# Managing medical records with blockchain

**Reginalda Santos Silva**
Universidade Salvador - UNIFACS, Brasil

**Paulo Caetano da Silva**
Universidade Salvador - UNIFACS, Brasil

**Daniel José Diaz**
Universidad Nacional de Rosario - UNR, Argentina

## Gestión de registros médicos con *blockchain*

Las aplicaciones de Internet y el uso de otras tecnologías de la información en el sector salud se denominan e-Health, cuyo objetivo es mejorar el flujo de información a través de medios electrónicos para facilitar la prestación de servicios y la gestión de los sistemas de salud. Los desafíos relacionados con el intercambio de datos médicos entre organizaciones giran en torno a la protección, confidencialidad y privacidad de los datos personales y sensibles de los pacientes (Lavina, 2018; Shi et al., 2020). Una tecnología que puede mitigar estos riesgos por sus características de transparencia, descentralización e inmutabilidad es *blockchain* (Kim et al., 2022). Por tanto, el objetivo de este trabajo es evaluar, a través de una revisión sistemática de la literatura, el uso de *blockchain* para garantizar la privacidad y seguridad de los datos en los sistemas de e-Health. La metodología adoptada se basa en las recomendaciones de (Kitchenham & Charters, 2007) y los criterios de calidad de artículos propuestos por (Dybå & Dingsøyr, 2008). Se realizaron búsquedas en 5 repositorios de trabajos científicos, que identificaron 3.214 artículos relacionados con el objetivo. Luego de realizar el proceso metodológico, resultaron 19 artículos para ser analizados. Los resultados alcanzados con este trabajo brindan una visión del estado del arte sobre el uso de *blockchain* en e-Health, indicando que el uso de esta tecnología es aún incipiente y poco aplicada en el entorno de intercambio de datos de salud. Se espera que los hallazgos logrados

https://doi.org/10.18800/contabilidad.2025ESP.001
**Contabilidad y Negocios 20 (esp.) 2025, pp. 10-47 / e-ISSN 2221-724X**

puedan ser beneficiosos para el ámbito de la atención médica para planificar y desarrollar un entorno seguro de gestión de datos de atención médica.

**Palabras clave**: *blockchain*, e-Health, EHR, registros médicos electrónicos, seguridad y privacidad

## Managing medical records with blockchain

Internet applications and the use of other information technologies in the health sector are called e-Health, which aims to improve the flow of medical information through electronic means, optimizing the provision of services and the management of health systems. The challenges related to exchanging medical data between organizations revolve around the protection, confidentiality and privacy of patients' sensitive and personal data (Lavina, 2018; Shi et al., 2020). Blockchain is an appropriate technology to mitigate these risks due to its characteristics of transparency, decentralization and immutability (Kim et al., 2022). Therefore, the goal of this work is to evaluate, through a systematic literature review (SLR), the use of blockchain to guarantee data privacy and security in e-Health systems. The methodology adopted is based on the recommendations of (Kitchenham & Charters, 2007) and the article quality criteria proposed by (Dybå & Dingsøyr, 2008). Searches were carried out in 5 scientific work repositories, which identified 3,214 articles related to the objective. After carrying out the methodological process, 19 articles resulted to be analyzed. The results achieved provide a state-of-the-art view of the use of blockchain in e-Health, indicating that the use of this technology is still incipient and little applied in the health data exchange environment. It is expected that the findings achieved can be beneficial for the healthcare domain to plan and develop a secure healthcare data management environment.

**Keywords**: blockchain, e-Health, EHR, electronic health records, security and privacy

## Gestão de registros médicos com *blockchain*

A saúde digital ou e-saúde, refere-se a aplicações web e ao uso de outras tecnologias da informação no setor da saúde e visa aprimorar o fluxo da informação médica a traves de médios eletrônicos e otimizar a prestação de serviços e a gestão de sistemas de saúde. Há desafios em manter a proteção, a confidencialidade e a privacidade das informações pessoais sensíveis dos pacientes na troca de informações médicas entre organizações (Shi et al., 2020) (Lavina, 2018). Blockchain é a tecnologia adequada para mitigar esses riscos pela sua transparência, descentralização e imutabilidade (Kim et al., 2022). Portanto, o objetivo deste artigo é avaliar, por meio de uma revisão sistemática da literatura, o uso de Blockchain para garantir a segurança e a privacidade de dados nos sistemas de saúde digital ou e-saúde. A metodologia utilizada baseia-se nas recomendações de (Kitchenham, B. e Charters, 2007) e nos critérios de qualidade para artigos de pesquisa propostos por (Dybå e Dingsøyr, 2008). Foram realizadas buscas em cinco repositórios de pesquisas científicas, e foram identificados 3.214 artigos relacionados ao objetivo. Após a

conclusão do processo metodológico, foram analisados 19 artigos. Os resultados revelam os avanços mais recentes no uso de Blockchain em saúde digital ou e-saúde, o que indica que o uso dessa tecnologia ainda é incipiente e que sua aplicação é limitada na troca de informações clínicas. Espera-se que os resultados contribuam a que haja planejamento e desenvolvimento de um ambiente seguro de gerenciamento de dados clínicos na área da saúde.

**Palavras-chave**: *blockchain, saúde digital ou e-saúde, prontuário eletrônico do paciente (PEP), segurança e privacidade*

## 1. Introduction

The use of electronic resources, technologies, and informatics can create an automated environment for the healthcare sector in which medical organizations can connect and communicate with each other. This is supported by healthcare market trends, such as the sharing of personal health records (PHR), which can help improve the accuracy of medical diagnosis and promote medical research progress. However, health data sharing is highly sensitive and must be confidential and highly secure to ensure the protection of patient medical and personal data.

E-Health systems, like Electronic Health Record (EHR), Electronic Medical Record (EMR) and PHR (e.g., public health management, patient online access, and sharing of patient medical data) have been prominent in the medical, technological, and scientific scenario. An example of this related to EHRs is the 2009 American law referring to Health Information Technology for Economic and Clinical Health (HITECH) Act (Stark, 2010). This law was enacted to encourage greater adoption of EHRs, the use of which is aimed at improving health and healthcare and other types of health information technology. An example of EHR usage is highlighted by the current scenario of the coronavirus pandemic (also known as 2019-nCoV and covid-19), where remote patient monitoring and other healthcare services have been adopted to control the situation. Many of the existing e-Health systems utilize a centralized server model, and therefore, their implementations have security and privacy limitations (Shi et al., 2020).

The healthcare infrastructure comprises several distinct segments such as hospitals, clinics, health centers, and laboratories, each generating patient medical history data that need to be stored and shared in a protected and reliable environment (Lavina, 2018). Patient data, usually stored in a centralized manner, can be susceptible to risks of loss and manipulation, which can compromise data privacy and security. Blockchain technology, on the other hand, can mitigate these risks due to its characteristics of

transparency, decentralization, and immutability (Kim et al., 2022). The use of blockchain technology can aid interoperability between systems and different healthcare organizations since data privacy and security would not be compromised, potentially creating an accessible and secure database (Lavina, 2018). Interoperability between systems facilitates transactions between different blockchain networks, allowing data sharing and transactions involving more than one blockchain network (Z. Liu et al., 2019).

Currently, there is an exponential growth in the implementation of blockchain across a wide domain of applications, including healthcare, e.g., public health management, prevention of counterfeit drugs, and clinical trials (Lavina, 2018). Considering that personal health data is so important and susceptible to privacy and security issues, blockchain fits into this context, and in various applications, such as: decentralization of patient clinical information and caregiver records, secure EHRs; health monitoring devices; medication prescription management; sharing and storage of EMRs (Huang, 2019). Blockchain can help healthcare managers and professionals with regard to data access and organization, transparency, auditability, security, privacy, service provision and interoperability of sensitive data (Elangovan et al., 2022).

The term "blockchain" emerged in 2008 with Bitcoin, described as "a system for electronic transactions without relying on third-party trust" (Nakamoto, 2008, p. 8). Blockchain can be considered as a distributed database in a decentralized peer-to-peer (P2P) network that contains a chain of chronologically ordered blocks, which can record transactions among various peers and maintain them permanently in an unchangeable and transparent manner. Additionally, information is stored using cryptographic code (Lavina, 2018; Zheng et al., 2019). Transactions are linked to cryptographic keys, where each client utilizes two keys, one private for signing the transaction (i.e., validating) and one public, allowing the system to verify the authorship (Da Silva Rodrigues & Rocha, 2021). Blockchain platforms are emerging and enable the development of applications based on their technology. Access to platforms and applications can be permissioned or permissionless. Platforms are a decentralized solution that allows tracking and documenting transactions, forming globally distributed transactional records to deter counterfeiting and fraud (Mohurle & Patil, 2017).

The problem of lack of interoperability among medical systems is described in (Gomes et al., 2022), specifically for the Unified Health System (SUS) which often processes a large amount of data (Da Silva et al., 2025). The SUS was implemented in Brazil in 1988 (Brasil, 1988), with the *Constitution of the Federative Republic of Brazil*. The analysis of medical data becomes complex due to the lack of interoperability

among current systems, whether they are from the Ministry of Health or from third parties (Brasil, 1988). In this context, some existing problems have been identified, such as: patients and other healthcare professionals not having access to care information; limitations of medical reports; regulatory issues[1]; the need for daily printing of medical reports; systems not being integrated; limitations related to the security and privacy of centralized servers; risks of improper manipulation and data loss due to centralization.

Records stored in centralized databases is a vulnerability of health data in today's healthcare systems. According to Mohurle and Patil (2017), various studies have indicated that centralization intensifies security risks and places trust in only one authority, as it can expose data to Ransomware[2] attacks that transform into cyber threats. An example of such an attack was the one that occurred at the Superior Court of Justice (Superior Tribunal de Justiça [STJ], 2020) in Brazil in November 2020. Another example of an attack was the data breach at Equifax in the US (Berghel, 2017), highlighting the vulnerability of EHR systems regarding data privacy and security (Reuters, 2019).

