IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 December 2022, accepted 4 January 2023, date of publication 12 January 2023, date of current version 19 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3236505

SURVEY

Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security

EDGAR R. DULCE VILLARREAL[1,2], JOSE GARCÍA-ALONSO[3], (Member, IEEE), ENRIQUE MOGUEL[4], AND JULIO ARIEL HURTADO ALEGRÍA[1]

[1]Facultad de Electrónica y telecomunicaciones, Universidad del Cauca, Popayán 190003, Colombia
[2]Escuela de Ciencias Básicas Tecnología e Ingeniería, Universidad Nacional Abierta y a Distancia (UNAD), Pasto 110110, Colombia
[3]Department of Computer and Telematic Systems Engineering, Universidad de Extremadura, 10004 Badajoz, Spain
[4]CénitS–COMPUTAEX, Extremadura Supercomputing, Technological Innovation and Research Center, 10004 Cáceres, Spain

Corresponding author: Edgar R. Dulce Villarreal (edgardv@unicauca.edu.co)

This work was supported in part by the Spanish Ministry of Science and Innovation under Project PID2021-124054OB-C31; and in part by the Regional Ministry of Economy, Science and Digital Agenda under Grant GR21133.

ABSTRACT In recent years it has been shown that the secure exchange of medical information significantly benefits people's life quality, improving their care and treatment. The interoperability of the entire healthcare ecosystem is a constant challenge, and even more, with all the risks posed to the security of healthcare information. Blockchain technology is emerging as one of the main alternatives when it comes to finding a balance in the healthcare ecosystem. However, the constant development of new Blockchain technologies and the evolution of healthcare systems make it difficult to find established proposals. From an architectural point of view, the design of blockchain-based solutions requires trade-offs e.g. security and interoperability. This paper focuses on two main objectives, in the first one, it was carried out a Systematic Literature Review for exploring architectural mechanisms used to support the interoperability and security of Blockchain-based Health Management Systems. Taking into account of results, a series of scenarios were generated where these mechanisms can be used along with their context, issues, and various architectural concerns (interoperability and security). In the second objective, a high-level architecture and its validation were proposed through an experiment for the whole process of developing a Domain Specific Language, using the Model Driven Engineering methodology for specific Smart Contracts.

INDEX TERMS Blockchain, DSL, health, interoperability, MDE, model, security, smart contracts, software architecture.

I. INTRODUCTION

In today's globalized world, where the percentage of universal health coverage is only 50%. It is necessary for everyone to have access to quality health services (diagnosis, treatment, and prevention) in an efficient, safe, and transparent manner [1]. For this purpose, technologies that increase the coverage and quality of hospital services are being developed every day, and without them, medical centers would be inefficient and lose credibility [2].

The large healthcare ecosystem includes several interconnected stakeholders with different and sometimes competing needs. The healthcare environment involves a high degree of comprehensive and reliable information exchange between stakeholders [3]. However, this information is highly fragmented and distributed in multiple non-integrated data storage systems, making it impossible to have adequate information to support the care process and decision-making. This occurs because each medical center manages health information in an isolated and centralized way, causing health personnel to have a small history of the patient's entire life, which leads to errors in diagnosis and treatment. Likewise, having centralized information presents multiple information risks. This is highlighted by [4], which mentions that healthcare is one of the sectors most vulnerable to cyberattacks. Denial-of-service (DoS) attacks can occur to indispose

The associate editor coordinating the review of this manuscript and approving it for publication was Taehong Kim.

information, or a ransomware attack to hijack information, which in many cases cannot be recovered [5]. For these and other reasons, it is necessary to have mechanisms that contribute to achieving interoperability between the information systems that support the care processes [6]. In addition, security is an indispensable element for disseminating patients' medical records, since this task entails various risks that cause serious damage to reputation, insurance, and finances, among other factors in the healthcare ecosystem [7].

