consents related to their own personal data, and ii) design services that can cope with consents that may change or be revoked dynamically. In [39], authors proposed a solution that relies on the blockchain technology to let data owners grant, access and rectify their consents in a decentralized peer-to-peer fashion, while guaranteeing consensual agreement of data owners and companies on the status of the relevant consents at any time. Although blockchains let all users access all contents freely.

XI. Conclusion

Blockchain is a new technology has the potential to disrupt a variety of data-driven industries, including the healthcare sector. The efficient management of EHRs is critical for patient telecare, which includes medicine for chronic patients, long-term telecare for special patients, and study of patients infected with a specific disease, among other things. The sharing of EHRs with medical practitioners can improve diagnosis accuracy; however, the system's privacy and security preservation of patients' records are drawbacks. Blockchain technology, due to its immutability, has recently been offered as a promising method for accomplishing EHR sharing while maintaining privacy and security [5]. Cyber resilience has become a major requirement in assuring the protection of patient data across devices, thanks to the introduction of healthcare 4.0, which is based on IOT and sensors. To all users in the network, blockchain provides crypto-enforced security, data immutability, and smart contracts-based business logic characteristics [6]. There are several other areas of healthcare and well-being that could be enhanced using blockchain technologies. Accessing and sharing health data, device tracking, clinical trials, pharmaceutical tracing, and health insurance are just a few examples. For accessing and sharing health data, patients can have their EHRs in a decentralized blockchain which any hospital can access instead of having their records scattered in different centralized hospital systems where they are difficult to access all at once and where they are susceptible to privacy breaches and alterations.

In this paper, authors tried to give a review about the usage of blockchain in eHealth to resolve problems of central bureaucratic authority, replaced by a peer-to-peer network allowing decentralized responsibility, even including the end user in certain blockchain solutions, while maintaining patient privacy and protecting the confidentiality of their health folder. Blockchain is still promising in the future of the healthcare domain as well as in other domains.

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review”, 2008, 21260.

[2] Blockchain.com [retrieved: May, 2022]. Available on: https://www.blockchain.com/, charts/n-transactions-total.

[3] M. Mettler, "Technology in healthcare: The revolution starts here. In: 2016 IEEE 18th international conference on e-health networking", applications and services (Healthcom). IEEE, 2016. p. 1-3..

[4] G. Zhang, Z. Yang, and W. Liu, "Blockchain-based privacy preserving e-health system for healthcare data in cloud", Computer Networks, 2022, 203: 108586.

[5] S. Shamshad, Minahil, K. Mahmood, S. Kumari, and C. M. Chen, "A secure blockchain-based e-health records storage and sharing scheme", Journal of Information Security and Applications", 2020, 55: 102590.

[6] N. Venkatachalam, P. O'connor, and S. Palekar, "Cyber Security and Cyber Resilience for the Australian E-Health Records: A Blockchain Solution. In: Handbook of Research on Advancing Cybersecurity for Digital Transformation", IGI Global, 2021. pp. 61-78.

[7] Frost and Sullivan, "Why Healthcare Industry Should Care About Blockchain?" 2017. [Online]. Available on: https://ww2.frost.com/files/8615/0227/3370/Why_Healthcare Industry_Should_Care_About_Blockchain_Edited_Version. [retrieved : June 2022]

[8] eHealth: Definition, History, Characteristics, Scope, Benefits and Challenges, September 5, 2019.

[9] S. Subashini and V. Kavitha, "Review: a survey on security issues in service delivery models of cloud computing", J Netw Comput Appl, 2011; vol. 34(1), pp. 1-11.

[10] A. Hasselgren, et al., "Blockchain in healthcare and health sciences—A scoping review". International Journal of Medical Informatics, 2020, vol. 134: 104040.

[11] L. Bell, W. J. Buchanan, J. Cameron, and O. Lo, "Applications of blockchain within healthcare. Blockchain in healthcare today", 2018.

[12] K. N. Griggs, et al., "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring". Journal of medical systems, 2018, vol. 42. Issue 7, pp. 1-7.

