PUIG-SALABARRÍA S.C.

Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/

Año: XI Número: 3 Artículo no.:84 Período: 1 de mayo al 31 de agosto del 2024

TÍTULO: La tecnología blockchain, modelos e integración en el sector salud. Análisis usando revisión sistemática de la literatura.

AUTORES:

1. Dra. Liliana Avelar Sosa.
2. Máster. Arturo Iván Mendoza Arvizo.

RESUMEN: Este artículo identifica y determina los principales elementos requeridos para una arquitectura blockchain donde se mejore la gestión de los registros médicos, y se pueda estructurar un sistema que controle el acceso a los datos clínicos. Se proponen cuatros pasos principales organizados como un RoadMap. La investigación, para llegar a estos resultados, se logró siguiendo una metodología mixta con una búsqueda estructurada de literatura. Los hallazgos indican que esta tecnología es adecuada para los requisitos operativos de un hospital, convirtiéndola en una red de datos orientada al servicio y preservando la seguridad y privacidad de los datos del paciente, pudiéndose aplicar en otros sectores específicos como actividades educativas, registros estudiantiles, etc.

PALABRAS CLAVES: sistema de salud, expedientes médicos, Blockchain, protocolo de consenso.

TITLE: Blockchain technology, models, and integration in the healthcare sector. An analysis using systematic literature review.

AUTHORS:

1. PhD. Liliana Avelar Sosa.
2. Master. Arturo Iván Mendoza Arvizo.

ABSTRACT: This article identifies and determines the main elements required for a blockchain architecture where the management of medical records is improved, and a system that controls access to clinical data can be structured. Four main steps are proposed, organized as a RoadMap. The research, to reach these results, was achieved following a mixed methodology with a structured literature search. The findings indicate that this technology is suitable for the operational requirements of a hospital, turning it into a service-oriented data network and preserving the security and privacy of patient data, and can be applied in other specific sectors such as educational activities, student records, etc.

KEY WORDS: health systems, medical records, Blockchain, consensus protocol.

INTRODUCTION.

Having an accessible and immutable medical record at any time is a valuable resource that allows doctors, nurses, and administrators to make better decisions about medical treatment (Gutiérrez et al., 2018).

The United States Institute of Medicine, through its Patient Safety and Healthcare Technology (PSHI) committee, states that in the area of healthcare, there is a high degree of information exchange between the actors involved in care processes, such as patients, doctors, nurses, administrative personnel, and companies (Chou, 2012). This information, with controlled and securely stored access, is essential to provide effective treatment to patients, as well as to prevent diseases and associated adverse patient events, unnecessary expenses generated by the double formulation of drugs and tests, and the loss of time generated for patients to access their complete medical history. However, the storage and use of information, year after year, has become a challenge in the area of information technology in hospitals, a process that requires not only storage but also analysis, reading, and the possibility that the information generates an operational benefit to the institution (Ocampo, 2017).

The World Health Organization (WHO) refers to the global e-health diffusion that, when integrated into the health sector Information and Communication Technologies (ICTs) have the potential to improve the quality of care, optimize spending, and contribute to safety and equity in patient care. ICTs are defined, according to Enakrire & Ocholla (2017), as a diverse set of technological tools and resources used to communicate, create, disseminate, store and manage information.

Unfortunately, an obstacle to the adoption of medical records through ICT services is that the number and severity of cyber-attacks on medical record files are on the rise; the US Department of Health and Human Services reports more than 4,419 cases of medical record breaches between 2009 and 2021, resulting in the exposure of 314,063,189 medical records.

A way of to protect information in healthcare sector whit ICTs is the use blockchain technology (BT), which is a distributed database of digital transactions or events executed and shared among its members. Some studies provided an overview BT, emphasizing its application in industrial data (Ahram et al., 2017) and analyzed blockchain application areas and related various topics (Yli-Huumo et al., 2016). However, none adopted an approach to review the target field. This study aims to identify the key aspects to consider when structuring blockchain software selection methodologies.

Authors as Hebert and Di Cerbo (2019) provided methodologies for the selection of parts of the software structure giving the details and stages on requirements analysis and task assignment for the field of architecture development, also using threat modeling. Nonetheless, they are based on data structure, programming, functionality, and portability, therefore some elements were not included. Designing a system that uses blockchain from ground up is time-consuming, expensive, and affects the operability of the enterprise network. In summary, here attempted to answer the following questions:

(1) How can a blockchain network be integrated into a traditional medical record management system?

(2) How can the key parts of a blockchain network be chosen such that data control is fully decentralized?

(3) Which consensus protocols have been used to validate them?

This paper first presents a systematic review for design of blockchain; and then, the research streams are identified: health sector areas, processes used in this sector, and some related works. Finally, it is suggested the technical requirements for managing medical records using BT.

DEVELOPMENT.

Methodology.