The healthcare field is a topic that is researched daily from different approaches, one of which is the relationship between *Blockchain* (BC) technology and the management of *Health Management Systems* (HMS), with the idea of improving aspects such as interoperability, security, traceability, confidentiality, and information integrity. BC was first introduced by Satoshi Nakamoto in a paper on Bitcoin [8]. Applications of BC have been studied in financial environments (where it began), as well as in other growing areas of ICT. Now, it is considered a mainstream technology, used in different industries and use cases, such as identity management, contracts, supply chain, insurance, healthcare, voting, etc. [9].

Cloud computing is a new way of delivering computing resources and services. Many managers and experts believe it can improve healthcare services, benefit healthcare research, and change the face of healthcare information technology [10]. However, as with any innovation, cloud computing must be rigorously evaluated before widespread adoption. [10] demonstrate how the cloud facilitates the exchange of healthcare data between providers, helping each provider manage their data, providing a seamless way to exchange data, and providing a unified/comprehensive view of each patient's (scattered) health records. In other words, cloud computing can be used to interconnect different healthcare providers, and be used by providers to cope with any sudden or seasonal changes. Scenarios in which the cloud plays an important role are discussed in the Background (Section II) and in Synthesis and Discussion (Section VI) of this document.

Software architecture is the result of several design decisions. The first kind of decision happens at the requirements level when architects realize trade-offs among quality attributes, such as security and interoperability. Often, security concerns arise when interoperability enables the system to share data with others systems. A system can give access to information (interoperability) from others, which could help improve a business process. However, it opens potential issues where the data becomes compromised (security vulnerabilities). A closed system could be an alternative to achieve security, but it will result in an unrealistic solution [11].

With the constant development of new BC technologies and the evolution of healthcare systems, it is difficult to know what the state of the art is and that is why we propose to perform a Systematic Literature Review (SLR). In conducting and reporting this review, we adopt the SLR guidelines of Kitchenham and Brereton [12], and Petersen et al. [13], to find out what architectural mechanisms are being used to improve the security and interoperability of HMSs using BC, and what architectural aspects these mechanisms rely on. This SLR provides the theoretical underpinning and sufficient basis for one of the main purposes of this work, which consists of developing a high-level architecture together with an experiment for the construction of an architectural mechanism for the *Interoperability and security* of HMSs through BC technology, creating an ecosystem of trust between them. This mechanism, in principle proposed as a *Domain Specific Language* (DSL) [14], which seeks to contribute to solving the difficulties of addressing interoperability of HMS through BC technology. A DSL would allow specifying *Smart Contracts (SC)* (code fragments that can be executed autonomously and automatically based on predefined conditional triggers) at a high level of abstraction, enabling independence from specific technologies and facilitating the reuse of contract implementation through *Model Driven Engineering* (MDE) approach [15].

A. PROBLEM STATEMENT

Healthcare has always been fundamental to society, where everyday accidents and emergencies arise those cause ailments and diseases that must be diagnosed, treated, and managed by different services [16]. Having these services presents technological challenges in health, such as storage, consultation, and exchange of information, where its implementation is associated with a decrease in morbidity and mortality [17].

Considering the above, there are several standards for Electronic Medical Records (EMRs). Roehrs et al. [3], discuss 14 standards for EMRs, each of these standards present its characteristics, strengths, and weaknesses, which make choosing one of them an additional problem to consider. Generally, health records are stored in databases within health organizations and rarely have access from remote sites, in this case, some inconveniences of slow access to data, and data access restrictions, among others, are generated [18].

Medical technology is an area that has evolved substantially, with a wide range of hardware, software, and communication networks that have as their main objective to improve the quality of the services provided [19]. BC and healthcare researchers [19], agree that the management of healthcare trending data is a latent challenge, but can help to improve the accuracy of physician diagnosis and promote research in the healthcare sector.