[13] N. B. A. Razak, G. Jones, M. Bhandari, M. C. Berndt, and P. Metharom, Cancer-associated thrombosis: an overview of mechanisms, risk factors, and treatment. Cancers, 2018, 10.10: 380..

[14] E. F. Coutinho, et al. "Modeling blockchain e-health systems", Proceedings of the 10th Euro-American Conference on Telematics and Information Systems. 2020.

[15] F. Yahmed and M. Abid, "Trust Execution Environment and Multi-party Computation for Blockchain e-Health Systems", International Conference on Smart Homes and Health Telematics. Springer, Cham, 2020.

[16] F. Michèle, "Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", Panel for the Future of Science and Technology EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 634.445 – July 2019 ENEPRS

[17] B. Arunkumar and G. Kousalya, "Blockchain-Based Decentralized and Secure Lightweight E-Health System for Electronic Health Records", Intelligent Systems, Technologies and Applications. Springer, Singapore, 2020. pp. 273-289.

[18] M. R. Yuce and J. Khan, eds. , "Wireless body area networks: technology, implementation, and applications", CRC Press, 2011.

[19] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria", Expert Systems with Applications, 2020, vol. 154: 113385.

[20] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-based approach for e-health data access management with privacy protection", In: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE, 2019, pp. 1-7.

[21] T. Hyla and J. Pejas, "eHealth integrity model based on permissioned blockchain", Future Internet, 2019, vol. 11.3: 76.

[22] L. Xu, A. Bagula, O. Isafiade, K. Ma, and T. Chiwewe, "Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) Platform", In: 2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K). IEEE, 2019, pp. 1-8.

[23] B. Assiri, "Using Leader Election and Blockchain in E-Health, Advances in Science", Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 46-54 (2020).

[24] M. M. Neto, E. F. Coutinho, L. O. Moreira, and J. N. de Souza, "Toward blockchain technology in iot applications: An analysis for e-health applications", In: IFIP International Internet of Things Conference. Springer, Cham, 2019, pp. 36-50.

[25] R. W. Ahmad, et al. "The role of blockchain technology in telehealth and telemedicine", International journal of medical informatics, vol. 148, 2021, 104399.

[26] S. Tessier, Operation of the blockchain and its interest for the pharmaceutical world, PhD thesis in pharmacy, UFR pharmaceutical sciences, university Bordeau, France, Sciences du Vivant, 2019, dumas-02296520

[27] U. Chelledurai, S. Pandian, and K. Ramasamy, "A blockchain based patient centric electronic health record storage and integrity management for e-Health systems", Health Policyand Technology, 2021, vol. 10, n° 4: 100513.

[28] M.S. Rahman, M. A. Islam, M. A. Uddin, and G. Stea, "A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges", Internet of Things, 2022, 100551.

[29] M. Javed, G. Ahmed, D. Mahmood, M. Raza, K. Ali., and M. Ur-Rehman, "TAEO-A thermal aware & energy optimized routing protocol for wireless body area networks", Sensors, vol. 19, n° 15, 2019, 3275.

[30] https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology

[31] https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/

[32] https://www.cdc.gov/phlp/publications/topic/hipaa.html

[33] https://www.investopedia.com/terms/b/blockchain.asp

[34] https://www.investopedia.com/terms/p/proof-work.asp

[35] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 2020, vol. 134, 104040.

[36] https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/

[37] D. P. Oyinloye, J. S. Teh, N. Jamil and M. Alawida, Blockchain consensus: An overview of alternative protocols. Symmetry, vol. 13 n° 8, 2021, 1363.

[38] A., Roehrs, C. A. Da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records", Journal of biomedical informatics, vol. 71, 2017, pp. 70-81.

[39] M. Calani, G. Denaro and A. Leporati, "Exploiting the Blockchain to Guarantee GDPR Compliance while Consents Evolve under Data Owners' Control", In ITASEC, 2021, pp. 331-343.