For the literature review was considered the academic literature that excluded works before the year 2017, i.e. reviews or meta-analyses, doctoral theses, studies that included some type of advertising, and works written in English; the criteria was: a) original articles in English; b) research articles relevant to blockchain technology and medical records. The review was conducted in three steps: 1) Collection of information: the type of information to be collected is defined. 2) Article review: collected information in the form of articles is reviewed for information relevant to the topic of analysis and a representative view of BT and interoperability. 3) Information analysis. The aspects analyzed were the author, year of publication, title, and relevant aspects in each one. Were identified 2267 articles of which 1108 were included for the next step of analysis and of which only 160 remained important. From these and considering the objective of this research only 30 were relevant.

Results.

Here is provided the main advantages and disadvantages of relying on blockchain and smart contracts around healthcare and discuss the baseline technical requirements for an EMR management system in a blockchain-based architecture. It is considered blockchain in healthcare, types, platform, smart contracts, identity and authentication of the nodes, consensus protocol, and finally, a roadmap to follow up to structure a medical record BA.

Blockchain in healthcare.

Blockchain technology can be benefit to management of resources in hospitals. The best applications of BA within the medical sector is Guardtime, from the Estonian government; a Dutch company developed it, and its method is to create links or bridges between entities, ensuring the flow of information through the blockchain, but it is finding a balance between various conflicting system objectives, such as security versus performance, and assurance versus control (Martinovic et al., 2017). Mettler (2016) developed MedRec that was a project of the public blockchain network type, with a link management method through pointers and creating bridges between hospital service providers and patients and hospitals. Having security weaknesses assumes that their administrators ensure the integrity of the databases of participating entities (Ekblaw, 2017). Jiang et al. (2018) developed the BlocHIE application, which joins two blockchains from different areas to enrich the output information in a common access system and increases the output flow of both systems by integrating transaction packaging algorithms that hosts the data outside the blockchain, as a disadvantage remains the lack of an evaluation of the algorithm in heavy information traffic scenarios.

The application made by Rahman et al. (2019) uses blockchain on data generated by mobile devices and mainly focused on diagnosing and assessing progress in the treatment of dyslexia, which is straightforward to apply without substantial innovation changes. Mashamba-Thompson and Crayton (2020) implemented a low-cost blockchain system coupled with artificial intelligence for the treatment of infectious diseases using a data collection methodology (patient information, geographic location of the patient, and test results), but did not consider interoperability (technical, semantic, syntactic, or organizational). Therefore, there is concern about limitations due to the weakness of the technological infrastructure in the health systems in which it would operate, inadequate monitoring in the capture of information, and the lack of validation of results in a real environment. Table 1 shown the main application and development areas in the healthcare sector.

Table 1. Applications in the hearth sector with blockchain.

Name/Area	Innovation	Disadvantage
Guardtime National health coverage system.	Use of Smart card.	Bridge connection type design doesn´t included primary.
May, provider liaison and clinical services.	Strengthens interoperability semantics and syntax.	Difficulty in finding information in data bases.
MedRec liaison of hospitals, patient.	Link management method through pointers.	Not considered the integrity of data.
FHIRChain Treatment of cancer patients.	Shields data between mobile devices and, the central database.	Poor interoperability.
BlocHIE Linking two blockchains.	Increase of the flow rate throughput, combining data from two blockchains.	Lack of algorithm evaluation for integration.
SpatialBCH Child dyslexia treatment with the Internet.	Encodes Internet of thing data, including mobile systems.	The infrastructure and WIFI focused on diagnostics.
IoTeHealth Internet of things and sensors.	Integrates the Internet of Things with cloud storage and blockchain.	Slow storage algorithm, not consider interoperability.
mHealthB Self-diagnosis of infectious diseases.	Integrates mobile devices and artificial intelligence in Health self-diagnostics with blockchain.	Does not consider interoperability in its development.

Types of Blockchain.

According to the literature, three main types of blockchain have been documented and which are: public (with fewer permissions), private (with permissions) and hybrid (as a consortium) (Alhadhrami et al., 2017; Zheng et al., 2018) and detailed in Table 2.

Table 2. Spectrum of blockchain types.

Property	Public	Hybrid	Private
Consensus determination	All	Selection of a set of nodes	Only the organization
Reading access	Public	Public or restricted	Public or restricted
Immutability	Robust	Could be manipulated	Could be manipulated
Central authority	No	Partial	Conditional
Consensus process	Unrestricted	Conditional	Conditional

A public blockchain is an open type in which anyone can participate. All participants may freely access data and make transactions, but since numerous unverified users are participating, advanced encryption and verification are needed, and thus, network expansion is difficult and it is very slow (Oh & Shong, 2017), the main feature of permissionless blockchains is that the nodes that participate in maintaining the ledger do not need to be trusted or even be known to each other. That is, any user can join and participate in the network (Alharby & van Moorsel, 2020), while on a private blockchain or "authorized" blockchain requires the identity of the participant to be known. Private blockchains are optimized for specific application scenarios and rely on preexisting trust relationships; only trusted nodes are allowed to write to blockchains. Hybrid blockchain networks generally combine both private and public blockchain at the same time, under which a collection of predetermined nodes are responsible for approving blocks (Albshri et al., 2022).

