Electronic health records in a Blockchain: A systematic review

André Henrique Mayer
Cristiano André da Costa
Rodrigo da Rosa Righi
Universidade do Vale do Rio dos Sinos (UNISINOS), Brazil

Abstract
Blockchain could reinvent the way patient’s electronic health records are shared and stored by providing safer mechanisms for health information exchange of medical data in the healthcare industry, by securing it over a decentralized peer-to-peer network. Intending to support and ease the understanding of this distributed ledger technology, a solid Systematic Literature Review was conducted, aiming to explore the recent literature on Blockchain and healthcare domain and identify existing challenges and open questions, guided by the raise of research questions regarding EHR in a Blockchain. More than 300 scientific studies published in the last ten years were surveyed, resulting in an up-to-date taxonomy creation, challenges and open questions identified, and the most significant approaches, data types, standards and architectures regarding the use of Blockchain for EHR were assessed and discussed.

Keywords
Blockchain, distributed systems, electronic health records, medical informatics

Introduction
Blockchain technology has the potential to transform health care by placing the patient at the center of the health system and increasing the security, privacy, and interoperability of health data. This technology could provide a new model for health information exchange (HIE) by making electronic health records (EHRs) more efficient and secure.¹

Corresponding author:
Cristiano André da Costa, Programa de Pós-Graduação em Computação Aplicada, Software Innovation Laboratory (SOFTWARELAB), Universidade do Vale do Rio dos Sinos (UNISINOS), Av Unisinos 950, São Leopoldo 93022-750, Brazil.
Email: cac@unisinos.br

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (http://www.creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
EHRs contain critical and highly sensitive private information for diagnosis and treatment in healthcare. These data are a valuable source of healthcare intelligence. The sharing of healthcare data is an essential step toward making the healthcare system smarter and improving the quality of healthcare service. An EHR is a structure in digital format of a patient’s health data that is created and maintained throughout the patient’s life and is typically stored by and spread among multiple hospitals, clinics, and health providers. These providers typically retain primary access to the records, preventing easy access to past data by patients. In situations where the patients have access to their health record, they end up interacting with data in a fractured manner that reflects the nature of how these records are managed.

Supporting a sharing and trust mechanism, Blockchain provides a possible future solution for data sharing, which could enable collaborative clinical decision-making in telemedicine and precision medicine. The main contribution of this article is a systematic literature review that highlights previous studies that are related to EHRs and Blockchain; in this review, we explore the application of a Blockchain structure to healthcare in EHR storage and access management.

A Blockchain is a distributed ledger protocol that was originally associated with Bitcoin. It uses public key cryptography to create an append-only, immutable, and timestamped chain of content. It was originally designed for maintaining a financial ledger; however, the Blockchain paradigm can be extended to provide a generalized framework for implementing decentralized computing resources, even in the healthcare ecosystem. In summary, this work aims to review and assess the literature on Blockchain in healthcare. Motivated by research on possible solutions for healthcare data concerns, such as storage and privacy issues, we seek to identify challenges and open questions. We also propose a taxonomy to facilitate understanding of the Blockchain ecosystem and to support future works.

**Methods**

This work is conducted using a systematic literature review methodology. A systematic literature review (often referred to as a systematic review) is a method for identifying, evaluating, and interpreting all available research that is relevant to a research question, topic area, or phenomenon of interest. Most research begins with a literature review. However, unless a literature review is thorough and fair, it is of little scientific value. This is the main rationale for undertaking systematic reviews. A systematic review synthesizes existing work in a manner that is fair and is considered fair.

All reviewed articles in this systematic literature review were identified by searching reliable academic repositories such as PubMed, Google Scholar, ACM, ScienceDirect, and IEE in October 2018. These databases index research articles and abstracts from most major academic publishers and repositories worldwide, including both free and subscription sources.

**Study design**

This section focuses on describing the adopted research methodology, presenting procedures, and outlining the main subsequent decisions via a systematic literature review that is designed to provide an overview of EHRs in a Blockchain research area, to establish whether research evidence exists on a topic, and to provide quantitative evidence.

The systematic literature review approach was adopted because our objectives are to group and synthesize available academic content regarding EHRs and Blockchains and to identify promising directions, which do not require in-depth analysis or synthesis. Widely recognized empirical guidelines were followed in planning and running systematic mapping studies.
The presented systematic literature review method was carried out by defining and executing the following steps:\(^6\)

1. **Research questions.** Introduce the research questions that are being investigated;
2. **Search strategy.** Outline the strategy and the libraries that are explored to collect data;
3. **Article selection.** Explain the criteria for selecting the studies;
4. **Distribution of studies.** Describe how the studies are distributed chronologically;
5. **Quality assessment.** Describe the quality assessment of the selected studies;
6. **Data extraction.** Compare the selected studies and research questions.