Although several architectural solutions in the literature cover non-functional requirements such as interoperability (e.g., a broker [20]), as well as security and privacy requirements (e.g., data encryption [20]), such as access control and data privacy [21], balancing between them is not a trivial task as off-the-shelf solutions do not exist [22]. Architectural solutions include trade-offs that can facilitate interoperable access between applications, but that could introduce a lot of distrust between parties [23], [24], [25], [26].

There is distrust between healthcare organizations and healthcare professionals, such as doctors, and nurses, among others, for using data from other unreliable sources, and competition has been generated in the exchange of sensitive information to generate concrete business objectives. Additionally, there is a lack of integrity in the shared information [27]. Taking into account the above, BC is more secure than other mechanisms for managing information, since it guarantees that the data is complete, and allows the traceability of the information to be seen [27].

In turn, as with most technologies, BC is no stranger to potential security threats, vulnerabilities, and other associated problems. One of the main components of BC is SC, in these, several challenges are presented, for example, writing secure SC can be extremely difficult due to various business logic, and limitations of the platform where they are generated [28]. The problems encountered in SC are classified according to the consensus mechanism used, the quality of the SC source code, the lack of standard programming languages, and the logic associated with the programmer, among others [29]. In addition, one of the biggest challenges in SC implementation is how to unify contract execution environments [30]. In this regard, several interoperability and security issues are arising from the SC analysis, design, and development phases.

Interoperable access to data in the healthcare ecosystem must provide the necessary functionality for the entities involved, maintaining security, trust, and privacy. Interoperability and security are issues that must be traded off in the specific context of the functional, non-functional, and business requirements of the healthcare ecosystem. The problem of knowledge and expertise required to design software architectures in this new scenario is a derivative of the opportunities of BC in the healthcare sector. The problem lies in the knowledge around architectures, particularly interoperability, which is incipient, and conceptual and technological strategies are required to facilitate the design considering qualities in trade-off with security and interoperability.

B. CONTRIBUTIONS

As a systematization of knowledge on BC interoperability and security in healthcare environments, this paper makes three contributions:

1) Present a Systematic Literature Review SLR, in which we identified and discussed BC interoperability and security solutions. We identify and classify papers to find architectural mechanisms used in healthcare environments that use BC and identify architectural elements that support solutions in these environments.
2) Detail 7 scenarios, representing 7 ways to architecturally approach solutions using BC in healthcare. In each scenario, we present an overview, of the problem, analyze interoperability and security, and relate some security and interoperability tactics. We then discuss some trade-offs used to balance interoperability and security in the healthcare ecosystem using BC.
3) We propose a MDE Framework for blockchain interoperability and security. This framework consists of a high-level architecture whose main objective is the development of a DSL for the specification of SC independent of the BC platform used, to contribute to the interoperability and security of the healthcare environment. We propose an experiment developed under the MDE methodology, to put this architecture in context and validate each of the elements required in this solution.

C. ORGANIZATION

Section II, provides background on BC technology, types of BC, its consensus algorithms, SC, BC Platforms, and we relate BC within healthcare. We also discuss interoperability and security, and other architectural aspects, such as quality attributes, patterns, and architectural tactics. We also briefly describe the MDE technology. Next, section III presents and describes the SLR process, while in section IV, we analyze and present the most relevant results of the SLR. Continuing, we present the answers to the research questions posed in section V, in this one, in RQ1, we analyze the architectural mechanisms found. In RQ2 we use the ISO 42010 standard, to classify in a unified view the main authors of BC within the context of software architecture. Then, in section VI, we give the synthesis and discussion of the results of the previous section, we propose a categorization into 7 different scenarios, in which BC is being used to impact the interoperability and security of HMS. Section VII presents the BC Interoperability MDE Framework, along with the experiment developed using MDE technology to perform SC translation between BC platforms. Finally, in Section VIII we conclude the paper. At the end, we present the acknowledgments and introduce the authors.

II. BACKGROUND

In this section, we provide the necessary background information.

A. BLOCKCHAIN

BCs are driving the development of multiple applications, such as in healthcare. A BC is a data structure consisting of an ordered sequence of batch entries, called blocks. The blocks are linked using the hash[1] of the immediately preceding record (Figure 1). The above guarantees immutability [8].