For medical data, the most suitable type of blockchain would be a private one because: first, it permits only authorized nodes to join the network. These attributes allow the administration to only authorized users to participate in the network, such as physicians, administrators, and beneficiaries; second, it determines the nodes that can carry out transactions. This agrees control over nodes designated by the administration of the network to adjust and change the state of variables or transactions; third, it determines the nodes that can execute smart contracts. It makes available hospital administrators to choose network users, whether doctors, nurses, or patients, so that they can participate through contracts in the processes related to patient care and making and executing actions and decisions inherent to processes. Fourth, it indicates which nodes can act as miners, and it allows to authorize network users, who are doctors, nurses, or patients, to solve the consensus algorithm puzzle and resolve it will be the winner, who will integrate new medical transactions into the blockchain and will be rewarded with points exchangeable for benefits.

Platform.

To develop a system with blockchain technology, the questions to be solved are the frameworks that support the development; therefore, a blockchain platform should be used, its advantages and disadvantages, and the consensus used. Here three main platforms detected, its selection was based on each platform's popularity, support level, and documentation. Table 3 shows some medical applications developed that use it, and Table 4 shows a comparison of the important properties between platforms.

Table 3. Applications with platforms.

Application	**Platform**
Medrec	Ethereum
Patientory	Ethereum
ClinicAppChain	Hyperledger
MedHypChain	Hyperledger
ModelChain	Multichain

Note: A variety of platform research was consulted. Source: Own.

Ethereum is a platform that allows developers to build and use smart contract-based applications running on BT and has adapted the PoW consensus protocol. Hyperledger is an open-source project introduced in 2015 by the Linux Foundation for the development of platforms to create private blockchains with tools and programming codes for the industry and community in general. Valenta and Sandner (2017) considered it as a solution for building private platforms

Table 4. Characteristics of spectrum of blockchain types.

Property	**Ethereum**	**Hyperledger**	**Multichain**
Consensus	PoW/PoS	PBFT/Adaptable	PoA/PBFT Modified
Language	Solidity, Serpent	C++, Python, Java	Bitcoin script, C++
Transactions/sec.	15	3000	1000
Smart Contracts	Yes, Second generation	Yes, Second generation	Yes, First generation
Software development kit.	Yes	Yes	Yes

Note: A variety of platform research was consulted. Source: Own.

Ethereum is a platform that allows developers to build and use smart contract-based applications running on BT and has adapted the PoW consensus protocol. Hyperledger is an open-source project introduced in 2015 by the Linux Foundation for the development of platforms to create private blockchains with tools and programming codes for the industry and community in general. Valenta and Sandner (2017) considered it as a solution for building private platforms. It uses protocols, such as PBFT or derivatives, which do not need to incentivize mining or smart contract execution. Multichains are platforms for creating and implementing a private BA. It focuses on providing features, such as the integration and management of user permissions and enhanced data logging functions and allows an administrator user to grant permissions to new nodes in the network, such as reading, writing, and mining.

The multichain consensus mechanism adapts PoA, in which mining nodes take turns mining blocks, it valued because it implements an economic consensus mechanism in a private blockchain. In healthcare, an example of building a BA to improve electronic medical records (EMR) is the Hyperledger project, which was considered because it is required that the public cannot see the blockchain; users are limited to using a private blockchain type, and the Hyperledger has a modular architecture and provides a great deal of flexibility, allowing for confidential and secure transactions, which are required in the medical record.

Smart contracts.

When choosing a blockchain platform with which to build an application, is important the use of smart contracts (SC) that refer to computer programs/codes designed to manage smart properties within the blockchain and that is automatically executed by a software program (Magazzeni et al., 2017). A SC is developed according to characteristics of platforms, where it is important to know whether scripting functions without full programming capacity (first-generation SC) or supports any algorithm (second-generation SC). According to Thurner (2018), if they require links to external data sources to be executed, smart contracts would be non-deterministic and deterministic when they do not depend on external information, because they only rely on information from the blockchain to be activated and operate effectively.

The SC are a key factor because they are used and interpreted as a contractual relationship between doctor-patient-administration users, in which actions or events will be established that will result in a series of specific conditions depending on the user's role or those that have been agreed upon in the said contract. The Hyperledger project can generate smart contracts with a second-generation level and a high number of transactions per second, which allows us to create a fast system and automate key events. The process of identity and privacy management is designed to respond to scenarios in which participants are known and identified, as well as to support implementations that provide high degrees of confidentiality, resilience, and scalability.

Authentication of actors and processes in the hospital environment.