The following sections describe how this process of mapping the study was carried out.

**Research questions**

According to Kitchenham and Charters\(^5\) and Petticrew and Roberts,\(^6\) the definition of research questions is the most important part of any systematic review. Therefore, we seek to identify and classify the technology that is related to EHRs in a Blockchain. Specific and general research questions were formulated to address subjects that are related to the features, problems, challenges, and solutions that are currently being considered and the research opportunities that exist or are emerging.

General research questions have been refined into more specific questions (SQs) to facilitate classification and subject analysis and to pinpoint promising research directions for further investigation. Our research questions are classified into two categories, namely, general questions (GQs) and SQs, as follows:

- **GQ1.** What is the taxonomy for EHRs in a Blockchain?
- **GQ2.** What are the challenges and open questions that are related to EHRs in a Blockchain?
- **SQ1.** What are the important principles behind Blockchain when it is applied to healthcare?
- **SQ2.** What are the healthcare protocols and standards that should apply in a Blockchain network?
- **SQ3.** What are the types, models, and approaches of a Blockchain architecture?
- **SQ4.** How can Blockchain indefinitely store the “ever-growing” patient medical records?

**Search strategy**

For conducting a reproducible systematic literature review, a proper search strategy is defined, and it is necessary to define the search keywords and the scope, which are the key concepts of our research questions, for retrieving accurate results.

To build an optimal search string, authors Kitchenham and Charters\(^5\) suggest breaking down the research question into individual facets, namely, research units, where their synonyms, acronyms, abbreviations, and alternative spellings are all included and combined using Boolean operators.\(^5\)

The final search string is obtained via the following three steps:

1. Identification of synonyms, acronyms, and related words;
2. Identification of terms and related words in the abstracts of the articles that were identified in the first search;
3. Construction of the search string using Boolean characters such as OR and operators.
Finally, we obtain the following search string: (“Blockchain”) AND ((“healthcare”) OR (“health”)) OR ((“health record”) OR (“EHR”) OR (“PHR”) OR (“medical record”) OR (“EMR”)).

Article selection

Article selection was conducted via exclusion processes, in which articles that do not completely address the research questions were removed with the objective of obtaining a corpus that matches the proposition of this work. To apply the exclusion criteria, we used the terms of population and intervention criteria as follows:

- **Exclusion criterion 1.** Removal of articles that do not address “healthcare” and “Blockchain” or related acronyms.
- **Exclusion criterion 2.** Removal of articles that do not address “health records,” “EHR,” or “PHR.”

The steps of the filtering process are as follows: (1) idiom filtering of articles that have a minimum of six pages and are written in English, (2) filtering of articles that were published in journals or conference proceedings, (3) survey removal, (4) impurity removal, (5) filtering by title and abstract, (6) removal of duplicates, and (7) filtering by full text.

These filtering steps are performed to ensure the quality assessment of the research corpus that resulted from the search string. Filtering steps 1, 2, 3, and 4 are intended to aggregate articles that have been elaborated and, ideally, reviewed by peers in accordance with good practices and academic rules. Blog posts, magazines, and all other nonscientific results were ignored or removed.

Impurities in the search results were removed, for example, articles on Bitcoin’s Blockchain on which there was a financial ledger were returned in the search results because of the Blockchain characteristics and had to be removed since they are outside our EHR and healthcare context.

The titles and abstracts of all remaining articles were analyzed, and those that did not address EHR and Blockchain as the main subjects were removed. Furthermore, all the remaining studies were grouped, duplicates were removed, and, finally, a full text review yielded our final working corpus of articles.

Quality assessment

It is important to assess the quality of the selected studies with quality criteria that are intended to evaluate the relevance of the articles. We evaluated the selected articles in terms of the purpose of the research, contextualization, literature review, related work, methodology, obtained results, and conclusion in accordance with the objectives and directions for future study. To apply all these requirements, each article’s quality was evaluated by subjecting it to questions for determining whether the study satisfies the quality criteria:

- Does the article clearly describe the purpose of the research?
- Does the article describe the literature review, background, or context?
- Does the article present related work?
- Does the article present an architecture proposal or a research methodology?
- Does the article contain research results?
- Does the article present a conclusion?
Results

Recruitment process

To answer each proposed research question, a total of 345 articles and scientific studies that are related to the research topic were assessed. The literature reviewing steps are described in the following subsections via elaborative information synthesis. In addition to answering the research questions, we have also proposed contributions in the EHR and Blockchain field from the study of related works, an updated taxonomy, and an updated description of the main challenges and issues.