A BC is maintained by a set of decentralized nodes (peers), which store a copy of the entire chain. These nodes, acting in response to a consensus protocol, are presented in this chapter. In the works [31], [32], and [33], the fundamentals of the BC technology are mentioned in more detail.

[1]mathematical algorithm that transforms any block of data into a new series of characters with a fixed length.

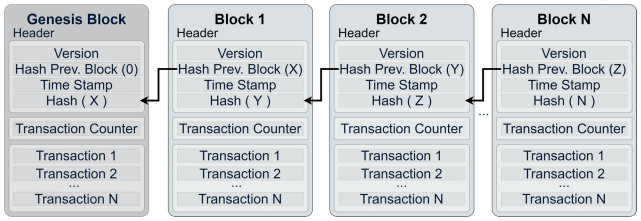


FIGURE 1. General representation of the structure of a BC.

B. TYPES OF BLOCKCHAIN

Currently, there are different types of BC each with unique capabilities and features that suit different needs. These types of BC are public, private, permissioned, and consortium [16].

1) PUBLIC BLOCKCHAINS

It is a public infrastructure network, i.e. anyone is free to join the network without permission. Network participants can view and even participate, in and validate transactions. The most commonly used infrastructures are Ethereum and Bitcoin. Public BCs are mostly those applications open to the general public, where full transparency and decentralization are required. In addition, they encourage network members, called ''miners''; to check transactions to receive in return some rewards in the form of cryptocurrency [21].

2) PRIVATE BLOCKCHAINS

They allow previously invited participants some type of transaction or extra block creation work within it. They are created for organizations that seek to have limited and private access to records and thus keep them out of the public's reach [34].

3) AUTHORIZED BLOCKCHAINS

In these networks, restrictions are imposed on who can participate in the network and in which transactions. Participants will need an invitation or permission to join [23].

4) CONSORTIUM BLOCKCHAINS

Several organizations can share the responsibilities of maintaining a BC. These pre-selected organizations determine who can send transactions or access data. A consortium BC is ideal for businesses when all participants must be authorized and have a shared responsibility for the BC [23].

C. CONSENSUS MECHANISMS

For a BC to be useful, there must be some mechanism by which nodes can mutually add new blocks to the chain. There are several consensus mechanisms, the most commonly used are the following [16]:

1) PROOF OF WORK (PoW)

Process by which nodes compete to generate the next block by expending computational effort to solve a challenging mathematical problem (e.g., in Bitcoin). The first node arrives at a solution that transmits the result to the network; the solution is verified by the remaining nodes, the block is added to the chain, and then work begins on the next block [21].

2) PROOF OF STAKE (PoS)

PoS algorithms waive the computational challenge but offer only a randomly selected subset of nodes the opportunity to produce each block. The probability of selection is weighted according to each entity's existing level of investment in the system, typically quantified as the value or duration of asset holdings relevant to that particular BC [35].

3) PROOF OF DELEGATED PARTICIPATION (DPoS)

Those who hold the network token are able to cast votes to elect block producers; votes are weighted by the voter's stake, and the block producer candidates that receive the most votes are those who produce blocks. Users can also delegate (''proxy'') their voting power to another user [36].

4) PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

This mechanism guarantees consensus despite the arbitrary behavior of the participants. A new block is added if more than two-thirds of all validation pairs propose the same response [37]. An important variant of this mechanism is discussed in [38], who propose a reputation-based Delegated Byzantine Fault Tolerance consensus (DBFT) algorithm to efficiently achieve consensus on the authoritative BC.

Other less relevant consensus mechanisms used are Proof of Authority (PoA) [39], QuorumChain [40], Raft [41], among others. An in-depth study of consensus mechanisms can be found in [42].