Architectures for electronic medical records management based on blockchain, despite all the advantages they integrate, still face problems or challenges to be solved, the main ones being: authentication is the process by which a computer system examines the identity of a user, provides a mechanism to discern and confirm the user's identity, and determines whether the user has access to and authorizes system resources (Liu & Xu, 2018). Its essence is to confirm the identity and protect legitimate users, considering that a blockchain is a P2P network, where a node is a peer and its initial function is to connect and communicate with other nodes in the network, the classification of a node within a blockchain structure will be within this list: a) Full node: operates with all attributes and permissions within the network and represents a computer that has all blockchain core client libraries installed, contains a copy of the blockchain database, creates and validates transactions, and creates and validates blocks (Ahram et al., 2017). b) Light node: perform transaction verification and do not store copies of the database. They query the status of the last block and transmit the transactions for processing.

Node authentication.

Blockchain-based identity authentication has the characteristics of a decentralized authentication, where each node in the network has two keys: a public key that is used to encrypt transactions, and a private key that is used to decrypt the content and allow a node to identify the sender. Encryption is the process of encoding the original message into a message that cannot be interpreted as the original message, while decryption is the process of changing the message that has been encoded into the original message.

Digital signature.

A digital signature is an essential component in a blockchain, as it is used to verify the authenticity of transactions and is a way to prove the authenticity of a digital message (Woda & Huzaini, 2021) and can be provide data integrity and authentication (Lee et al., 2017).

With a signature, one wants to prove that a message or contract is approved or authorized; in essence, it can be seen as a digital analog to a written signature, but with considerably stronger security guarantees. The theoretical framework of the process is framed as follows: S = (G, S, V), which encompasses three algorithms, where S is equal to the digital signature, G is key generation, S signature, and V verification. If someone generates a transaction, they must prove that they are authorized to all nodes in the system. Blockchain mining nodes have knowledge of public keys and verify the transaction conditions and validate the signature's authenticity. The flow of a transaction from the generation of the signature and its verification includes the sending or transmitting entity, receiving entity, and state change the variable or message.

The identity information of the network nodes is stored in the blockchain; therefore, it is extremely difficult to manipulate, and smart contracts to perform addition, deletion, modification, and verification operations streamline the process.

To identity assignments to actors in the medical record management process is necessary:

1) User-patient node: complete node; the main function of the user patient is to check data, request accesses they could add authorized information, and authorize doctors or other people to check their medical information.

2) Node user-doctor: complete node; the main function of the medical user is to add, delete, modify, and check data; doctors can also add medical records to patients.

3) Query user node: Light node; querying user only has a query function.

4) User administrator node: a complete node manages the accounts, keys, and permissions of users participating in the network, password recovery, and the linking of public and private keys.

Consensus protocol.

Nakamoto (2008) mentioned that a blockchain is cooperatively managed by a P2P network, integrating a consensus protocol to authenticate new blocks. The core of a blockchain is the consensus mechanism, which establishes rules for nodes in the integration of shared data (Aljassas & Sasi, 2019). The implementation of the consensus algorithm depends on the nature of the target environments, or business networks. This ensures order in transactions and guarantees the integrity and consistency of a blockchain in its distributed nodes, its algorithm is the most important factor in a blockchain system because its efficiency directly determines performance in the chain (Yang et al., 2017).

The best known because of its origin in the early days of Bitcoin cryptocurrency is the Proof of Work (PoW). In PoW, each node generate blocks by having more computational resources than others, which significantly consumes energy resources and leads to the inefficiency of integrating only one block every 10 min into the blockchain (Shen et al., 2019). Other recent blockchain platforms have used alternative mechanisms, such as Proof of Stake or Proof of importance (PoS) widely used in BT, and that uses stakes in competition to create blocks.

According to Li et al (2021), the most common consensus algorithms in blockchain systems are Proof of work (PoW), Proof of stake (PoS), Practice of Byzantine fault tolerance (PBFT), Delegated proof of stake (DPoS), Proof of authority (PoA), Proof of elapsed time (PoET), and Proof of bandwidth (PoB). Table 5 highlights the main characteristics of the consensus protocols. The consensus protocols were proposed for specific application areas, such as medicine, IoT and electric vehicles (Oyinloye et al., 2021; Yang et al., 2019) and that a quite a number of consensus protocols with good trade-offs between the consensus protocol metrics like energy consumption and throughput have been designed specifically for permissioned blockchain (Gai et al., 2018; Li et al., 2017; Yang et al., 2019). Otherwise, developing consensus protocols for blockchain that can achieve a balanced trade-off of these requirements is still an open problem.

Table 5. Summary of Consensus Protocols.

Name protocol	**Platfom**	**Concept**
Proof-of-work (PoW)	Bitcoin	Proof-of-work (PoW) is an algorithmic tool that protects networks by imposing a computational cost on participating devices.
Proof-of-stake (PoS)	Bitcoin/ Ethereum	Requires low computational resources to carry out the block testing. It is seen as an alternative to the PoW model.
Proof of Activity (PoA)	Decred	It is a combination of PoW and PoS. It ensures that the transactions are genuine and that the miners reach a consensus.
Proof-of-Interoperability (PoI)	HealthCare	Designed to leverage the effort required to achieve network consensus by verifying that incoming messages are interoperable concerning a known set of structural and semantic.
Practical Byzantine Fault Tolerance (PBFT)	HyperLedger	Has the ability of provide without the need for confirmation of the transaction. The nodes share message with each other to send a block.