Furthermore, interoperability is a fundamental issue to be addressed in healthcare systems. Gomes et al. (2022) describe the problem of lack of interoperability among medical systems, specifically for the Brazilian SUS, which often processes a large amount of data. Health data in the systems are segmented, and it is not easy to share with healthcare professionals or stakeholders due to their diverse formats and standards. This situation makes it difficult to integrate and analyze patient data, hindering the applicability of data sharing in e-Health systems in emergency situations.

This work goal is to conduct an applications analysis in the healthcare sector through a systematic literature review (SLR), to infer on the challenges and benefits of security and privacy proposals related to e-Health applications using blockchain technology. The use of blockchain, with its privacy and security features, can offer several benefits to e-Health systems, such as data security, centralization of clinical information, accreditation of doctors on a single platform, easier sharing of research data, privacy, and data interoperability. It is expected that this work, based on the analysis of identified methodologies and techniques, can assist in understanding the

---

1 The regulation of the SUS is the patient's access to the services of the SUS. According to the patient's care needs, they are referred to the most suitable unit for their care. The information generated by the system directs strategic actions to solve bottlenecks and reduce queues.

2 It is an extortion software that can block a device or encrypt its contents to extort money from its owner.

implementation of blockchain for e-Health systems. Furthermore, it aims to identify an understanding of the development and implementation of e-Health systems, related to the need for detecting security features and analyzing integration with blockchain technology.

In this work, section 2 describes the theoretical framework, presenting the concepts of the technologies used such as cloud computing - InterPlanetary File System (IPFS), fundamental characteristics of blockchain, presenting consensus protocols, and describing smart contracts. It also discusses e-Health and EHR, EMR, and PHR systems. Section 3 presents related works. Section 4 describes the methodology used to conduct the SLR on existing proposals to address the EHR problems mentioned in this section. Section 5 presents the results of the review on solutions to address some EHR problems. Finally, section 6 concludes this paper and discusses its future direction.

## 2. Theoretical foundations

Health records hosted on cloud servers can be subject to intrinsic attacks, e.g., people with authorized credentials, such as database administrators or key managers, improperly accessing data, these people could be the attackers, which makes prevention substantially more difficult than external attacks. In this context, connectivity in medical equipment machines used to treat patients and store data can be attacked by cybercrimes, because of which patients can lose direct control over their PHRs and cloud services providers can have falsified or disclosed PHRs. Therefore, it is essential to have a system that is accessible only to authorized stakeholders.

The objectives of system interoperability in the health area are the standardization of e-Health systems, access to patient-controlled data, and constant transfers of health registers between different health service providers. In recent years, there has been a marked development of e-Health systems (X. Liu et al., 2019). The use of blockchain helps e-Health systems standardize, expand interoperability and preserve patient privacy; this can be monitored through smart contracts (Han et al., 2022). Therefore, alternative technologies like blockchain need to be analyzed. In addition, generally, in current systems, patients do not have authorization to access their health records, as they are managed by service providers.

In this section, the fundamental concepts of the technologies involved in the development of medical record integration are explained, they are blockchain, e-Health, and cloud computing - IPFS.

### 2.1. Blockchain fundamentals

Blockchain is a chain of chronologically ordered, shared and immutable blocks used to record transactions, increasing trust on a distributed basis among the nodes that are part of the consensus group[3]. These consensus groups are resources where validators (known as mining nodes) within a blockchain network agree with the current state of the network, are linked through a secure hash algorithm (hash) (Khan et al., 2021). The chain of blocks formed is chained to the preceding block by a reference called hash. The Genesis block initiates the chain of blocks that generate subsequent blocks, these store data from the current transaction and a copy of the previous key code (hash)[4] (Berghel, 2017). The blocks are chained by cryptography, if the information contained is changed, both it and the entire sequence of blocks will be modified, a cascade effect (Gomes et al., 2022; Khan et al., 2021; Shahnaz et al., 2019). Transactions are linked to encrypted keys, each client uses two keys, a private one that allows signing the transaction, and a public one, which allows the system to prove authorship (i.e., validate) (Da Silva Rodrigues & Rocha, 2021). Based on a network of acceptability verification, a unique encrypted key is generated for each transaction carried out, making transactions secure and immutable (Moura et al., 2020). The users themselves submit these transactions to a network of processors connected by a P2P network, they operate in the collection of transactions building and validating blocks and connecting them to a linked list (J. Zhang et al., 2020). In this way, the alteration of any data in the information chain invalidates all subsequent blocks. The mechanism creates a protected system for continuous data registration. The destruction of a node in the blockchain does not affect its integrity. As for its security and credibility, the data once verified are permanently saved in the blockchain database, making it impossible to change them (Li et al., 2021). The various essential features of blockchain technology, some of its main characteristics, and the definition of each of them are shown below (Alahmadi et al., 2021):

I. Block time or (timelock): it is the fraction of time for conception of a new block on a blockchain platform, that is, it is the time used for miners to reach consensus to admit a new block to the network, detailed in section 2.2. (Gomes et al., 2022).

---

[3] Consensus protocols perform the validation of transactions and the state of the system, synchronization of the Ledger, and protocol rules within the network.

[4] SHA-256 is the secure 256-bit Hash algorithm used for cryptographic protection. It is a mathematical algorithm whose main objective is to encode data to form a unique character string.

II. Blocks: they consist of header structures and a list of transactions. The transaction list points to the transactions executed and included in the block. The header has the hash code of the previous block and some information about the transactions carried out, it is the identifier field based on a unique value. It also adds other data, such as timestamp (records the date and time of the transaction) and nonce (a cryptographic token, created arbitrarily, used to contain replay attacks) (Agyekum et al., 2022).
III. Trust and security: blockchain is decentralized and does not depend on intermediaries and focuses on providing anonymity, security, privacy, and transparency. Trust is produced with the use of consensus protocols in which all nodes of the network validate the transaction (Erdem et al., 2019).
IV. Decentralized: blockchain facilitates record a transaction securely, traceably, and validly, decentralizing procedures, in which all transactions are cryptographically cataloged in a P2P distributed network.
V. Smart contracts: they are self-executing programs on the blockchain. They are used to establish an agreement between participants without the involvement of an intermediary, that is, the network has to have a consensus for the execution of the contract (Shah et al., 2021). Smart contracts are enabled to provide a high degree of reliability, are stored in a distributed database, and cannot be changed (Mohanta et al., 2018).

The application of blockchain technology is described as an electronic transaction system independent of third-party trust. It started with Bitcoin (Nakamoto, 2008), which recorded transactions as a distributed accounting ledger. With the evolution of blockchain, applications for other domains emerged and four types of blockchain structures were developed:

I. Public blockchain: the network operates in a transparent and open manner, with no entry restrictions, decentralized and with democratic participation. Anyone can investigate and audit the transactions carried out on the network simultaneously. However, none of the personal data or names of those involved is mentioned on the network, since the authors of these transactions are not pointed out. Examples of public blockchain are Bitcoin, Ethereum Litecoin, Monero and Zcash (Tsai et al., 2021).
II. Private or permissioned blockchain: these are blockchains where permissions are kept centralized for an organization or entity. It is geared towards the development of the business environment, banks and institutions that need to carry out a sequence of standardization and need control of data and user identity. Access is managed with private rules and with restricted access, in general the

release is executed by some password or authorization mechanism. The transactions carried out on a private blockchain are executed between its members (P2P). They hold the membership of name and identity of those involved, which makes it possible to know who carried out and what was carried out (Mughal et al., 2022; Nunes et al., 2021). Private blockchains have the advantage of tolerating many transactions. However, due to centralization, security breaches and attacks may occur (Rocha, 2021). Examples are Hyperledger (IBM), TradeLens, Corda (R3 consortium).

III. Hybrid blockchain: It is an association of both blockchains, public and private. They mix fragmented privacy models and can even use their own tokens which is the digital reproduction of a real financial asset on the network, similar to cryptocurrencies, examples of this blockchain are XRP Ledger (Ripple) and XinFin (Lamounier, 2019).

IV. Consortium or federated blockchain: this type of blockchain preserves some power of control, in addition to the characteristics of the public blockchain, such as transparency and decentralization. The consensus protocol feature is conducted by a pre-selected conglomerate of nodes, that is, entities. Organizations can define whether visibility and data sending will be restricted to network members or whether they will be made publicly available, thus controlling access and privacy of transactions. Examples of this type of blockchain are Hyperledger Fabric, Quorum and Corda (Mughal et al., 2022; Nunes et al., 2021).

Given the context presented, blockchain technology can solve problems such as interoperability of EHR systems, security, transparency, data sharing, increasing trust between healthcare providers, auditability, privacy and control of access to patient data. However, it is important to consider some challenges:

One challenge pointed out by Pimenta and Silva (2021) for applications that use blockchain is the speed of transaction execution (latency). Latency refers to the time between sending and receiving a signal. In the case of blockchain, latency is the transmission time of a transaction between the sender and the receiver. This situation particularly affects public networks such as Bitcoin and the Ethereum platform. In the healthcare field, it can affect the integrated assistance feature when including different healthcare service providers, since networks with more participants need more time to execute transactions.

Another challenge, discussed by Conceição et al. (2019), is scalability in the blockchain scenario for healthcare. Scalability refers to both the number of transactions

that the system operates and the searches that it can respond to within a given time interval. In systems that integrate different participants, such as healthcare systems (e.g. doctors, patients, hospitals, clinics, medical service providers, etc.), scalability is important for the proper functioning of the system. This is an issue that deserves attention and investigation in the implementation of EHR systems (Conceição et al., 2019).

In this scenario, there are several problems related to interoperability due to the number of outdated health information systems. However, it is necessary to overcome the challenges mentioned above, as well as the need for investments in infrastructure and the creation of models for data sharing. In addition, it is necessary to take into account the complexity of health systems and the demand for technology integration with current systems. The use of blockchain in the health field needs to evolve in infrastructure and interconnection. The integration of blockchain with health systems is critical, as many of the current systems use obsolete technologies that are incompatible with blockchain technology. This makes integration costly and complex, requiring significant investments in infrastructure (Alves et al., 2022).