D. BLOCKCHAIN PLATFORMS

The following is a description of the most commonly used BC platforms in healthcare environments:

1) ETHEREUM

Ethereum,[2] is an open-source platform to write and distribute decentralized applications and the first platform that supports advanced general-purpose SC (Turing-complete) whose primary language used in the BC is Solidity [43] and transactions are sent to Ethereum through Virtual Machine (EVM) to execute methods [44].

2) HYPERLEDGER FABRIC

Hyperledger,[3] the open global ecosystem for enterprise-grade BC technologies. Is an open-source, enterprise-grade, permissioned distributed ledger technology (DLT) platform designed for use in enterprise contexts [45]. This project, called Fabric, has a highly modular and configurable architecture, enabling innovation, versatility, and optimization for a wide range of industry use cases, including banking, finance, insurance, healthcare, human resources, and supply chain. Fabric is the first distributed accounting platform to support

[2]https://ethereum.org/en/
[3]https://www.hyperledger.org/

SC (called Chaincode) built-in general-purpose programming languages such as Java, Go, and Node.js, and run in containers (Dockers) [46], [47].

E. SMART CONTRACT SC

In 1996, Nick Szabo, a lawyer, and computer scientist, first introduced the concept of SC [48]. With the use of robust cryptographic protocols, Szabo recognized the possibility of writing software that resembled contract clauses (from paper contracts between people), that was binding on the parties and that reduced their chances of non-compliance. It also recognized that the term did not involve the use of artificial intelligence, but the use of computer algorithms that would be eventually used in all types of contracts. Although it was a novel idea in the 1990s, the technology needed for its proper development was not available. It was only in 2008 when the development of BC technology provided the necessary platform and ecosystem for SC. SC are immutable digital programs deployed on BC platforms to encode agreements. They enable BC technology to play a vital role in many fields, such as finance and healthcare. An important aspect of modeling and implementing SC is to define the process of exchanging messages and the rules governing the agreements under which the corresponding actions are executed [49].

F. CLOUD COMPUTING AND BLOCKCHAIN

Cloud computing is a widely used way today to deliver IT resources and services. Many managers and experts believe that when combined with BC technology, they will be able to improve healthcare services and change the face of health IT [10]. However, as with any innovation, the combination of cloud computing and BC must be rigorously evaluated before widespread adoption. Cloud computing enables real-time data sharing regardless of geographic location and offers resource elasticity based on needs [50]. Various scenarios of cloud usage are discussed in Section VI. Another scenario being analyzed in healthcare environments is edge computing [51], which, compared to cloud computing, can significantly reduce service latency, alleviate backbone load, and improve the quality of user experience by migrating part of the cloud resources (e.g., communication, computation, and storage) proximally to other locations closer to the user. Thus, in edge computing BC offers its features to achieve integrity and security of confidential data [52].

Likewise, healthcare solutions are supported by cloud platforms, the two most relevant cases being Amazon Web Services (AWS) and Microsoft Azure [53] provides an in-depth comparison of these two platforms and discusses complementary services for BC environments in the cloud known as Blockchain-as-a-service (BaaS). For example, on AWS there is the Blockchain Amazon Quantum Ledger Database (QLDB),[4] which is a new database that provides the functionalities of a distributed ledger database without creating a ledger. Amazon QLDB mainly focused on developing an immutable and transparent ledger. This QLDB can create a distributed ledger application both with relational and BC databases. To maintain both immutable (relational) and distributed (Hyperledger Fabric and Ethereum) databases simultaneously [53]. On the other hand, Microsoft's Azure has the BaaS service supported on its Azure Blockchain Workbench (ABW)[5] platform. Which establishes a scalable and integrated BC development environment along with an Ethereum, Hyperledger, and Corda BC application development environment. ABW enables the direct development of distributed applications (DApps) without worrying too much about the underlying system services [54].