Delegated Proof of Stake (DPoS)	BitShares	The term shareholder is used for participants who vote for witnesses assigned to verify transactions and produce blocks.

Note: A variety of platform research was consulted. Source: Own.

Relevant characteristics of the protocol.

Each consensus protocol has own characteristics, for example: Byzantine fault tolerance, fault tolerance, and outflow that is the ability of a computer system or algorithm to withstand Byzantine faults. This term derives from faulty nodes that have been identified into two types, one called Byzantine nodes and the other called non-Byzantine nodes, respectively. It is also known as malicious nodes and can take any action to interfere with the system to reach a consensus, such as deliberately not responding to messages or responding to messages with errors.

The Fault tolerance (CFT) is a property that allows a system to continue to function correctly if one or more of its components fail. This mechanism prevents the system from collapsing when nodes fail or are disconnected. The output flow, also throughput (transactions per second), or TPS, is the property or speed at which transactions are integrated into the blockchain; however, when designing consensus algorithms, the key points are to make the mining power sufficiently dispersed, to increase the difficulty of attackers to master most of the competitiveness, and to reduce the possibility of individual nodes or organizations rewriting the blockchain (Wan et al., 2020).

Algorithms used in blockchain based medical record system.

The consensus algorithm embodies the performance and functionality of the blockchain system and it is the most important part (Wan et al., 2020). Over the years, numerous lesser-known alternative blockchain consensus protocols have been proposed, some of which are for specific areas of application (Oyinloye et al., 2021). The core of a blockchain is the consensus mechanism, which establishes the rules for the nodes in the integration of shared data (Aljassas & Sasi, 2019).

The implementation of the consensus algorithm depends on the nature of the target environment, which showed different types of algorithms in blockchain-based medical record system implementations and its evaluation parameters. In a public blockchain accessible to everyone in a common area where everyone can become one of the participating nodes and make contributions, the most appropriate consensus algorithms are PoW, PoS, and DPoS (Kraft, 2016).

In a private blockchain, the owner or administrator has the maximum authority to change information, and the remaining nodes have limited access. The best option in this scenario is to use PBFT (Mingxiao et al., 2017) and the algorithm within a private blockchain must take into account the efficiency, cost, and Byzantine fault tolerance (BFT); therefore, PBFT using the more classical state machine scheme has become an optimal choice (Lei et al., 2018).

Roadmap proposed for the integration of a blockchain architecture.

A lack of knowledge about the decisions regarding BA emerged as one of the major reasons for companies not being willing to adopt the technology immediately (Tiwari et al., 2023). Existing research for the development process for building a blockchain based solution is mostly conceptual and focused on use-case development and early pilots; there are no clear guidelines to follow, also has a scarcity of good resources for structure an architecture.

In the academic literature, most prior studies have extensively examined the methodologies that can be implemented to decide if a company needs blockchain or not; however, once the company has decided to implement a blockchain system, it often depends only on vendors for knowledge (Ekblaw, 2017). A step-by-step guide for building a blockchain based solution for implementation in healthcare systems and how to integrate it into the businesses is summarized in Figure 1, which shows the technical requirements and steps for structuring a medical record management system using BT.