Implementing the search strategy

To cover as many related studies as possible, we selected articles from reliable academic repositories such as PubMed, Google Scholar, IEEE, Springer, ACM, and ScienceDirect as our main electronic databases for our literature review, which cover the most relevant journals and conferences within the computer science and healthcare fields. To limit our search, we set the years to range from 2008 to 2018.

Proceeding with article selection

The article selection process is summarized in Figure 1, which illustrates the filtering process step by step. Initially, a total of 345 articles were returned for the search string prior to applying the exclusion criteria; of these, a total of 122/345 (35.36%) articles were removed by filtering by English idioms and a minimum of six pages, thereby leaving us with a total of 223 articles remaining. Then, we applied the journal and conference proceeding filter and the number of articles was reduced to 138, which corresponds to a reduction of 85/223 (38.11%) articles. In addition, all
survey articles were removed since they tend to provide a superficial analysis that is often based on questionnaires, thereby leaving us with a total of 124 articles, where 14/138 (10.14%) articles were removed. Then, 67/124 (54.03%) articles with impurities were identified and were removed.

The first exclusion criterion was applied to the studies that remained after we withdrew these articles. Continuing the process, 15/57 (26.31%) articles were filtered through a title and abstract analysis review, followed by duplicate removal, where 4/42 (9.52%) were removed, thereby leaving us a total of 38 articles for full-text review.

Finally, 38 articles were selected as the baseline for this study. An overview of all primary studies is presented in Table 1, with the identifier, reference, publication year, publisher, and type of each study, which are sorted by the year of publication.

**Performing the quality assessment**

The proposed quality criteria scores were assessed for each obtained article. Although most articles did not fully satisfy all six criteria for evaluation, they responded positively to at least four out of six of the quality assessment criteria that are described in section “Quality assessment.” All the assessed articles clearly presented their research purpose, presented a literature review, and were supported by a research methodology, bibliographical references, or models/architectural proposals. This quality assessment did not exclude articles from the corpus; it only evaluated whether the articles had a satisfactory structure/organization.

**Data extraction and answers to the research questions**

Finally, in this section, we discuss and answer the GQs that are listed in this work.

**GQ1. What is the taxonomy for EHRs in a Blockchain?** To facilitate understanding and to provide a clearer description of EHRs within Blockchain, we created a taxonomy, which is illustrated in Figure 2. The primary purpose of the taxonomy was to create a schema for categorizing and summarizing ideas from a corpus by applying organization to clarify concepts and build connections.

In the literature review of the selected articles, several current issues were investigated that are addressed in the EHR and Blockchain fields. Therefore, this taxonomy is created for answering the first general research question and for gathering and organizing the various possibilities that are related to the proposed study. The taxonomy aims at representing and illustrating important EHR and Blockchain’s characteristics; in addition, this taxonomy could help classify, compare, and evaluate EHR Blockchain types. Moreover, this classification can provide an overview of possible alternatives in terms of aims, content, and techniques.

The proposed taxonomy represents the fundamental characteristics of EHRs in a Blockchain by combining the properties that arise from the intersection of both concepts. We primarily divided the taxonomy into five main characteristics: governance, interoperability, privacy, scalability, and security. Each characteristic is further subdivided into possibilities for addressing each of these properties in the representation of EHR using Blockchain. The taxonomy uses a “has-a” type of relation among nodes.

Most of our taxonomy’s aspects and characteristics are self-explanatory. However, the security field is too broad; hence, we divide it into four criteria as suggested in Bodin et al.:40

- **Confidentiality.** Prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it.
- **Integrity.** The information is accurate, complete, and consistent and only authorized individuals may change it.
Availability. The information is available to authorized users when needed.

Authentication. The system ensures that users are who they claim to be.

**GQ2. What are the challenges and open questions that are related to EHRs in a Blockchain?** To answer this question, challenges, open questions, aspects, issues, and common concerns in the adoption of EHRs in a Blockchain among the analyzed studies were identified. Aspects that are related to