G. BLOCKCHAIN AND HEALTHCARE

BC has attracted huge attention in healthcare for its secure, interoperable, and more efficient access to health data and EMRs among patients, providers, and participating entities [55]. Compared to the existing health information exchange model, patients, healthcare professionals, medical facilities, and government institutions can benefit from BC-enabled applications due to their features of decentralized data, privacy protection, integrity, data security, and access control of their data [55].

It is critical to ensure interoperability in healthcare, particularly for Electronic Health Records (EHR) exchange for the following reasons [56]:

- Rapid and seamless access to patient information;
- Prevention of manual errors;
- Improving the efficiency of health care providers;
- Reduced healthcare costs;
- Verifiable and immutable transactions.

By providing a mechanism to achieve consensus among distributed entities without relying on a single trusted party, BC technology facilitates data management in healthcare environments. In addition, BC provides a shared, immutable and transparent history of all transactions to create applications with security, accountability, and transparency. This provides a unique opportunity to develop a secure and reliable data management and exchange system [55].

H. LEGAL ASPECTS IN BLOCKCHAIN SYSTEMS

Legal aspects are an element that must be taken into account in any discussion involving the processing of personal data. Some legal and regulatory situations in BC environments are listed below. Authors from the BC world [57], highlight issues related to the General Data Protection Regulation (GDPR), such as security, trust, confidentiality, and data privacy issues. In particular, security threats are exacerbated by the presence of multiple BCs and potentially multiple administrators. In terms of privacy, the authors highlight issues with the right to be forgotten, where a user can request that their data be removed from the BC. Currently, most BCs do not provide effective mechanisms that can respond to this request. Fine-grained BC access control is designated

[4]https://aws.amazon.com/es/qldb/

[5]https://azure.microsoft.com/en-us/solutions/blockchain/

as a key requirement to minimize information leakage and confidentiality risk [33].

Likewise, and due to the contradictions in health legislation [58], important legal problems are generated for medical institutions, health personnel, patients, and their families. These legal problems are compounded when a patient's care requires crossing borders [55], or when devices are used that intervene in healthcare decision-making towards the patient. To counteract these problems, currently, some institutions, such as the European Commission, have developed frameworks to fill this gap. For example, guidelines on a medical device vigilance system, controls, and cybersecurity requirements ensure the security of medical devices and maintain an adequate level of functionality and security of devices [59].

I. INTEROPERABILITY AND SECURITY, AND OTHER ARCHITECTURAL ASPECTS BETWEEN HMS

A Software architecture of a computer program or system is defined according to Bass et al. [11], as "the structure or structures of the system, comprising the software components, the externally visible properties of those components, and the relationships between them". Obtaining the appropriate architecture is crucial for the success of a software system [60]; today it is recognized as essential to have an architectural representation of the system, for the analysis and description of high-level properties. Moreover, architectural descriptions have been recognized as essential for a well-designed system [11].

There are widely used **architectural styles** (e.g., pipelines and filters) and others that represent particular domains, the latter providing a structure for a group of applications and simplifying the process of building new systems through the reuse of existing infrastructure, reducing costs and facilitating system maintenance [61]. **Quality Attributes**, such as interoperability and security, are measurable properties of a system, indicating how well the system meets the needs of stakeholders. Quality Attributes can be achieved using well-known **Architectural Patterns and Tactics** specific to each attribute [11].

There are several definitions of **Interoperability**, one of them is given by the IEEE [62], which defines it as "...the ability or capability of two or more systems to exchange information and to use the information exchanged...". This definition encompasses two distinct ideas: the first mentions the exchange of information (syntactic interoperability), and the second focuses on the exchanged information that can be correctly understood, processed, and effectively used by the receiver (semantic interoperability).

In a healthcare environment, interoperability is defined by the Healthcare Information and Management Systems Society as "...the ability of different health information systems (hospital systems, departmental systems, electronic clinical records, etc.), to exchange data and use information that has been exchanged within and across organizational boundaries, to improve the effective delivery of healthcare to individuals and communities..." [63].