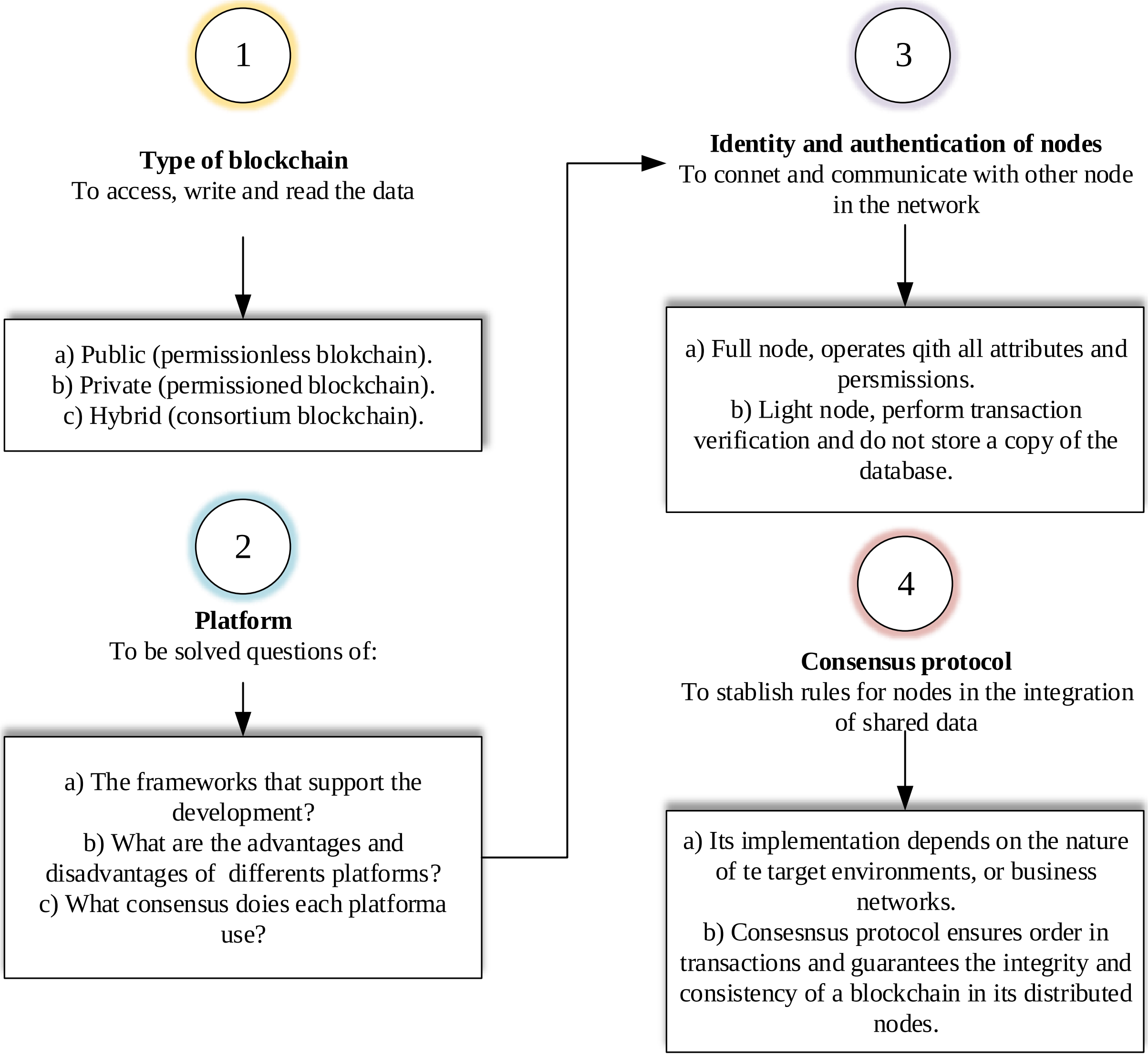
1
Type of blockchain
To access, write and read the data
a) Public (permissionless blokchain).
b) Private (permissioned blockchain).
c) Hybrid (consortium blockchain).
2
Platform
To be solved questions of:
a) The frameworks that support the development?
b) What are the advantages and disadvantages of differents platforms?
c) What consensus doies each platforma use?
3
Identity and authentication of nodes
To connet and communicate with other node in the network
a) Full node, operates qith all attributes and persmissions.
b) Light node, perform transaction verification and do not store a copy of the database.
4
Consensus protocol
To stablish rules for nodes in the integration of shared data
a) Its implementation depends on the nature of te target environments, or business networks.
b) Consesnsus protocol ensures order in transactions and guarantees the integrity and consistency of a blockchain in its distributed nodes.

Figure 1. Roadmap to structure a blockchain in the health sector. Source (Own).

Discussion.

Architectures for electronic medical records management based on blockchain, despite all the advantages they integrate, still face problems or challenges to be solved, the main ones being:

1) The high energy consumption of the architecture is mainly associated with poor development of the internal structure of the blockchain, such as the use of an inappropriate or poorly implemented consensus mechanism for the type of architecture or process, incomplete or structurally flawed algorithms, and omission of system modeling.

2) Weak access regulation, which includes deficient verification and authentication of entities requesting access to the system, contributes to the architecture's high energy consumption, forcing it to filter and verify attributes of unregistered users, consume valuable system resources, and decrease the output flow.

3) High transaction costs and increased energy consumption were correlated with decreased output flow.

4) Processing speed is also a cause-effect of an inappropriate or poorly implemented consensus mechanism for the type of architecture or process, incomplete or structurally flawed algorithms, and omission of system modeling.

5) Technical training of health personnel, in which the contributing factor is the lack of usability of the system, where the term usability is used to replace "easy to use" and defined by ISO 9241-11 as the extent to which specific users can use a product to achieve specific objectives with efficiency and satisfaction in the context of use. Usability is understood as the degree to which software is easy to use, ensuring that the system's functionalities help a user with an average ability to achieve its intended purpose.

6) Standardization is related to the lack of norms and modeling structures when designing the architecture.

CONCLUSIONS.

This article describes the potential benefits and challenges of using blockchain technology for electronic health record applications and provides some examples that including not only how blockchain works, but also its importance in the development of systems for the health sector that comply with current regulations and take a step forward in covering fundamental axes of medical history. These benefits are the privacy of information: given the nature of the type of data, personal, diagnostic, and treatment data, the actors will have the protection of the privacy rights of the records and the operations performed on them, and on the entities that perform them. The immutability: because each block contains a previous block hash, any change in a medical record will result in different data in block identification. In this way, a modification was identified, thus avoiding alteration of the data. The identity of actors: access to data must be performed only by authorized entities, with the system's capacity to manage different operations according to the type of user or node. The traceability of data: data access must always be recorded. The writing, reading, and modification of data is accessible to authorized actors in the blockchain without restrictions. Also are presented the relevant variables in this type of applications.