| Id. | Author | Year | Publisher | Type |
|-----|--------|------|-----------|------|
| A01 | Linn and Koo | 2016 | HealthIT | Journal |
| A02 | Ekblaw et al. | 2016 | IEEE | Conference |
| A03 | Yue et al. | 2016 | Springer | Journal |
| A05 | Nichol and Brandt | 2016 | ResearchGate | Journal |
| A16 | Hashemi et al. | 2016 | IEEE | Conference |
| A04 | Roehrs et al. | 2017 | Elsevier | Journal |
| A07 | Yang and Yang | 2017 | NISK | Conference |
| A10 | Smith and Dhillon | 2017 | AMCIS | Conference |
| A11 | Rabah | 2017 | MRJOURNALS | Journal |
| A12 | Cheng et al. | 2017 | Taylor & Francis | Journal |
| A13 | Liu et al. | 2017 | IEEE | Journal |
| A15 | Ichikawa et al. | 2017 | JMIR | Journal |
| A19 | Kshetri | 2017 | Elsevier | Journal |
| A21 | Shae and Tsai | 2017 | IEEE | Conference |
| A23 | Karafiloski and Mishev | 2017 | IEEE | Conference |
| A24 | Xia et al. | 2017 | IEEE | Journal |
| A25 | Thomason | 2017 | GHJ | Journal |
| A26 | Dubovitskaya et al. | 2017 | JAMIA | Journal |
| A27 | Lemieux | 2017 | IEEE | Conference |
| A29 | Priisalu and Ottis | 2017 | Springer | Journal |
| A35 | Kuo et al. | 2017 | JAMIA | Journal |
| A06 | Cyran | 2018 | Partners in Digital Health | Journal |
| A08 | Patel | 2018 | SAGE | Journal |
| A09 | Dagher et al. | 2018 | Elsevier | Journal |
| A14 | Ribitzky et al. | 2018 | Partners in Digital Health | Journal |
| A17 | Zhang et al. | 2018 | JNCA—Elsevier | Journal |
| A18 | Niranjanamurthy et al. | 2018 | Springer | Journal |
| A20 | Guo et al. | 2018 | IEEE | Journal |
| A22 | Fan et al. | 2018 | IET Comm | Journal |
| A28 | Mannaro et al. | 2018 | IEEE | Conference |
| A30 | Wang and Song | 2018 | Springer | Journal |
| A31 | Kleinaki et al. | 2018 | Elsevier | Journal |
| A32 | Banerjee et al. | 2018 | Elsevier and KeAi | Journal |
| A33 | Gordon and Catalini | 2018 | Elsevier | Journal |
| A34 | Grover et al. | 2018 | Elsevier | Journal |
| A36 | Jiang et al. | 2018 | IEEE | Conference |
| A37 | Mamoshina et al. | 2018 | Impact Journals | Journal |
| A38 | Roman-Belmonte et al. | 2018 | MEDKNOW Publications | Journal |
interoperability, privacy, and authorization (access control) are among the major concerns and challenges that were identified in the EHR Blockchain literature. These aspects and concerns are presented in Table 2.

Interoperability challenges between provider and hospital systems pose additional barriers to effective data sharing. Due to this lack of coordinated data management and exchange, health records are fragmented rather than cohesive. Many studies have highlighted concerns regarding data interoperability and heterogeneity and as possible solutions to these concerns, studies have identified the adoption of open standards and compliance with regulatory bodies.

As healthcare data are already distributed across multiple stakeholders, the Blockchain’s distributed ledger technology (DLT) infrastructure could outperform existing centralized systems in accessing, extending, and securing the data. Decentralized systems could also streamline costs, reduce transaction times, and be more efficient than centralized systems due to lower overhead and fewer intermediaries.

Regarding infrastructure costs, private Blockchains typically impose no interaction costs (e.g., transaction fees), whereas public Blockchains tend to not be free of charge. However, the convenience that is provided by a public Blockchain may justify the cost of usage versus the costs of licensing, running, and maintaining a private clinical data exchange infrastructure.27
SQ1. What are the important principles behind Blockchain when it is applied to healthcare?

The literature review highlighted important principles regarding Blockchain technology. These principles are listed in Table 3.

In the Blockchain, all transactions are logged. The register includes information on the date, time, participants, and amount of every transaction. Each node in the network has a full copy of the Blockchain and on the basis of cryptographic principles, the transactions are verified by the Bitcoin miners, who maintain the ledger. These principles also ensure that these nodes automatically and continuously agree regarding the current state of the ledger and every transaction in it. If anyone attempts to corrupt a transaction, the nodes will not reach a consensus and, hence, will refuse to incorporate the transaction into the Blockchain.

Regarding transparency, historically, the dominant principle for protecting health-related data in the healthcare field has been to keep the records inaccessible except to those who are directly involved in a patient’s care. The Blockchain privacy model keeps data records widely accessible; however, the patients to whom they refer are either secret or anonymized.

Central data storage has often proved disastrous in the modern age of cyberattacks and data leaks. Distributing this health data over the network makes it persistent. Mainly due to consensus and the digital record, Blockchain transactions can’t catch fire, be misplaced, or become damaged by water.