Security is a measure of the system's ability to protect data and information from unauthorized access while providing access to authorized people and systems, Bass et al. [11]. Every action taken in a secure environment is called a computer attack. Computer attacks can primarily affect the confidentiality, integrity, and availability of data, and can also impact non-repudiation, authentication, and authorization. The above, considering data at rest, in transit, and computational processes.

J. MODEL DRIVEN ENGINEERING (MDE)

It is a discipline within software engineering that deals with the systematic uses of software models to improve productivity and some other aspects of software quality, such as maintainability and interoperability between systems. In addition, it provides a higher level of abstraction and raises the level of automation [64].

The MDE paradigm has some basic principles that can be considered as its fundamental elements [64]:

- A model fully or partially represents an aspect of a software system.
- These models are represented with DSLs.
- A metamodel is used to formally represent a DSL.
- Automation is usually achieved through the translation of models into code or through model transformations.

A DSL is a language designed specifically for a certain domain, context, or company to facilitate the task of people who need to describe things in that domain, such as SQL for the database domain [15]. A DSL is composed of abstract syntax (or metamodel), concrete syntax, and semantics [64].

III. RESEARCH METHODOLOGY OF THE SLR

To carry out this SLR, we followed the methodology defined by Petersen et al. [13] and Kitchenham and Brereton [12]. The main objective is to explore what architectural mechanisms are being used to support the interoperability and security of HMSs using BC. The SLR is divided into different sequential steps, as can be seen in figure 2:

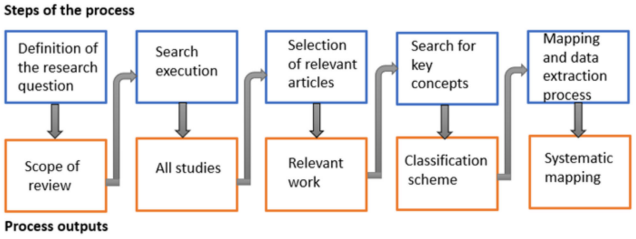


FIGURE 2. Systematic Literature Review Process.

A. DEFINITION OF RESEARCH QUESTIONS (RQ)

The first step of this SLR is to define the RQs that are intended to provide answers as to what architectural mechanisms are being used to improve the security and interoperability of

HMSs using BC. For this purpose, the following RQs have been defined:

RQ1: What architectural mechanism is being used to support the interoperability and security of HMS using BC?

RQ2: What architectural aspects are associated with the interoperability and security of HMS using BC?

B. CONDUCTING THE SEARCH

The second step is to collect all related research works based on the specific search terms. To this end, we make use of the PICOC methodology [65] (Population, Intervention, Comparison, Outcome, and Context) for the definition of the RQs and the search string [66], [67]. The keywords identified using the PICOC strategy can be seen in Table 1.

TABLE 1. Keywords identification using PICOC strategy.

Concepts	Keywords
Population	"Blockchain", "Blockchains", "Block chain"
Intervention	"Health", "Healthcare", "ehealth", "e-Health"
Comparison	"mde", "model driven engineering", "model-driven engineering", "dsl", "protocol", "broker", "meta-model", "ontology", "connector", "api", "gateway", "proxy", "framework", "intermediary"
Outcomes	
Context	"Interoperability" "Security"

For the defined keywords we generate the following search string:

```
 (blockchain OR blockchains OR "block chain")
AND
(health OR healthcare OR ehealth OR e-health)
AND
(mde OR "model driven engineering" OR
    "model-driven engineering" OR dsl OR protocol
    OR broker OR metamodel OR ontology OR
    connector OR api OR gateway OR proxy OR
    framework OR intermediary)
AND
(interoperability OR security)
```

For the selection of the bibliographic databases, we relied on [68], which provides the four most important in the field of Computer Science and Engineering: ACM Digital Library, Scopus, IEEEXplore, and Web of Science. Figure 3 shows a bubble diagram reporting the number of works obtained and categorized by each of the databases.