### 2.2. Consensus protocol

Consensus protocols are secure and fault-tolerant mechanisms present in blockchains and are used to determine how the nodes of the network come to an agreement regarding a certain decision, that is, to ensure that the chain data that is stored in the blockchain become legitimate and are not altered. The consensus protocols agree with the verifiable state of each node of the blockchain (Berghel, 2017; Khan et al., 2021; Li et al., 2021; Mohurle & Patil, 2017). Consensus allows users or machines to organize themselves in a distributed structure to achieve data security by ensuring that members of a system can agree on a single source of truth (Erdem et al., 2019). In this way, the alteration of any data in the information chain invalidates all subsequent blocks. The mechanism creates a system for continuous invulnerable data registration. As for its security and credibility, the data once verified are permanently saved in the blockchain, making it impossible to change them. This means that a transaction cannot be modified or tampered with once it is recorded on the blockchain. That is, errors are repaired in future transactions and the past transaction (with the error) is recorded and visible to everyone who has access to the network (J. Zhang et al., 2020). Some of the consensus protocols used in the blockchain are:

I. Proof of work (PoW): a consensus mechanism that requires considerable computational effort. PoW is a fundamental part of adding new blocks to the

blockchain. Miners (name of system participants) mutually compete to add the block to the system. This "competition" occurs through the resolution of complex mathematical calculations. A new block is accepted by the network each time a miner presents a new victorious PoW (resolution), which occurs around approximately 10 minutes. As a reward, miners receive cryptocurrencies (F. Yang et al., 2019).

II. Proof of stake (PoS): the validation of a new block is defined by the amount of coins that a user or miner has on the network, that is, cryptocurrency owners validate block transactions, based on the amount of coins staked (Asif et al., 2020).
III. Proof-of-authority (PoA): it is a consensus algorithm mainly used in blockchain consortium, to directly process open transactions and verify user identity, that is, to certify that a validator is who they claim to be (Wang et al., 2022). In PoA, the rights to create blocks are given to nodes that have proven their authority to exercise it (Apla Revision, 2018). To possess this authority and the right to create blocks, this node needs to go through authentication first.
IV. Zero knowledge proof (ZKPs): it is a mechanism by which one party (the prover) can prove to another party (the verifier) that information is authentic, in opposition, the prover makes it difficult to disseminate any additional information. The protocol uses four distinct functions: "a key generator function, an input program function, a prover function and a verifier function" (Pop et al., 2020, p. 6).
V. Byzantine Fault Tolerance (BFT): it is a technique of decentralized and non-permissioned systems that are capable of successfully detecting and refusing reprehensible or defective information. The purpose of a BFT mechanism is to protect against system failures. Fault tolerance is the way for a distributed network to achieve consensus (decision about the same value) even if certain nodes in the network fail to respond or respond with false information (J. Yang et al., 2022).
VI. Zero trust architecture (ZTA): ZTA is a security approach whose principle is to never trust whoever is accessing the network before carrying out a security assessment. In this approach, no user, device or server is trusted until authentication confirms their identity. User identity and privileges are defined by access control. Access control verifies the conduct of different operations including protected resources (Syed et al., 2022). Basically, the purpose of zero trust is to allow users on an untrusted network to access trusted information through authentication and control policies. (He et al., 2022).

### 2.3. Smart contracts

Smart contracts are contracts entered into in a digital coding model provided with self-enforceability. (Kemmoe et al., 2020) considers the following objectives of a smart contract: observability (monitoring the contract performance), verifiability (execution of the document must be proven), privacy (only those responsible can have access to the execution of the processes) and applicability. A smart contract is a code that can specify norms and rules. In them, the duties, rights, and due punishments of any of the parties involved are determined, allowing reliability in the relations between the network (Muneeb et al., 2022). Smart contracts were initially created with the purpose of executing financial transactions. The following are the characteristics to create and carry out a smart contract in this context, however, these characteristics and rules are extended to other contexts:

I. The object of the contract: the terms of the contract are associated with the object. Because it implements the governance rules for some kind of business object so that they are automatically applied when the smart contract is executed.
II. Digital signatures: an agreement is signed by the contract participants using their private keys[5].
III. Contract terms: the terms of the smart contract are a chain of operations that must be signed by the participants.
IV. Decentralized platform: the smart contract is implemented and distributed among the blockchain nodes.

A smart contract is executed on the blockchain, which implies that the terms are stored in a distributed database and cannot be modified (Kemmoe et al., 2020). The contracts contain all the information about the terms of the contract between parties. The contracts are modified in the programming code. This provides the exchange of information that automatically triggers the actions provided for in the contract (Pinna et al., 2019). Transactions are also processed by the blockchain, which automates payments and counterparts (Kemmoe et al., 2020). The next step after generating the contract is to release the contract. These signed contracts are shared with the nodes on the P2P network. The node temporarily stores the hosted contract in memory waiting for a consensus to be reached (Atici, 2022).

[5] It is a secret key created during the process of asymmetric encryption. It serves to decrypt the received messages and transform them into readable information.

### 2.4. E-health and EHR, EMR and PHR systems

According to the Healthcare Information and Management Systems Society (HIMSS, 2025), e-Health are internet applications associated with other information technologies, with the purpose of improving the conditions of clinical processes, in the treatment of patients, and offering better conditions to the health system. E-Health or "digital health" aims to improve the requirements of clinical processes, surveillance, investigation and knowledge of patient treatment. Furthermore, electronic health systems improve service delivery and coordination by refining the flow of information through electronic means.

The applications used in e-Health are EMR, EHR and PHR. The doctor can consult all the patient's information and history in their medical records, enabling them to make an accurate diagnosis based on each patient's pathologies. However, these sensitive medical records can be altered or incomplete, which can stimulate users (such as doctors, research institutes and other patients) to create a wrong diagnosis, which can lead to a threat to a human being's life (Sun, Ren, et al., 2020). Thus, the concern with the privacy and confidentiality of this amount of medical data manipulated by patients and others permissioned stakeholders to use this data is manifested (Rifi et al., 2017).

The EHR is defined in "ISO/TR 20514: 2005 Health Informatics" as a standard for recording patient data electronically and in real time (International Organization for Standardization [ISO], 2005). Through EHR systems, information is provided immediately and securely, granting access to authorized users, with the aim of observing the continuity of care efficiently and benefiting integrated care. EHR data can be structured and unstructured. Unstructured EHR data (i.e., written or dictated clinical notes) is the clinical documentation that represents the patient's state. And structured EHR data can be divided into two classes. Administrative data are those that remain unchanged during the course of a clinical commitment (i.e., demographic and personal identification data) and those that change all the time (i.e., diagnoses and procedures) (Wu et al., 2017). Additionally, EHRs store a patient's complete health history, e.g., diagnoses, medications, treatments, immunization information, allergies, radiological images, and laboratory tests; it allows access to data for a certain decision making related to patient care; it automates processes and thus optimizes the workflow of professionals (Picot et al., 2020).

The EHR offers various operational benefits to organizations, as well as those related to the quality and safety of patient care and increased privacy due to the use of blockchain technology. Whereas the EMR system stores specific care data from a

particular institution, producing a limited clinical history. The PHR contains health data and information related to patient health care (Picot et al., 2020).

### 2.5. Cloud computing - IPFS

Cloud computing technology refers to the on-demand provision of IT resources via the Internet. Instead of using software or hardware services that are stored locally, technology hosted in a remote database is used. Some basic characteristics of cloud computing are rapid elasticity, multitenancy, On-demand service and pay-per-use model (Ismail et al., 2021). The physical layer consists of hardware resources, e.g. servers, storage, network, installation resources for cooling, ventilation, power, supply and basic interfaces, to support offered cloud services. The software installed in the physical layer are the components of the abstraction layer, through a software abstraction they allow access to physical resources. They are responsible for allocating and monitoring the use of physical resources (Berghel, 2017).

The IPFS is a decentralized storage protocol designed to store and share various types of files and create a hash value for each file based on its content. This way, files can be accessed based on their hash. IPFS has a mechanism that saves storage space by preventing data from being stored repeatedly (Sun, Yao, et al., 2020). Furthermore, the same distributed file system connects all computing devices. Through this protocol, files are identified by their cryptographic hash, with this, the content becomes original. This cryptographic identifier protects the data from modification, as any action to modify the data stored in IPFS can only be executed by modifying the identifier (Shahnaz et al., 2019). The data sent is authenticated, so it is classified as a self-certified system. One of the main advantages of IPFS is its network, which is composed of several connection points, that is, it is decentralized and does not depend on a single node, which makes the network much more efficient (Nunes et al., 2021). It operates using a P2P network, which includes a data structure called IPFS object, including data and links. The data is binary and unstructured, and the link consists of a matrix (Shahnaz et al., 2019).

Ortega and Monserrat (2020) report that to share the IPFS file, which contains a large volume of data, it fragments it into several interconnected blocks. These blocks are stored using a Merkle tree, which is a multi-layered data structure that links each node to a single root. Each set of data is encrypted into a hash, which results in a unique and secure content identifier (CID).

## 3. Related works

Senbekov et al. (2020) present a literature review aiming to discuss and analyze applications of artificial intelligence, big data, telemedicine, blockchain platforms and smart devices in the field of digital health. The evolution of 3D printing is discussed, as well as its application for the manufacture of organ models and implants. There is also a discussion about the difficulties of health and medical education in relation to tools and services that can integrate and restructure existing traditional systems, and they also address the issue of security and privacy in medical systems.

A literature review that researched the current scenario, design choices, limitations, and impending trends of blockchain technology-based PHRs was presented by Fang et al., (2021). The authors reveal that despite the evolution with research on PHRs and blockchain, this technology is largely in the phase of conceptual studies for application in e-Health. They point out problems with PHRs in blockchain that need to be solved such as scalability, privacy, and usability limitations.