For Blockchain applications in healthcare, an important characteristic is immutability, which may conflict directly with privacy rights. For example, in a case in which a patient has the right to be forgotten, requiring the deletion of his or her stored health records from the Blockchain clashes with the immutability objective of the Blockchain-enabled solution. In such a case, health data can be stored off-chain, and if a patient exercises his or her right to be forgotten, the personal information that is stored off-chain could be deleted.

SQ2. What are the healthcare protocols and standards that should apply in a Blockchain network?

Healthcare providers may use both open standards and proprietary formats to organize
their health records, which are typically used by internal applications and encountered in various formats. To answer this research question, the standards that were identified in the literature review are summarized in Table 4 and present a vast number of organizational data patterns for health records.

EHRs were not designed to manage multi-institutional, lifetime medical records. Patients leave data scattered across various organizations as life events take them away from one provider’s data silo and into another. In doing so, they lose easy access to past data, as the provider, not the patient, typically retains primary stewardship. The Blockchain architecture may help address this problem by supporting the development of interoperability standards and requirements that address privacy and enable the secure exchange of data across systems. Open standards play a substantial role in health data exchange by providing system flexibility and helping realize interoperability.

Countries or regions that differ in terms of regulations have their own healthcare protocols and standards due to national medical regulations. The standards are intended to systematize the patients’ clinical datasets and define protocols for ensuring the uniformity of health information. These are usually dedicated to standardizing the storage of and regulating clinical and demographic data about patients. Health records typically incorporate data regarding vital signs, laboratory exams results, evolution, and diagnosis.

Without the adoption of interoperable data standards (such as HL7 FHIR or OpenEHR), clinical data can be specified in formats and structures that are difficult to interpret and integrate into other systems. Therefore, a standards-based architecture is necessary for ensuring the integration with existing telemedicine systems to enable secure and scalable clinical data sharing for improving collaborative decision support.
Regarding patient identification on the Blockchain, various authors propose the adoption of personally identifiable information (PII), which is also known as a unique patient identifier (UPID). PII is a standard that assigns an alphanumeric identification code that is designed to uniquely represent a patient in a hospital. It is used by the medical information system (MIS) and other subsystems and on all paper forms and in all manual processes that are related to the patient and may be used to identify the patient inside Blockchain.\(^4\)

**SQ3. What are the types, models, and approaches of a Blockchain architecture?** The reviewed architectural components often are composed of connected devices, sensors, and a collector that collects data and sends them to the Blockchain network for storage.\(^28\) The amount of data that originate from mobile devices and wearable sensors is growing at an exponential rate and architectures that are based on commodity hardware provide cost-efficient high scalability.\(^7\)

Blockchains are currently the most popular form of DLT.\(^26\) Blockchain technologies can be divided into three types:\(^13\)

- **Public Blockchains.** Everyone can participate in the distributed network, check data transactions and verify them, and participate the process of reaching consensus.
- **Consortium Blockchains.** The node that has authority may be selected in advance and usually has partnerships, such as business-to-business partnerships. The data in the Blockchain can be open or private and it is considered a partly decentralized network.
- **Private Blockchains.** Nodes will be restricted, and not everyone can participate in the Blockchain, which has strict authority management of data access.

A set of proposed architectures and models are presented in the literature review. A Blockchain is typically the central component of these architectures and is responsible for the persistence (storage), authorization, and assistance with open standards, as the healthcare interoperability infrastructure is enabled. The proposed Blockchain architectures should support the storage of medical data, including formal medical records and health data from mobile applications and wearable
sensors, and should follow the user throughout his life. Additional advantages of Blockchain’s distributed architecture are built-in fault tolerance and disaster recovery.7

Blockchain’s address generation mechanism for authentication and authorization in the network employs public key cryptography to manage identities in the framework. In public key cryptography, a pair of mathematically related public and private keys are to create digital signatures and encrypt data. It is computationally infeasible to obtain a private key based on a public key. Thus, public keys can be shared freely, thereby enabling users to encrypt content and verify digital signatures. Likewise, private keys are kept secret to ensure that only the owners of the private keys can decrypt the content and create digital signatures.27

Another key feature of the Blockchain architecture is smart contracts. A smart contract is a software program that executes programs in a Blockchain; it can read other contracts, make decisions, and execute other contracts.28 A smart contract can be used to store digital assets into the Blockchain and claim ownership of the assets. The assets are managed by the smart contract, which is executed automatically by the program code. The smart contract code defines the rules and conditions for management and triggering the action of asset ownership.15

When applied in healthcare, smart contracts may create intelligent representations of existing medical records that are stored within individual nodes on the network. Smart contracts may contain metadata about the record ownership, permissions, and data integrity.