Some open challenges must be addressed to achieve optimal usability in a blockchain-enabled system. This paper contributes in the identification of the technical requirements for managing an EMR with BT, such as blockchain type, platform, node identity and authentication, and consensus protocols. Information that in not clear in other investigations and that does not simplify the most important requirements, it is understandable that they protect the contributions of authorship in these key respects**.** We believe that it can also be used in the education sector to manage the academic information of both public and private institutions through consensus protocols for the access of persons authorized to modify student records. It has the flexibility that medical aspects such as visits to the psychologist can be added, which is very common at the elementary, secondary, high school and university levels.

Acknowledgement.

The support granted by CONAHCYT to carry out the research project doctoral is appreciated, also to the Doctorate program in Advanced Engineering Sciences (DOCIA) of the Autonomous University of Ciudad Juárez, and the Center for Artificial Intelligence for the support granted in the research stay in 2022. The authors declare that they have not conflicts of interest.

BIBLIOGRAPHIC REFERENCES.

1. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. 2017 IEEE technology & engineering management conference (TEMSCON),
2. Albshri, A., Alzubaidi, A., Awaji, B., & Solaiman, E. (2022). Blockchain Simulators: A Systematic Mapping Study 2022 IEEE International Conference on Services Computing (SCC), https://doi.ieeecomputersociety.org/10.1109/SCC55611.2022.00049
3. Alhadhrami, Z., Alghfeli, S., Alghfeli, M., Abedlla, J. A., & Shuaib, K. (2017, 21-23 Nov. 2017). Introducing blockchains for healthcare. 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA),
4. Alharby, M., & van Moorsel, A. (2020). BlockSim: An Extensible Simulation Tool for Blockchain Systems [Methods]. Frontiers in Blockchain, 3. https://doi.org/10.3389/fbloc.2020.00028
5. Aljassas, H. M. A., & Sasi, S. (2019). Performance evaluation of proof-of-work and collatz conjecture consensus algorithms. 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS),
6. Chou, D. (2012). Health IT and Patient Safety: Building Safer Systems for Better Care. JAMA, 308(21), 2282-2282. https://doi.org/10.1001/jama.308.21.2282-a
7. Ekblaw, A. C. (2017). MedRec: blockchain for medical data access, permission management and trend analysis Massachusetts Institute of Technology]. U.S.A. http://hdl.handle.net/1721.1/109658
8. Enakrire, R. T., & Ocholla, D. N. (2017). Information and communication technologies for knowledge management in academic libraries in Nigeria and South Africa [ICT facilities; ICT services; academic libraries; university libraries; Africa; Nigeria; South Africa]. 2017, 19(1). https://doi.org/10.4102/sajim.v19i1.750

9. Gai, F., Wang, B., Deng, W., & Peng, W. (2018). Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network. In J. Pei, Y. Manolopoulos, S. Sadiq, & J. Li, Database Systems for Advanced Applications Cham.

10. Gutiérrez, O. Y. B., Saavedra, J. J., Wightman, P. M., & Salazar, A. (2018). BC-MED: Plataforma De Registros Médicos Electrónicos Sobre Tecnología Blockchain. https://doi.org/10.1109/colcomcon.2018.8466733

11. Hebert, C., & Di Cerbo, F. (2019). Secure blockchain in the enterprise: A methodology. Pervasive and Mobile Computing, 59, 101038. https://doi.org/https://doi.org/10.1016/j.pmcj.2019.101038

12. Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018). Blochie: a blockchain-based platform for healthcare information exchange. 2018 ieee international conference on smart computing (smartcomp),

13. Kraft, D. (2016). Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications, 9(2), 397-413. https://doi.org/10.1007/s12083-015-0347-x

14. Lee, B., Malik, S., Wi, S., & Lee, J.-H. (2017, 2017//). Firmware Verification of Embedded Devices Based on a Blockchain. Quality, Reliability, Security and Robustness in Heterogeneous Networks, Cham.