The work of Ng et al. (2021) is a SLR with the purpose of analyzing blockchain applications in the health area, relevant and not relevant to covid-19. EMRs management, internet of things (i.e., remote monitoring or mobile health), and supply chain monitoring were three applications described for covid-19.

Mayer et al. (2020) conducted a literature review regarding the identification of problems, challenges, and advantages of blockchain applied to access management in EHR. In the review, the authors identified several limitations, such as technological limitations, adoption of suppliers, and infrastructure costs. They conclude that blockchain technology can solve problems such as EHR interoperability, trust sharing among health providers, auditability, privacy, and access control to data by patients.

The difference between this RSL and related works is the analysis of solutions based on blockchain technology to preserve privacy and security in the exchange of patients' medical data in EHRs. This RSL aimed to analyze solutions that meet security and privacy demands, showing the benefits and negative aspects of the solutions found; other works did not specifically focus on these issues.

A relevant fact about this literature review is that few works related to this topic were found, in addition to few literature reviews carried out to verify the state of the art. This was proven by the verification that most of the research carried out is guided in the integration, integrity, and access control of health records and data related to the patient. Therefore, the importance of carrying out the literature reviews presented

in this section is highlighted in order to analyze the studies found on the structures, architecture, or models using blockchain technology in the health area.

## 4. Methodology

The objective of this paper is to present a literature review on security and privacy issues for e-Health applications from the use of blockchain technology in the health domain. To identify blockchain-based solutions aimed at solving existing privacy and data security challenges in these systems, this SLR was conducted. For the development of this work, the research methodology was used according to the recommendations of (Kitchenham & Charters, 2007).

The SLR was carried out to identify works that address the use of blockchain for e-Health related to an analysis of applications in the health sector that provide a security and privacy solution regarding the applications of the integration of health records, whose goals were to provide elements for the exhibition of research data, discover the most suitable system for data collection and analysis, know the available studies related to the main theme of this work. In addition, to collect fundamental information for the elaboration of the possibilities of research questions. The search strategy included electronic databases and manual searches in conference proceedings. The search strings for the research question were structured as follows:

- Identify keywords.
- The execution of the research was carried out from the search of the terms inserted in the search strings.
- Perform empirical research with the candidate search strings, using the repositories: IEEE Xplore (Institute of Electrical and Electronics Engineers [IEEE], 2025), ACM Digital Library (Association for Computing Machinery [ACM], 2025), ScienceDirect (Elsevier, 2025), Capes Periodicals (Capes, 2024) and the National Library of Medicine (n. d.).

As a result of using the methodology, the search string presented in table 1 was established.

**Table 1.** *Search string*

| | Search strings |
|---|---|
| CP1 | (“Blockchain”) AND (“Security and Privacy” OR “Security” OR “Privacy”) AND (“e-Health”). |
| CP2 | (“Blockchain”) AND (“Architecture” OR “Software Architecture”) AND (“e-Health”). |

### 4.1. Inclusion and exclusion criteria

To obtain accurate research results, inclusion criteria (IC) and exclusion criteria (EC) were defined, which can be seen in Table 2. All studies that were delimited in the EC were classified as ineligible immediately. The adopted criteria were:

**Table 2.** *Inclusion and exclusion*

| | IC |
|---|---|
| IC1 | Works published in the period (2016-2023) |
| IC2 | The title must contain at least one of the keywords of the work |
| IC3 | Articles published in a conference or scientific journal |
| IC4 | Title, abstract and full text must be correlated with the theme of this work |
| **EC** | |
| EC1 | Duplicate work |
| EC2 | The proposed solution was not outlined for e-Health, EHR, EMR and PHR. |
| EC3 | Full text cannot be accessed in repositories |

### 4.2. Selection of articles

In addition to the preliminary selection criteria, it is essential to perform a quality assessment on the identified works. However, there is no defined quality standard for the selection of related works. Therefore, the concordance guidelines (Kitchenham & Charters, 2007) were used, which propose that a research quality is one that generates reliable results and produces results to avoid systematic errors. After defining the quality of the studies, the criteria proposed by (Dybå & Dingsøyr, 2008) were used. For this, it was applied through the definition of quality assessment questions, then criteria were determined to investigate the quality pointed out in the articles and that met at least 70% of the following questions. These criteria are presented in table 3.

**Table 3.** *Quality criterion used in RSL*

| ID | Quiz | Aspects |
|---|---|---|
| CQ1 | Is the solution clearly detailed? | Rigidity |
| CQ2 | Is there a clear description of the scope of the proposed solution? | Rigidity |
| CQ3 | Are the research objectives and motivation clearly defined? | Rigidity |
| CQ4 | Did the authors present a real case? | Relevance |
| CQ5 | Is there an evaluation and validation process, as well as a statement of the results achieved? | Relevance |
| CQ6 | Did the study identify a scenario to evaluate the application? | Relevance |
| CQ7 | Do the authors describe the main problems that can be solved with blockchain? | Relevance |
| CQ8 | Does the study have value for research or practice? | Credibility |
| CQ9 | The authors cite what benefits were achieved with the application of blockchain in e-Health systems. | Credibility |
| CQ10 | Does the study describe what types of blockchain technologies were used? | Credibility |

The works were analyzed according to the specifications of (Dybå & Dingsøyr 2008) and each article was assigned a grade to pass the quality assessment. For each question in the questionnaire, table 7, score 1 was given, totaling 10 points. Although most of the articles did not fully satisfy all 10 questions of the evaluation, it was established as a cut-off grade article with a minimum grade 7, considered to be fully evaluated. Some articles obtained a grade below 7 points, which indicates that some of the criteria were not met, among them the most common were the absence of real applications of blockchain technology, clear identification of the problems to be solved with the technology and the adequate description of the results achieved with the application of this technology, resulting in a limitation of the study. In addition to the articles with a grade lower than the cut-off grade, some studies that achieved a grade above 7 showed some contradictions in their evaluation, (i.e., the way the results were described). In addition, a small number of studies showed limitations of the proposed projects, in which a project solution was modeled, but there was no execution of it.

The analysis of the quality criteria of the works was carried out in accordance with table 4. To apply the grade, the quality issues were classified based on the scoring matrix illustrated in table 4.

**Table 4.** *Scoring matrix*

| Criteria | Article evaluation | note |
|---|---|---|
| Excellent | Relevant, coherent conclusion. | 10 |
| Good | Relevant. | Between 8 and 9 |
| Average | Simple but coherent discussion | 7 |
| Poor | Weak discussion and disconnected conclusions | Below 7 |

During the selection process, the articles that were selected for quality analysis were read by all authors and the evaluation was carried out through discussions until a consensus was reached. The base collection of studies was achieved based on the application of search string. Automatic search results returned 3.214 works distributed in the search repositories: 232 in Semantic Scholar, 1.059 in Science Direct, 71 in IEEE Xplore, 1.164 in the National Library of Medicine, 451 in Capes Periodicals and 237 in the ACM. However, not all papers were completely related to the research topic, as they went through an elimination procedure, in which each analysis and decision-making delimits the group of original articles.

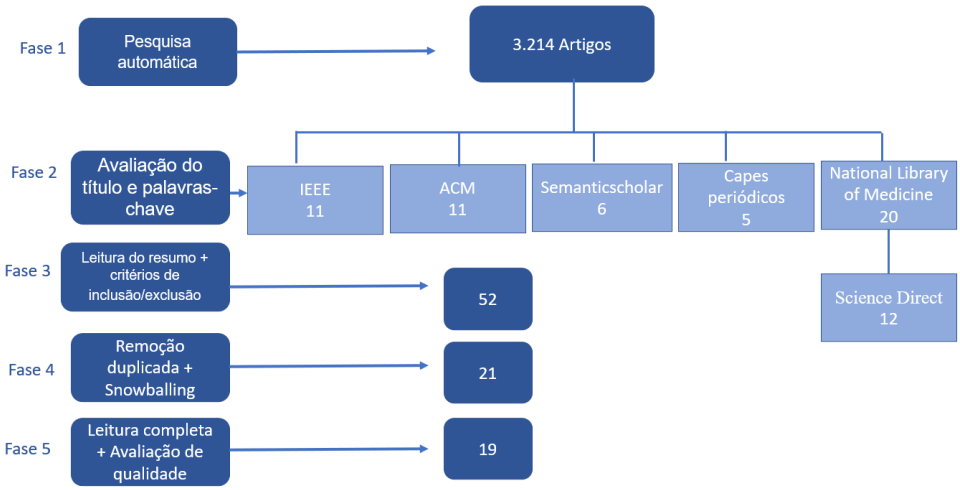
In the first screening stage, the articles were analyzed based only on the title and keywords, using the IC and EC. 52 articles were pre-selected in this stage were cataloged, on the Parsifal (2021) platform, recording the following information: abstract, authors, title, repository, year.

The IC and EC criteria were then applied again by reading the abstracts. In some cases, it was difficult to identify whether the article was aligned with the objective of this systematic review. In this scenario, the articles were kept for a new evaluation in the next stages. For better refinement, the EC were also used at this stage, since their use in the previous stage was applied only to the title and keywords. After this phase, the 52 articles selected in the previous stage were kept and included in the Mendeley® reference management tool.

The subsequent step excluded 27 duplicate papers. In addition, the snowball technique was used to manually include other papers. This technique allows selecting articles from reference lists or citations of other papers (Wohlin, 2014). At the end of this step, 21 papers remained.

Finally, the papers were read in full, with the inclusion and EC being applied again, in an even broader manner. A more detailed investigation was carried out with an assessment of the quality of the papers, resulting in the selection of 19 papers. Figure 1 illustrates this entire process of searching and selecting papers.

**Figure 1.** *Search strategy and results*




## 5. Analysis of the proposed solutions for EHR systems

Kim et al. (2022) proposed a PHR application based on blockchain technology and user experience with the aim of preventing personal data from being tampered with. Through the application, patients can manage their own data and connect at anytime and anywhere to check their medical record data that are gathered through different channels. In addition, they can count on the following benefits: restrict the duality of diagnoses and medical prescriptions, life quality refinement through "health management services and the exchange of medical information between hospitals" (Kim et al., 2022, p. 1).