**SQ4. Can Blockchain indefinitely store “ever-growing” patient medical records?** The Blockchain directory model supports the ability to grow and change dramatically throughout the lifetime of the Blockchain by adding new participants and changing organizational relationships.2 It’s technology is particularly useful for recording the continuous and steady growth of transactions. For the EHR system, there is an upper bound on the number of records, which is the number of citizens it serves. Population growth is relatively slower than the growth of the number of monetary transactions, for example, in the Bitcoin Blockchain.4

Blockchain’s chain structure also helps support the ever-growing medical records by maintaining a continuously growing linked list of medical records, in which each block contains a timestamp and a link to a previous block.11 An alternative solution would be a Blockchain that contains pointers to off-chain data; the metadata that are associated with such pointers can include the information that is required for supporting interoperability.19,26,27 Using this approach, heavy-weight data, including imaging exam results (X-ray and others), could be stored off-chain.

In the context of the sharing of imaging exam result, a few authors proposed storing encrypted health information directly on the Blockchain; however, storing the encrypted imaging studies of all patients would result in an enormous Blockchain, which would be far too large for a node that is running on a mobile device or even a modern workstation to download, store, and validate. Blockchain size is a problem that is under active study and has been shown to be a limiting factor even for chains that store simple transactional data, much less the massive blocks that would be required for storing medical imaging studies.24

As a Blockchain continues to grow, the scalability of the system may be compromised because only users who have large storage spaces and high computational power will be able to partake in the Blockchain as miners or full nodes. To overcome this issue, Blockchain typically supports three types of nodes: full nodes, light nodes, and archive nodes:

- **Full nodes.** They process every transaction and store every block in the Blockchain.25
- **Light nodes.** It is possible to verify transactions without running a full network node. Users must only keep a copy of the block headers of the longest proof-of-work chain, which they can obtain by querying network nodes until they have received the longest chain.41
By storing the block header, a light node can verify that a transaction has not been altered without committing large portions of memory to the Blockchain. Light nodes can also access the data they desire.25

- **Archive nodes.** They store every transaction and block on the Blockchain. In addition, they store transaction receipts and the entire state tree.25

The versatility of these three types of nodes increases the scalability of the Blockchain such that large corporations and individual users can interact with the Blockchain for their purposes and with their available resources.23

**Discussion**

This literature review successfully identified both quantitative and qualitative sets of studies that enabled us to obtain a clear view of the ecosystem regarding EHRs on a Blockchain in the last 10 years, starting from a selected number of articles. Some of the most relevant studies of the field were highlighted according to systematic selection criteria.

We planned to identify several common aspects of studies by answering several research questions. As a result, we were able to propose a taxonomy and identify open questions to be further researched that represent challenges and issues that have been identified in recent years. An up-to-date taxonomy was created and we identified challenges, open questions, current data types, related standards, objectives, functions, and architectures regarding EHR and Blockchains.

Various Blockchain studies aim to address recordkeeping challenges, such as greater patient control over sensitive health information,20 and the main findings that are presented in this review include the importance of realizing EHR interoperability via the adoption of Blockchain by healthcare providers and the definition of open standards. These might be essential for the improvement of health care services due to health data sharing, availability, and integration. Furthermore, the use of Blockchain technology in clinical trials may enhance the development of drugs and medical devices.13

To the best of our knowledge, this is the first systematic review that focuses on Blockchain-based EHR. Most healthcare providers are still storing health records on centralized servers and in various formats, which hinders interoperability. Moreover, the need for more investments and efforts in consolidating open standards is clear for establishing higher interoperability levels among providers and patients.

EHRs are viewed as a standardized information model that enables integration among multiple healthcare providers; this integration is considered their main advantage. EHRs have several benefits, which range from supporting medical prescriptions, improving disease management, and contributing to the reduction of severe medication errors. However, EHRs have limitations regarding interoperability, for example, when health organizations adopt international but heterogeneous standards.4

Blockchain applications in healthcare are still in early stages of development and evaluation, and these obstacles might eventually be overcome, thereby opening the path for other possibilities,16 which is in line with our findings in the literature review.

**Limitations**

This research is limited to aspects that are related to EHRs and Blockchain and does not include other Blockchain applications in the healthcare field, for example, supply chain and drugs access control. In this sense, the review focused strictly on articles that address the inherent EHR and Blockchain concepts.
In this literature review, various limitations were identified, such as technological limitations, vendor adoption, and infrastructure costs. To realize a global and fully interoperable EHR with Blockchain, these limitations must be overcome. For example, currently, technologies do not fully address the desired requirements and concerns because they might encounter problems that are related to security, privacy, scalability, and interoperability. Consider a case in which a patient has the right to be forgotten, thereby requiring the deletion of their stored health data from the Blockchain. This demand directly clashes with the immutability objective of the Blockchain-enabled solution.