15. Lei, K., Zhang, Q., Xu, L., & Qi, Z. (2018). Reputation-based byzantine fault-tolerance for consortium blockchain. 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS),

16. Li, K., Li, H., Hou, H., Li, K., & Chen, Y. (2017). Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism &amp; Consortium Blockchain 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems

(HPCC/SmartCity/DSS), https://doi.ieeecomputersociety.org/10.1109/HPCC-SmartCity-DSS.2017.61

17. Li, X., Wang, Z., Leung, V. C. M., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered Data-driven Networks: A Survey and Outlook. arXiv:2101.12375. Retrieved January 01, 2021, from https://ui.adsabs.harvard.edu/abs/2021arXiv210112375L
18. Liu, L., & Xu, B. (2018, 20-22 April 2018). Research on information security technology based on blockchain. 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA),
19. Magazzeni, D., McBurney, P., & Computer, W. N. J. (2017). Validation and Verification of Smart Contracts: A Research Agenda. 50(09), 50-57. https://doi.org/10.1109/mc.2017.3571045
20. Martinovic, I., Kello, L., Sluganovic, I. J. C. f. T., & Global Affairs, U. o. O. (2017). Blockchains for governmental services: Design principles, applications, and case studies. Working Paper Series https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickelloslugano vic.pdf
21. Mashamba-Thompson, T. P., & Crayton, E. D. (2020). Blockchain and Artificial Intelligence Technology for Novel Coronavirus Disease 2019 Self-Testing. Diagnostics, 10(4), 198. https://www.mdpi.com/2075-4418/10/4/198
22. Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 1-3. https://doi.org/10.1109/HealthCom.2016.7749510
23. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2567–2572. https://doi.org/10.1109/smc.2017.8123011

24. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available at SSRN 3440802, 9. https://doi.org/http://dx.doi.org/10.2139/ssrn.3440802

25. Ocampo, C. E. (2017). Blockhain la nueva base de datos no SQL en BIG Data. https://hdl.handle.net/10901/11220.

26. Oh, J., & Shong, I. (2017). A case study on business model innovations using Blockchain: focusing on financial institutions. Asia Pacific Journal of Innovation and Entrepreneurship, 11(3), 335-344. https://doi.org/10.1108/APJIE-12-2017-038

27. Oyinloye, D. P., Teh, J. S., Jamil, N., & Alawida, M. (2021). Blockchain Consensus: An Overview of Alternative Protocols. Symmetry, 13(8), 1363. https://www.mdpi.com/2073-8994/13/8/1363

28. Rahman, M. A., Rashid, M. M., Hossain, M. S., Hassanain, E., Alhamid, M. F., & Guizani, M. (2019). Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City. IEEE Access, 7, 18611-18621. https://doi.org/10.1109/ACCESS.2019.2896065

29. Shen, N., Bernier, T., Sequeira, L., Strauss, J., Silver, M. P., Carter-Langford, A., & Wiljer, D. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. International Journal of Medical Informatics, 125, 1-12. https://doi.org/https://doi.org/10.1016/j.ijmedinf.2019.01.014

30. Thurner, T. (2018). Business innovation through Blockchain: The B perspective. foresight, 20(5), 583-584. https://doi.org/10.1108/FS-09-2018-102

31. Tiwari, S., Sharma, P., Choi, T.-M., & Lim, A. (2023). Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap. Transportation Research Part E: Logistics and Transportation Review, 170, 103012. https://doi.org/https://doi.org/10.1016/j.tre.2022.103012

32. Valenta, M., & Sandner, P. (2017). Comparison of ethereum, hyperledger fabric and corda. FSBC Working Paper, 8. http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf

33. Wan, S., Li, M., Liu, G., & Wang, C. (2020). Recent advances in consensus protocols for blockchain: a survey. Wireless Networks, 26(8), 5579-5593. https://doi.org/10.1007/s11276-019-02195-0

34. Woda, M., & Huzaini, Z. (2021). A Proposal to Use Elliptical Curves to Secure the Block in E-voting System Based on Blockchain Mechanism. In W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, & J. Kacprzyk, Theory and Engineering of Dependable Computer Systems and Networks Cham.

35. Yang, J., Onik, M. M. H., Lee, N.-Y., Ahmed, M., & Kim, C.-S. (2019). Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making. Applied Sciences, 9(7), 1370. https://www.mdpi.com/2076-3417/9/7/1370

36. Yang, Z., Zheng, K., Yang, K., & Leung, V. C. M. (2017). A blockchain-based reputation system for data credibility assessment in vehicular networks 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada. https://doi.org/10.1109/PIMRC.2017.8292724

37. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. Plos One, 11(10). https://doi.org/10.1371/journal.pone.0163477

38. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 14(4), 352-375. https://doi.org/10.1504/IJWGS.2018.095647

DATA OF THE AUTHORS.

1. **Liliana Avelar Sosa.** Doctor en Ciencias de la Ingeniería, Departamento de Ingeniería Industrial y Manufactura, Universidad Autónoma de Ciudad Juárez, Profesor Investigador. Ciudad Juárez,

México. Correo electrónico: liliana.avelar@uacj.mx ORCID: https://orcid.org/0000-0001-9490-2520

2. **Arturo Iván Mendoza Arvizo**. Maestro en Automatización y Control. Departamento de Ingeniería Industrial y Manufactura, Universidad Autónoma de Ciudad Juárez, Profesor de Medio Tiempo. Ciudad Juárez, México. Correo electrónico: arturo.arvizo@uacj.mx ORCID: https://orcid.org/0000-0002-1204-0187

RECIBIDO: 4 de enero del 2024. **APROBADO:** 13 de febrero del 2024.