Cernian et al. 2020 presents an approach based on blockchain technology called PatientDataChain, aiming at the interoperability of the intrinsic sensors of various wearable devices, enabling the collection of unique data from patients' medical records in the PHR system. Connecting different healthcare providers, where the collected data are attached to a single system of confidential health records PHR. The approach has advantages of data confidentiality and privacy and simultaneously in offering secure access to patients' medical records (Cernian et al., 2020).

Xiao et al. (2021) HealthChain proposal sought to address security and privacy issues in EHRs and the lack of system integration. The project differs from other blockchain for EHR because the HealthChain is a consortium blockchain that is the combination

between hospitals, insurers and government agencies thus forming the consortium. HealthChain is based on a governance standard, therefore, the interaction of users with the blockchain can be determined according to the principles of access control, i.e., access is restricted to authorized people. In addition, HealthChain has characteristics of blockchain technology, e.g. immutability and transparency, this means that when EHR data are inserted in the list chained by hash[6] there is no possibility of being altered. HealthChain employs the Transport Layer Security (TLS) protocol that allows both parties to detect, authenticate and converse respectively with data confidentiality and integrity.

Nunes et al. (2021) describes the analysis of the SUS[7] regarding medical data, sensitive patient data, reports, diagnoses and medical prescriptions that are stored in an electronic environment. The current system model is centralized, which they consider inappropriate for storing this critical data. So, in this scenario, the authors propose a different system from the current one, the proposal of a decentralized medical data system adaptable to the General Data Protection Law (LGPD) (Brazil, 2018), using the IPFS, blockchain and Pretty Good Privacy (OpenPGP) cryptography that works through asymmetric keys. The proposal of the decentralized system to preserve privacy and assist in the access of medical data by permitted institutions, health professionals to health server bodies, would provide transparency, integrity, integration and security in the system currently used by the SUS.

Medicalchain is a company that works with healthcare providers to run blockchain-based medical records. To build the Medicalchain solution, they used two blockchain frameworks. The first framework uses Hyperledger Fabric to control access to health records. The second framework, used as the basis for all applications and services on the platform, is based on Ethereum's ERC20 token. Ethereum is an open-source decentralized platform that allows the sending of cryptocurrencies to some users at the cost of a small fee of the currency (Ether). The Medicalchain payment system works with the use of tokens called "MedTokens", issued by the platform to patients. Tokens allow patients to perform certain tasks, e.g. register their data on the blockchain, pay for services on the platform, use third-party applications (Capece & Lorenzi, 2020).

Stamatellis et al. (2020) propose the Privacy-Preserving Healthcare (PreHealth), an approach that has the capacity to use in the storage of EHRs, ensuring patient privacy using the structure of the permissioned blockchain technology of Hyperledger

6 SHA-256 Secure Hash Algorithm.

7 Check footnote 2.

Fabric, and an Identity Mixer (Idemix) which is a cryptography protocol based on proof of knowledge, the ZKP, which offers a privacy protection mechanism, such as anonymity and unlinking. PreHealth can be used by patients or other health agents. With the capacity to accommodate patient records efficiently, enabling anonymity and disassociation. In addition, it provides pillars for secure auditing, protection of the privacy of sensitive data collected. The advantage of PreHealth is the privacy protection features that are following General Data Protection Regulation (GDPR) (Intersoft Consulting, n. d.).

A smart contract-based architecture, called SmartMed Chain, has been developed for a Smart Healthcare (S-Healthcare) environment. The structure uses Hyperledger Fabric and data is stored on IPFS. The system is to protect the sharing of health data among different stakeholders. Patients can access the upload and reading of their EHRs, as well as s-healthcare providers can upload and read these generated EHRs. Furthermore, in relation to patient choices and in accordance with relevant privacy laws, S-Healthcare stakeholders may incorporate supervision of the service application with a privacy agreement management scheme (El Majdoubi et al., 2021).

Hussien et al. (2021) presents a study related to the failures of PHRs technology and blockchain technology applied to health, such as difficulties with privacy and the storage capacity of the blockchain. In addition, the data is exposed to everyone on the network due to its transparency and decentralization and for specific applications it becomes inadequate. So, to solve these limitations, the authors propose a user attribute-based access control (ABAC) scheme. The encryption is based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) text policy attribute and searchable symmetric encryption (SSE), and the use of smart contracts. The purpose of access control is to achieve an attribute of the CP-ABE access structure policy and ensure that medical data is only accessed through user attribute matching. The encryption used is based on text policy attributes and SSE, which associated with smart contract technology aims to achieve security in data access control and external encrypted data.

A remote patient monitoring system, called mHealth, was developed by Taralunga and Florea (2021) based on Ethereum to share and interpret medical data, where wearable sensors are devices that allow capturing a series of health information (e.g. behavior, vital signs, activity), in addition to facilitating communication with a smart device (i.e., smartphone or smart tablet) using a P2P hypermedia protocol, the IPFS, for the distributed storage of health-related data. Data research, access to patient data by health professionals, the recording of diagnoses, treatments and therapies and the issuance of warnings to patients and medical professionals are all created in

smart contracts. The approach has the advantage that only health professionals are represented in the blockchain network nodes and thus exchanging a centralized EHR database for a distributed database.

Dubovitskaya et al. (2017) state that many EHRs are regularly shared between healthcare professionals, pharmacies, and patients for clinical diagnosis and treatment. Therefore, they proposed scenarios of health data management applications based on blockchain technology in different health sectors (e.g. primary care, medical data research and connected health), especially for sharing EMR data among health providers and for research studies. In addition, the proposal of a structure to manage and share EMR data for patient care with cancer. For the implementation of the structure, they partnered with Stony Brook University Hospital, producing a prototype that ensures privacy, security, availability, and enhanced access control related to EMR data. Enabling a considerable reduction in response time for EMR sharing.

Sun, Yao, et al. (2020) presented a proposal for a searchable scheme of distributed EMRs based on blockchain technology. The integrity and authenticity of electronic medical data are presumed through a hash calculation that is stored in the blockchain, and then these data are encrypted and stored in the IPFS system. The association of IPFS and blockchain allows to process large volumes of data by doctors, suppressing the demand to store them in the blockchain, and thus saves network bandwidth in blockchain. These encrypted EMR data are housed in the Ethereum blockchain, implemented by a smart contract. To ensure that only the attributes that have access policy are able to decipher the encrypted electronic medical records.

Abunadi and R. L. Kumar (2021) propose an access control framework called BSF-EHR to maintain data consistency and protect patient privacy. The goal of this framework is to grant permission to authorized parties (e.g., physicians, insurance agents) to share healthcare data on the blockchain, preventing unauthorized access and external attacks. The BSF-EHR proposal is made up of five parts: “the patient, the doctor, the insurance agent, the EHR server, and the data verifier” (Abunadi & Kumar, 2021, p. 4). For access control, the authors applied smart contracts on the Ethereum platform. Each patient has access to their own EHR data. Similarly, the physician can only view the EMRs of patients who have received treatment and whose electronic records can only be accessed with authorization. Likewise, the insurance agent can only view the care of patients with authorization granted.

MedRec is a Ethereum platform that controls the “authentication, confidentiality, accountability, and data sharing” of EHRs, where patient data can be stored and obtained by different institutions, people, and health professionals (Azaria et al.,

2016, p. 26). Its modular design fits into the data storage of providers, contributing to interoperability making the system suitable and flexible. MedRec has a failover model (fault tolerance), with several entities that are part of the system to avoid a single point of failure. MedRec stores medical records locally in separate provider and patient databases, each node stores copies of the authorization data in the network. However, according to the authors, MedRec does not address the security of individual databases, since local security management must be ensured by the specific system administrator. In addition, it also does not solve the problem of digital rights management. The system is governed by external regulation, Health Insurance Portability and Accountability Act (HIPAA)[8] (Azaria et al., 2016).

Tuler De Oliveira et al. (2022) propose an ABAC system for sharing medical records among organizations, called SmartAccess. The work aims at the control of data access in organizations through the ABAC model. It uses smart contracts and private and permissioned blockchain. SmartAccess has as reference the architecture established by the XACML (XML Access Control Markup Language)[9] standard and implements the ABAC components as smart contracts. Policies are managed and defined by the controllers in the blockchain network.

Zhang et al. (2018) presents the FHIRChain for data sharing based on the FHIR (Fast Healthcare Interoperability Resources) standard, it is a standard for health information exchange. Five basic interoperability requirements are addressed by FHIRChain: secure data exchange, consistent data formats, user identification and authentication, authorized access to data, and system modularity. A smart contract that manages a token for controlling access to data. Access tokens use asymmetric cryptography that encrypts the addresses of data off-chain. The proposed framework uses users' digital health identities to encrypt the content, so that only users who have the private keys of the digital identity can decipher the content.

Dagher et al. (2018) presents the Ancile platform, an EMRs interoperability system using smart contracts based on the Ethereum blockchain, preserving the privacy of patient data. Blockchain adoption through smart contracts speeds up processes and reduces manual record-keeping costs. Smart contracts automatically execute specific actions when predefined conditions are met.

---

8 HIPAA is a set of standards that American health organizations must comply with to protect information.

9 XACML (Extensible Access Control Markup Language) is an XML-based language for access control policy, designed to present security policies and access requests to information.

The HealthyBlock architecture proposed by Gutiérrez et al. (2020) considers different clinical providers for unification of EMR systems; data recovery when there is a connectivity failure. HealthyBlock has usability, security and privacy features. A prototype of the HealthyBlock architecture was implemented for patient care in a hospital network. The results of the analysis revealed high efficacy in preserving the unified, updated, and secure EMRs of patients. The authors highlight that the need for storage can quickly grow, as it encompasses the records of all patients in the hospital network. According to the authors, the advantages of security and accessibility outweigh the cost of storage.