Another important variable that must be taken in account when considering the Blockchain solution is the scalability constraints in terms of the tradeoff between the transaction volume and the computer power for processing the transactions. The limitations that are discussed in this literature review might be overcome if the industry sector defines and adopts open standards; then, many technologies may migrate from experimental prototypes to real applications.

Conclusion and future work

In this study, a systematic literature review regarding EHRs within a Blockchain was conducted, with the objective of identifying and discussing the main issues, challenges, and possible benefits from Blockchain adoption in the healthcare field. The application of Blockchain has exceeded the scope of the field of economics and we have highlighted Blockchain’s potential for the healthcare area, while also revealing that it still highly depends on the acceptance of the new technology within the healthcare ecosystem.

Analyzing the results that were obtained from the literature review, we conclude that Blockchain technology might be a future suitable solution for common problems in the healthcare field, such as EHR interoperability, establishing sharing trust between healthcare providers, auditability, privacy, and granting of health data access control by patients, which would enable them to choose whom they want to trust and with whom to share their medical records. However, additional research, trials, and experiments must be carried out to ensure that a secure and established system is implemented prior to using Blockchain technology on a large scale in healthcare, since a patient’s health data are personal, highly sensitive, and critical information.

This study may serve as a basis or inspiration for future works and studies. Our answered research questions and taxonomy may contribute to the proposition of an architecture or model that addresses the challenges that are discussed in this article. In addition, a possible direction for future work is to survey the combination of Blockchain and the Internet of the things (IoT) in healthcare, with the objective of realizing network scalability improvements by supporting low-end devices.

Author contributions

All authors contributed equally in writing the article. All authors have read the final version and agree with their content.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported in part by the Coordination for the Improvement of Higher Education Personnel—Brazil (CAPES)—Finance Code 001 and by the the National Counsel of Technological and Scientific Development—Brazil (CNPq)—Grant numbers 405354/2016-9 and 303640/2017-0.
ORCID iD
Cristiano André da Costa https://orcid.org/0000-0003-3859-6199