Haritha and Anitha (2023) propose a mechanism based on Ethereum blockchain that encompasses the lattice-based access control (LBAC)[10] model and smart contracts to ensure the security of the interaction between the combination of objects (documents, files, databases, folders etc.') and subjects ('developers, users, processes, etc.'). Only where authorized users can access, security requirements (e.g. security analysis, authorization policies, and transaction policies) are enforced by LBAC. The requirement may be limited to changes where users are authorized as 'true', this means that the user is trusted if the mechanism certifies that he has access permission. The authors describe that the proposed system, compared to benchmarking methods, preserves privacy, maintains transparency, provides an authentication process and data integrity, and provides access control security.

An access control system, called LightMED, was proposed by Fugkeaw et al. (2023). The system enables sharing of medical record data in a blockchain-integrated fog computing environment using CP-ABE. They included a signature algorithm to handle authentication derived from records collected from IoT devices, which according to the authors is not supported by most current CP-ABE schemes. They describe that several fog nodes are established to execute the CP-ABE encryption and implement the connection with the cloud server and blockchain. This improves communication and reduces the cost of outsourcing data computation. Furthermore, for fog nodes to encrypt data without revealing the content of the policy, an attribute tree-based encryption is applied to maintain the privacy of the access policy while it is sent to the fog node. To encrypt data from IoT devices and decrypt it after receiving it, two algorithms have been proposed. According to the authors, the application of these two algorithms can prevent patient data from being improperly exposed (Fugkeaw et al., 2023).

[10] LBAC is an access control model based on the relationship between a combination of objects (such as resources, computers, and applications) and subjects (such as users, groups, or organizations).

For better understanding, a summary of the solutions analyzed, and some related characteristics were shown in Table 5.

**Table 5.** *Summary of solutions found*

| Selected studies | Category | Author | Observations |
|---|---|---|---|
| Aplicativo PHR | Access control | Kim et al. (2022) | The app's strength is to prevent personal data from being tampered with. However, in the study, the authors report that the satisfaction or feasibility of each function of the application was not verified. |
| PatientDataChain | Access control | Cernian et al. (2020) | In the proof of concept, the proposal proved the feasibility of the model in the integration of varied PHRs and scalability for many users. |
| HealthChain | EHR storage system | Xiao et al. (2021) | Immutable, permissioned, scalable, HIPAA-compliant, privacy rule, and security rule, and performs well. However, two disadvantages were discussed. "First, the single orderer causes a single point of failure. If the orderer fails, EHR transactions cannot be ordered into a block, causing the entire system to fail, as read latency increases with the growth of the blockchain" (p. 2). |
| Decentralized model using IPFS | Analysis of proposal for the SUS | Nunes et al. (2021) | The proposal presented is a study and there was no execution of the project to prove the proposal. |
| Medicalchain | Healthcare providers | Capece and Lorenzi (2020) | It presents Medicalchain with a proposal based on two blockchain frameworks and a payment system. |
| PreHealth | EHR storage system | Stamatellis et al. (2020) | According to the proof of concept, PreHealth ensures privacy and, simultaneously, less overhead in queries with a high volume of stored data. |
| SmartMed Chain | Data sharing architecture | El Majdoubi et al. (2021) | SmartMed Chain has proven to be efficient in ensuring security, privacy, confidentiality, integrity and scalability requirements for health data. |

| Selected studies | Category | Author | Observations |
|---|---|---|---|
| Criptografia pesquisável SC-ABSE | Access control | Hussien et al. (2021) | The proposal achieves an increased level of security with lower computation, storage and communication costs. |
| MedRec | Access control | Azaria et al. (2016) | The implementation is based on the permissionless blockchain and PoW protocol, which has transaction fees and requires "mining" processes and account management. |
| mHealth remote patient monitoring system | mHealth remote patient monitoring system | Taralunga and Florea (2021) | A remote patient monitoring system, called mHealth, based on Ethereum to share and interpret medical data, using wearable sensors to capture a series of health information. |
| Healthcare data management application scenarios | Framework for managing and sharing EMR data | Dubovitskaya et al. (2017) | The storage is cloud-based, and encryption and key sharing is applied to ensure data availability, even if the hospital node is momentarily offline. |
| Searchable schema for distributed EMRs | Storage system | Sun, Ren; et al. (2020) | The proposal showed lower costs in the implementation of contracts for sharing EMRs and is acceptable to users. Although in the call of some of the functions in the smart contract the cost can increase according to a larger volume of medical records. Despite this, they consider the increase irrelevant and the scheme viable. |
| BSF-EHR structure | Access control | Abunadi and Kumar (2021) | In the experimental results, the BSF-EHR access control system showed security and privacy protection in sharing EHRs data between users. |
| SmartAcces | Access control | Tuler de Oliveira et al. (2022) | Conducting the SmartAccess proof of concept has proven its feasibility. In which the "complexity and scalability of the functions of the contracts and measuring the latency and throughput of transactions." (p. 17). The results regarding the overhead when performing the SmartAccess functions were acceptable. |

| Selected studies | Category | Author | Observations |
|---|---|---|---|
| FHIRChain | Data sharing system between doctors and researchers | P. Zhang et al. (2018) | Some limitations of the FHIRChain prototype were discussed: "Does not address semantic interoperability, may not be compatible with legacy systems that do not support FHIR, cannot control clinical negligence, DApp deployment costs." (p. 275). However, to solve these limitations, the implementation of the DApp on a consortium blockchain platform is proposed as a future work. |
| Ancile | Access control | Dagher et al. (2018) | Ancile provides privacy preservation and data integrity. It is designed to be implemented on existing systems and uses the Ethereum platform. |
| HealthyBlock | Unified EMR system | Gutiérrez et al. (2020) | One element evaluated in performance tests when programming the HealthyBlock architecture is the synchronizer. It is the core of the system, because of its function in preserving the integrity of the system data. It has a high impact on system latency. |
| LBAC model | Access control | Harittha and Anitha (2023) | They use smart contracts to ensure secure access control to data while preserving privacy. However, there are some limitations, such as focusing only on the development of multi-level security. |
| LightMED | Access control | Fugkeaw et al. (2023) | The performance of LightMED experiments and results showed that the cryptographic operations achieved considerable throughput, and the scheme was effective and extremely scalable. However, some issues related to user and attribute revocation were not fully addressed and are considered as priorities for further development and research. |

## 6. Conclusions

This SLR took place through the main information regarding the application of blockchain in the health area. In all the chosen studies, the impact of technology is considered promising. Data security and data ownership, according to Huang (2019), are two

important issues that need to be addressed, he considers that blockchain can be the solution to these issues. It can be applied to the access and sharing of patient medical records. Access to medical records can be complex as they may be spread across various health entities. Therefore, blockchain allows patients to have full and secure access to all their records and medical history.

Regarding the application proposals discovered in the literature, the application of IPFS was the most explored use case. The presented works adopted the use of blockchain based on smart contracts and IPFS. Mechanisms such as encryption protocol were used to ensure privacy, secrecy, and security in the storage of medical records, in the control of access to patient data, as well as to other health professionals and outsourced. Some works used the permissioned blockchain from Hyperledger Fabric and Ethereum. Others used the consortium type blockchain. It also verified the use of several protocols such as ZKPs, PoW, PoS, PoA. In most of the works, the use of the decentralized storage protocol IPFS. In addition to the security features of blockchain, encryption was added to further enhance security, such as CP-ABE, SSE, and OpenPGP.

A relevant fact is that few works are related to the ZTA[11], the combination of blockchain with ZTA is still little explored in the literature, probably because it is a new technology. The analysis of the articles found in this literature review points to relevant facts, such as the trend of adopting blockchain in EHR systems. Another aspect identified is that most of the proposed solutions depend on storing the data directly on the blockchain, which is not scalable, other solutions propose off-chain storage, which are not completely decentralized or congruent with the blockchain.

This literature review identified only works related to applications in the health area and the technical subjects that were discussed in this review may need to be reviewed. Therefore, if it is necessary to examine some project decision pointed out in the works, it is interesting to reexamine the literature on the subject without restricting the search to the health domain.

This literature review contributed to presenting solutions for the healthcare sector, highlighting issues related to privacy and security in the sharing of EHR systems. This literature review identified the need to address some gaps in future work, e.g. issues of scalability, latency and integration of an architectural model that preserves the privacy and security of patient data in EHR systems. It is intended to present an archi-

[11] ZTA is an enterprise cybersecurity architecture based on zero trust standards and designed to block data breaches. The ZTA approach is primarily focused on protecting data and services.

tecture based on the combination of blockchain technology that integrates the principles of ZTA to solve security and privacy problems related to medical records sharing and storage.

**Author contributions:**

**Silva, R. S.:** Conceptualization, Validation, Investigation, Data curation, Writing, review. **Silva, P. C.:** Conceptualization, Methodology, Validation, Writing – original draft, Writing, review, and editing, Supervision, Project administration. **Diaz, D. J.:** Conceptualization, Methodology, Validation, Writing, review, and editing, Supervision.

Reginalda Santos Silva (Silva, R. S.)

Paulo Caetano da Silva (Silva, P. C.)

Daniel Josè Diaz (Diaz, D. J.)

**Conflict of interest statement**

Authors declare that, throughout the research process, there has not been any sort of personal, professional, or economic interest that may have influenced the researchers' judgement and/or actions during the elaboration and publication of this article.

## References

Abunadi, I., & Kumar, R. (2021). BSF-EHR: Blockchain security framework for Electronic Health Records of patients. *Sensors*, *21*(8), 1-10. https://doi.org/10.3390/s21082865

Agyekum, K. O.-B. O., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., & Gao, J. (2022). A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain. *IEEE Systems Journal*, *16*(1), 1685–1696. https://doi.org/10.1109/JSYST.2021.3076759

Alahmadi, D. H., Baothman, F. A., Alrajhi, M. M., Alshahrani, F. S., & Albalawi, H. Z. (2021). Comparative analysis of blockchain technology to support digital transformation in ports and shipping. *Journal of Intelligent Systems*, *31*(1), 55-69. https://doi.org/10.1515/jisys-2021-0131

Alves, C. J. R., dos Reis, L. T. P., Neto, L. R., da Silva, D. O., & Da Costa, C. A. (2022). Blockchain em Saúde: uma análise de pesquisas na base Scopus. *Journal of Health Informatics*, *14*, 110-116. https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935

Apla Revision. (2018). Proof-of-authority consensus. https://apla.readthedocs.io/en/latest/concepts/consensus.html#proof-of-authority-consensus

Asif, R., Ghanem, K., & Irvine, J. (2020). Proof-of-PUF enabled blockchain: Concurrent data and device security for internet-of-energy. *Sensors*, *21*(1), 1-32. https://doi.org/10.3390/s21010028

Association for Computing Machinery. (2025). *ACM Digital Library*. https://dl.acm.org/

Atici, G. (2022). A review on blockchain governance. In G. M. Mantovani, A. Kostyuk, & D. Govorun (Eds.), *Corporate governance: Theory and practice* (pp. 128-133). Palgrave Finance. https://doi.org/10.22495/cgtapp23

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In I. Awan, & M. Younas (Eds.), *2016 2nd International Conference on Open and Big Data (OBD)* (pp. 25-30). IEEE. https://doi.org/10.1109/OBD.2016.11

Berghel, H. (2017). Equifax and the latest round of identity theft roulette. *Computer*, *50*(12), 72-76. https://doi.org/10.1109/MC.2017.4451227

Brasil. (1988). *Constituição da República Federativa do Brasil De 1988*. https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

Capece, G., & Lorenzi, F. (2020). Blockchain and healthcare: Opportunities and prospects for the EHR. *Sustainability*, *12*(22), 1-32. https://doi.org/10.3390/su12229693

Capes. (2024). Portal de Periódicos da Capes. https://www-periodicos-capes-gov.br/

Cernian, A., Tiganoaia, B., Sacala, I., Pavel, A., & Iftemi, A. (2020). PatientDataChain: A blockchain-based approach to integrate personal health records. *Sensors*, *20*(22), 1-24. https://doi.org/10.3390/s20226538

Conceição, A. F. da, Rocha, V., & Moreira, P. R. F. de. (2019). Blockchain e aplicações em saúde. In N. Castro Fernandes, A. Ziviani, & D. C. Muchaluat Saade (Eds.), *Mini-cursos do XIX Simpósio Brasileiro de Computação Aplicada à Saúde* (pp. 1-50). Sociedade Brasileira de Computação (SBC).

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of Electronic Health Records using blockchain technology. *Sustainable Cities and Society*, *39*, 283-297. https://doi.org/10.1016/j.scs.2018.02.014

Da Silva Costa, M. V., Castro Santos Camargos, M., Nunes Viana, S. M., & Vieira de Souza Mendes, U. (2025). Avanços e desafios da interoperabilidade no Sistema Único de Saúde. *Journal of Health Informatics*, *17*(1), 1-6. https://doi.org/10.59681/2175-4411.v17.2025.1112

Da Silva Rodrigues, C. K., & Rocha, V. (2021). Towards blockchain for suitable efficiency and data integrity of iot ecosystem transactions. *IEEE Latin America Transactions*, *19*(7), 1199-1206. https://doi.org/10.1109/TLA.2021.9461849

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. In American Medical Informatics Association (Ed.), *AMIA 2017 Annual Symposium Proceedings* (pp. 650-659). American Medical Informatics Association. https://doi.org/10.48550/arXiv.1709.06528

Dybå, T., & Dingsøyr, T. (2008). Empirical studies of agile software development: A systematic review. *Information and Software Technology*, *50*(9-10), 833-859. https://doi.org/10.1016/j.infsof.2008.01.006

Elangovan, D., Long, C. S., Bakrin, F. S., Tan, C. S., Goh, K. W., Yeoh, S. F., Loy, M. J., Hussain, Z., Lee, K. S., Idris, A. C., & Ming, L. C. (2022). The use of blockchain technology in the health care sector: Systematic review. *JMIR Medical Informatics*, *10*(1), 619-624. https://doi.org/10.2196/17278

El Majdoubi, D., El Bakkali, H., & Sadki, S. (2021). SmartMed Chain: A blockchain-based privacy-preserving smart healthcare framework. *Journal of Healthcare Engineering*, *2021*(1), 1-19. https://doi.org/10.1155/2021/4145512

Elsevier. (2025). *ScienceDirect* . https://www.sciencedirect.com/

Erdem, A., Yildirim, S. Ö., Angin, P., Erdem, A., Yildirim, S Ö, & Angin, P. (2019). Blockchain for ensuring security, privacy, and trust in iot environments: The state of the art. In Z. Mahmood (Ed.), *Security, privacy and trust in the IoT environment* (pp. 97-122). https://doi.org/10.1007/978-3-030-18075-1_6

Fang, H. S. A., Tan, T. H., Tan, Y. F. C., & Tan, C. J. M. (2021). Blockchain personal health records: Systematic review. *Journal of Medical Internet Research*, *23*(4), 1-33. https://doi.org/10.2196/25094

Fugkeaw, S., Wirz, L., & Hak, L. (2023). Secure and lightweight blockchain-enabled access control for fog-assisted iot cloud based electronic medical records sharing. *IEEE Access*, *11*, 62998–63012. https://doi.org/10.1109/ACCESS.2023.3288332

Gomes, N. B. P., Franco, S. de C., & Salvador, L. do N. (2022). ONTOVID - Uma abordagem para construção de grafos de conhecimento semântico com enfoque em notificações e óbitos relacionados ao novo coronavírus (covid-19). In R. da Rosa Righi, & P. E. Ambrósio (Coords.), *Anais Do XXII Simpósio Brasileiro de Computação Aplicada à Saúde* (pp. 425-436). https://doi.org/10.5753/sbcas.2022.222723

Gutiérrez, O., Romero, G., Pérez, L., Salazar, A., Charris, M., & Wightman, P. (2020). HealthyBlock: Blockchain-based it architecture for electronic medical records resi-

lient to connectivity failures. *International Journal of Environmental Research and Public Health*, *17*(19), 1-38. https://doi.org/10.3390/ijerph17197132

Han, Y., Zhang, Y., & Vermund, S. H. (2022). Blockchain technology for Electronic Health Records. *International Journal of Environmental Research and Public Health*, *19*(23), 1-6. https://doi.org/10.3390/ijerph192315577

Haritha, T., & Anitha, A. (2023). Multi-level security in healthcare by integrating lattice-based access control and blockchain-based smart contracts system. *IEEE Access*, *11*, 114322–114340. https://doi.org/10.1109/ACCESS.2023.3324740

Healthcare Information and Management Systems Society. (2025). *Interoperability in healthcare*. https://www.himss.org/resources/interoperability-healthcare

He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, *2022*(1), 1-13. https://doi.org/10.1155/2022/6476274

Huang, X. (2019). Blockchain in healthcare: A patient-centered model. *Biomedical Journal of Scientific & Technical Research*, *20*(3), 1-10. https://doi.org/10.26717/BJSTR.2019.20.003448

Hussien, H. M., Yasin, S. M., Udzir, N. I., & Ninggal, M. I. H. (2021). Blockchain-based access control scheme for secure shared personal health records over decentralised storage. *Sensors*, *21*(7), 1-36. https://doi.org/10.3390/s21072462

Institute of Electrical and Electronics Engineers. (2025). *IEEE Xplore*. https://ieeexplore.ieee.org/Xplore/home.jsp

International Organization for Standardization. (2005). ISO/TR 20514: 2005 Health Informatics. https://www.iso.org/obp/ui/#iso:std:iso:tr:20514:ed-1:v1:en:en

Intersoft Consulting. (n. d.). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Ismail, L., Materwala, H., & Hennebelle, A. (2021). A scoping review of integrated blockchain-cloud (BcC) architecture for healthcare: Applications, challenges and solutions. *Sensors*, *21*(11), 1-23. https://doi.org/10.3390/s21113753

Kemmoe, V. Y., Stone, W., Kim, J., Kim, D., & Son, J. (2020). Recent advances in smart contracts: A technical overview and state of the art. *IEEE Access*, *8*, 117782–117801. https://doi.org/10.1109/ACCESS.2020.3005020

Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences*, *11*(20), 1-27. https://doi.org/10.3390/app11209372

Kim, J. W., Kim, S. J., Cha, W. C., & Kim, T. (2022). A blockchain-applied personal health record application: Development and user experience. *Applied Sciences (Switzerland)*, *12*(4), 1-13. https://doi.org/10.3390/app12041847

Kitchenham, B. and Charters, S. (2007, January 9). *Guidelines for performing systematic literature reviews in Software Engineering*. Elsevier. https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

Lamounier, L. (2019, January 9). Blockchain hibrida: O melhor de dois mundos. *101 Blockchain*. https://101blockchains.com/pt/blockchain-hibrida-explicado/

Lavina, M. E. (2018). Validação do uso da tecnologia blockchain para o tráfego seguro de dados na área da saúde. *Unisul*, *1*(2), 1-16.