References
1. Rabah K. Challenges & opportunities for blockchain powered healthcare systems: a review. *Mara Res J Med Health Sci* 2017; 1(1): 45–52.
2. Yue X, Wang H, Jin D, et al. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J Med Syst* 2016; 40(10): 218.
3. Ekblaw A, Azaria A, Halamka JD, et al. A case study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data. *Proc IEEE Open Big Data Conf* 2016; 13: 13.
4. Cheng EC, Le Y, Zhou J, et al. Healthcare services across China — on implementing an extensible universally unique patient identifier system. *Int J Healthc Manage* 2018; 11(3): 210–216.
5. Kitchenham BA and Charters S. Guideline for performing systematic literature reviews in software engineering. EBSE Technical Report EBSE 2007-01, 9 July 2007. Kelele and Durham: Kelele University and Durham University.
6. Roehrs A, da Costa CA and da Rosa Righi R. OmniPHR: a distributed architecture model to integrate personal health records. *J Biomed Inform* 2017; 71: 70–81.
7. Petticrew M and Roberts H. *Systematic reviews in the social sciences: a practical guide*. Malden, MA: Blackwell Publishing, 2006.
8. Forrest JL and Miller SA. Evidence-based decision making in action: part 1– finding the best clinical evidence. *J Contemp Dent Pract* 2002; 3(3): 10–26.
9. Hashemi SH, Faghri F, Rausch P, et al. World of empowered IoT users. In: *Proceedings of the 2016 IEEE first international conference on internet-of-things design and implementation (IoTDI)*, Berlin, 4–8 April 2016.
10. Nichol P and Brandt J. Co-creation of trust for healthcare: the cryptocitizen framework for interoperability with blockchain. *Res Propos*, 2016, https://www.researchgate.net/profile/Peter_Nichol2/publication/306013124_Co-Creation_of_Trust_for_Healthcare_The_Cryptocitizen_Framework_for_Interoperability_with_Blockchain/links/57aa227808ae7a6420bcd091.pdf
11. Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform J* 2019; 25(4): 1398–1411.
12. Liu W, Zhu SS, Mundie T, et al. Advanced block-chain architecture for e-health systems. In: *Proceedings of the 2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom)*, Dalian, China, 12–15 October 2017.
13. Ichikawa D, Kashiyama M and Ueno T. Tamper-resistant mobile health using blockchain technology. *JMIR mHealth uHealth* 2017; 5(7): e111.
14. Kshetri N. Blockchain’s roles in strengthening cybersecurity and protecting privacy. *Telecommun Policy* 2017; 41(10): 1027–1038.
15. Shae Z and Tsai JP. On the design of a blockchain platform for clinical trial and precision medicine. In: *Proceedings of the 2017 IEEE 37th international conference on distributed computing systems (ICDCS)*, Atlanta, GA, 5–8 June 2017.
16. Karafiloski E and Mishev A. Blockchain solutions for big data challenges: a literature review. In: *Proceedings of the IEEE EUROCON 2017-17th international conference on smart technologies*, Ohrid, 6–8 July 2017.
17. Xia Q, Sifah EB, Asamoah KO, et al. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* 2017; 5: 14757–14767.
18. Thomason J. Blockchain: an accelerator for women and children’s health? *Glob Heal J* 2017; 1(1): 3–10.
19. Dubovitskaya A, Xu Z, Ryu S, et al. Secure and trustable electronic medical records sharing using blockchain. *AMIA Annu Symp Proc* 2017; 2017: 650.
20. Lemieux VL. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In: *Proceedings of the 2017 IEEE international conference on big data (big data)*, Boston, MA, 11–14 December 2017, pp. 2271–2278. New York: IEEE.
21. Priisalu J and Ottis R. Personal control of privacy and data: Estonian experience. *Health Technol* 2017; 7(4): 441–451.
22. Kuo T-T, Kim H-E and Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. *J Am Med Inform Assoc* 2017; 24(6): 1211–1220.
23. Linn LA and Koo MB. Blockchain for health data and its potential use in health it and health care related research. In: *ONC/NIST use of blockchain for healthcare and research workshop*, Gaithersburg, MD, 2016, https://www.healthit.gov/sites/default/files/11-74-ablochainforhealthcare.pdf
24. Cyran MA. Blockchain as a foundation for sharing healthcare data. *Blockchain Healthc Today*. Epub ahead of print 23 March 2018. DOI: 10.30953/bhty.v1.13.
25. Yang H and Yang B. A blockchain-based approach to the secure sharing of healthcare data. In: *Proceedings of the Norwegian information security conference*, Oslo, 27–29 November 2017.
26. Ribitzky R, Clair JS, Houlding DI, et al. Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. *Blockchain Healthc Today*. Epub ahead of print 23 March 2018. DOI: 10.30953/bhty.v1.124.
27. Zhang P, White J, Schmidt DC, et al. Flirchain: applying blockchain to securely and scalably share clinical data. *Comput Struct Biotechnol J* 2018; 16: 267–278.
28. Nirajanamurthy M, Nithya BN and Jagannatha S. Analysis of blockchain technology: pros, cons and SWOT. *Cluster Comput* 2018; 20: 1–15.
29. Guo R, Shi H, Zhao Q, et al. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access* 2018; 776(99): 1–12.
30. Fan K, Ren Y, Wang Y, et al. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. *IET Commun* 2017; 12(5): 527–532.
31. Mannaro K, Baralla G, Pinna A, et al. A blockchain approach applied to a teledermatology platform in the Sardinian region (Italy). *Information* 2018; 9(2): 44.
32. Wang H and Song Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *J Med Syst* 2018; 42(8): 152.
33. Kleinaki AS, Mytis-Gkometh P, Drosatos G, et al. A blockchain-based notarization service for biomedical knowledge retrieval. *Comput Struct Biotechnol J* 2018; 16: 288–297.
34. Banerjee M, Lee J and Choo KKR. A blockchain future for internet of things security: a position paper. *Digit Commun Netw* 2018; 4(3): 149–160.
35. Gordon WJ and Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Comput Struct Biotechnol J* 2018; 16: 224–230.
36. Grover P, Kar AK and Davies G. “Technology enabled health” —insights from twitter analytics with a socio-technical perspective. *Int J Inform Manage* 2018; 43: 85–97.
37. Jiang S, Cao J, Wu H, et al. BlochIE: a BLOCKchain-based platform for healthcare information exchange. In: *Proceedings of the 2018 IEEE international conference on smart computing (SMARTCOMP)*, Taormina, 18–20 June 2018, pp. 49–56. New York: IEEE.
38. Mamoshina P, Ojomoko L, Yanovich Y, et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget* 2018; 9(5): 5665.
39. Roman-Belmonte JM, De La Corte-Rodriguez H and Rodriguez-Merchan EC. How blockchain technology can change medicine. *Postgrad Med* 2018; 130(4): 420–427.
40. Bodin LD, Gordon LA and Loeb MP. Evaluating information security investments using the analytic hierarchy process. *Commun ACM* 2005; 48(2): 78–83.
41. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf
42. Dagher GG, Mohler J, Milojkovic M, et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain Cities Soc* 2018; 39: 283–297.
43. Smith K and Dhillon G. Blockchain for digital crime prevention: the case of health informatics, 2017, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1040&context=amcis2017