Li, D., Han, D., Weng, T. H., Zheng, Z., Li, H., Liu, H., Castiglione, A., & Li, K. C. (2021). Blockchain for federated learning toward secure distributed machine learning systems: A systemic survey. *Soft Computing*, *26*(9), 4423-4440. https://doi.org/10.1007/s00500-021-06496-5

Liu, X., Wang, Z., Jin, C., Li, F., & Li, G. (2019). A Blockchain-based medical data sharing and protection scheme. *IEEE Access*, *7*, 118943-118953. https://doi.org/10.1109/ACCESS.2019.2937685

Liu, Z., Xiang, Y., Shi, J., Gao, P., Wang, H., Xiao, X., Wen, B., & Hu, Y. C. (2019). Hyperservice: Interoperability and programmability across heterogeneous blockchains. In L. Cavallaro, J. Kinder, X. Feng Wang, & J. Katz (Eds.), *Proceedings of the 2019 ACM Conference on Computer and Communications Security* (pp. 549-566). Association for Computing Machinery. https://doi.org/10.1145/3319535.3355503

Mayer, A. H., da Costa, C. A., & Righi, R. da R. (2020). Electronic Health Records in a blockchain: A systematic review. *Health Informatics Journal*, *26*(2), 1273-1288. https://doi.org/10.1177/1460458219866350

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An overview of smart contract and use cases in blockchain technology. In Institute of Electrical and Electronics Engineers (Ed.), *2018 9th International Conference on Computing, Communication and Networking Technologies* (pp. 1-4). IEEE. https://doi.org/10.1109/ICCCNT.2018.8494045

Moura, L. M. F. de, Brauner, D. F., & Janissek-Muniz, R. (2020). Blockchain e a perspectiva tecnológica para a administração pública: Uma revisão sistemática. *Revista de Administração Contemporânea*, *24*(3), 259-274. https://doi.org/10.1590/1982-7849rac2020190171

Mughal, M. H., Shaikh, Z. A., Ali, K., Ali, S., & Hassan, S. (2022). IPFS and blockchain based reliability and availability improvement for integrated rivers' streamflow data. *IEEE Access*, *10*, 61101-61123. https://doi.org/10.1109/ACCESS.2022.3178728

Muneeb, M., Raza, Z., Haq, I. U., & Shafiq, O. (2022). SmartCon: A blockchain-based framework for smart contracts and transaction management. *IEEE Access*, *10*, 23687-23699. https://doi.org/10.1109/ACCESS.2021.3135562

Nakamoto, S. (2008, August 21,). Bitcoin: A peer-to-peer electronic cash system. *SSRN*. https://ssrn.com/abstract=3440802

National Library of Medicine (n. d.). National Center for Biotechnology Information. https://www.ncbi.nlm.nih.gov/

Ng, W. Y., Tan, T.-E., Movva, P. V. H., Fang, A. H. Sen, Yeo, K.-K., Ho, D., Foo, F. S. S., Xiao, Z., Sun, K., Wong, T. Y., Sia, A. T.-H., & Ting, D. S. W. (2021). Blockchain applications in health care for covid-19 and beyond: A systematic review. *The Lancet Digital Health*, *3*(12), e819-e829. https://doi.org/10.1016/S2589-7500(21)00210-7

Nunes, C. C., Ma, S., & Filho, M. S. T. (2021). Armazenamento descentralizado no Sistema Único de Saúde brasileiro (SUS) usando Interplanetary File System (IPFS) e blockchain. *Revista de Direito*, *13*(01), 01-25. https://doi.org/10.32361/2021130111695

Ortega, V., & Monserrat, J. F. (2020). Semantic distributed data for vehicular networks using the inter-planetary file system. *Sensors*, *20*(22), 1-21. https://doi.org/10.3390/s20226404

Parsifal. (2021). *Parsifal*. https://parsif.al/

Picot, S., Marty, A., Bienvenu, A.-L., Blumberg, L. H., Dupouy-Camet, J., Carnevale, P., Kano, S., Jones, M. K., Daniel-Ribeiro, C. T., & Mas-Coma, S. (2020). Coalition: Advocacy for prospective clinical trials to test the post-exposure potential of hydroxychloroquine against covid-19. *One Health*, *9*, 1-5. https://doi.org/10.1016/j.onehlt.2020.100131

Pimenta, F. U., & Silva, M. A. D. da. (2021). Enabling secure sharing of Electronic Health Records (EHR) with blockchain. *Research, Society and Development, 10(16),* 1-6. https://doi.org/10.33448/rsd-v10i16.23410

Pinna, A., Ibba, S., Baralla, G., Tonelli, R., & Marchesi, M. (2019). A massive analysis of ethereum smart contracts empirical study and code metrics. *IEEE Access*, *7*, 78194-78213. https://doi.org/10.1109/ACCESS.2019.2921936

Pop, C. D., Antal, M., Cioara, T., Anghel, I., & Salomie, I. (2020). Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy. *Sensors*, *20*(19), 1-21. https://doi.org/10.3390/s20195678

Reuters. (2019, July 22). Equifax faz acordo para pagar R$ 2,6 bi por vazamento de dados de clientes nos EUA. *Globo Notícias*. https://g1.globo.com/economia/tecnologia/noticia/2019/07/22/equifax-faz-acordo-para-pagar-r-26-bi-por-vazamento-de-dados-de-clientes-nos-eua.ghtml

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017). Towards using blockchain technology for eHealth data access management. In Institute of Electrical and Electronics Engineers (Ed.), *2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICABME.2017.8167555

Rocha, L. (2021, July 30). Blockchain pública, privada e híbrida: entenda as diferenças entre elas. *Criptofacil*. https://www.criptofacil.com/blockchain-publica-privada-e-hibrida-entenda-as-diferencas-entre-elas/

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938-1940. https://doi.org/10.26483/IJARCS.V8I5.4021

Senbekov, M., Saliev, T., Bukeyeva, Z., Almabayeva, A., Zhanaliyeva, M., Aitenova, N., Toishibekov, Y., & Fakhradiyev, I. (2020). The recent progress and applications of digital technologies in healthcare: A review. *International Journal of Telemedicine and Applications*, *2020*(1), 1-18. https://doi.org/10.1155/2020/8830200

Shah, D., Patel, D., Adesara, J., Hingu, P., & Shah, M. (2021). Integrating machine learning and blockchain to develop a system to veto the forgeries and provide efficient results in education sector. *Visual Computing for Industry, Biomedicine, and Art*, *4*(1), 1-13. https://doi.org/10.1186/s42492-021-00084-y

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for Electronic Health Records. *IEEE Access*, *7*, 147782-147795. https://doi.org/10.1109/ACCESS.2019.2946373

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of Electronic Health Record systems: A survey. *Computers & Security*, *97*, 1-20. https://doi.org/10.1016/j.cose.2020.101966

Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. (2020). A privacy-preserving healthcare framework using Hyperledger Fabric. *Sensors*, *20*(22), 1-14. https://doi.org/10.3390/s20226587

Stark, P. (2010). Congressional Intent for the HITECH Act. *American Journal of Managed Care*, *16*(12), 24-28. https://www.ajmc.com/view/ajmc_10dechit_stark_sp24tp28

Sun, J., Ren, L., Wang, S., & Yao, X. (2020). A blockchain-based framework for electronic medical records sharing with fine-grained access control. *Plos One*, *15*(10), 1-23. https://doi.org/10.1371/journal.pone.0239946

Sun, J., Yao, X., Wang, S., & Wu, Y. (2020). Blockchain-based secure storage and access scheme for electronic medical records in IPFS. *IEEE Access*, *8*, 59389-59401. https://doi.org/10.1109/ACCESS.2020.2982964

Superior Tribunal de Justiça. (2020, November 4). Em razão de ataque cibernético, STJ funcionará em regime de plantão até o dia 9. *Superior Tribunal de Justiça*. https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access*, *10*, 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679

Taralunga, D. D., & Florea, B. C. (2021). A blockchain-enabled framework for mHealth systems. *Sensors*, *21*(8), 1-24. https://doi.org/10.3390/s21082828

Tsai, C.-W., Chen, Y.-P., Tang, T.-C., & Luo, Y.-C. (2021). An efficient parallel machine learning-based blockchain framework. *ICT Express*, *7*(3), 300-307. https://doi.org/10.1016/j.icte.2021.08.014

Tuler De Oliveira, M., Reis, L. H. A., Verginadis, Y., Mattos, D. M. F., & Olabarriaga, S. D. (2022). SmartAccess: Attribute-based access control system for medical records based on smart contracts. *IEEE Access*, *10*, 117836-117854. https://doi.org/10.1109/ACCESS.2022.3217201

Wang, Q., Li, R., Wang, Q., Chen, S., & Xiang, Y. (2022). Exploring unfairness on proof of authority. *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 123-137. https://doi.org/10.1145/3488932.3517394

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. In M. J. Shepperd, T. Hall, & I. Myrtveit (Eds.), *EASE '14: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering* (pp. 1-10). Association for Computing Machinery. https://doi.org/10.1145/2601248.2601268

Wu, P. Y., Cheng, C. W., Kaddi, C. D., Venugopalan, J., Hoffman, R., & Wang, M. D. (2017). –Omic and Electronic Health Record big data analytics for precision medicine. *IEEE Transactions on Biomedical Engineering*, *64*(2), 263-273. https://doi.org/10.1109/TBME.2016.2573285

Xiao, Y., Xu, B., Jiang, W., & Wu, Y. (2021). The healthchain blockchain for Electronic Health Records: Development study. *Journal of Medical Internet Research*, *23*(1), 1-13. https://doi.org/10.2196/13556

Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, *7*, 118541-118555. https://doi.org/10.1109/ACCESS.2019.2935149

Yang, J., Jia, Z., Su, R., Wu, X., & Qin, J. (2022). Improved fault-tolerant consensus based on the PBFT algorithm. *IEEE Access*, *10*, 30274-30283. https://doi.org/10.1109/ACCESS.2022.3153701

Zhang, J., Zhong, S., Wang, T., Chao, H. C., & Wang, J. (2020). Blockchain-based Systems and applications: A survey. *Journal of Internet Technology*, *21*(1), 1-14. https://doi.org/10.3966/160792642020012101001

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. *Computational and Structural Biotechnology Journal*, *16*, 267-278. https://doi.org/10.1016/j.csbj.2018.07.004

Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., & Chen, R. (2019). NutBaaS: A blockchain-as-a-service platform. *IEEE Access*, *7*, 134422-134433. https://doi.org/10.1109/ACCESS.2019.2941905

Reception date: 08/05/2024
Review date: 10/05/2024
Acceptance date: 24/04/2025
Contact: caetano.paulo@animaeducacao.com.br