C. SCREENING OF RELEVANT PAPERS

Next, inclusion (I) and exclusion (E) criteria are defined to add/remove the works that are relevant/irrelevant to this study:

Inclusion Criteria

- **I1:** Papers published in the last five years.
- **I2:** If several papers are related to the same study, only the most recent one is selected.
- **I3:** If a paper describes more than one study, each study is evaluated individually.
- **I4:** If there are short and full versions of the same study, we select the full version.

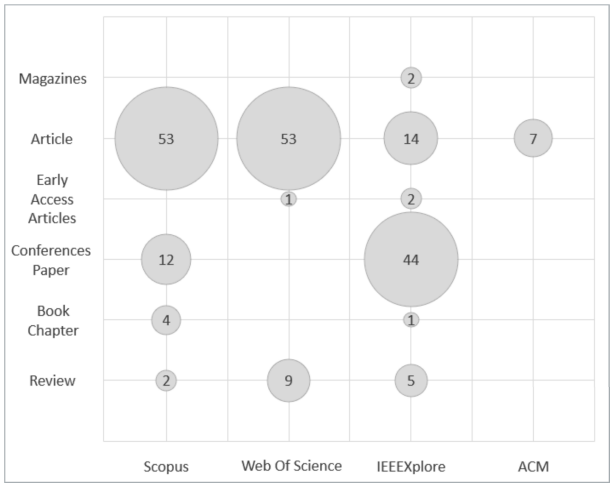


FIGURE 3. Visualization of the number of works by type in each database.

Exclusion Criteria

- **E1:** Technical reports, abstracts, surveys (gray literature) and secondary studies (SMS).
- **E2:** Papers that are written in languages different from English.
- **E3:** Papers that do not present studies related to BC, health, security, interoperability, and architectural mechanism or synonyms.
- **E4:** Only Journal, Conference and Early Access papers.

D. KEYWORDING ON THE BASIS OF THE ABSTRACT

The next step is the review of the title, abstract, and keywords to identify those that may be of interest and discard those that do not satisfy the inclusion and exclusion criteria already defined [13]. Once this step was completed, all the selected papers were analyzed and classified. The final set of works relevant to this study and their analysis are presented in the Results section (section IV).

E. DATA EXTRACTION AND MAPPING PROCESS

The papers were analyzed and classified according to categories created to separate the research contributions of each paper (Results section IV). The data extracted from the papers were stored and subjected to qualitative and quantitative analysis. This analysis aimed to find evidence to answer the RQs defined in the Conducting Search section (III). To organize the findings and document the data extraction process, a spreadsheet was used, which also allowed other statistical analyzes to be carried out, such as determining the number of publications per year, by place, and by type, among other analyzes.

IV. ANALYSIS AND PRESENTATION OF SLR RESULTS

The aim of SLR is to explore what architectural mechanisms are being used to improve the security and interoperability of HMSs using BC, and by what architectural aspects these mechanisms are supported. Figure 4 summarizes the entire

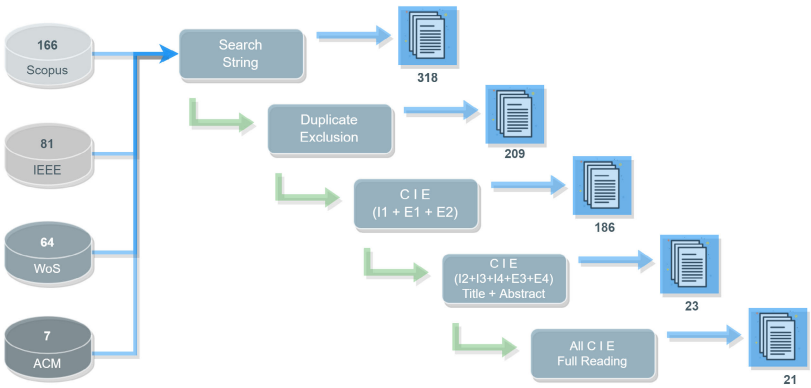


FIGURE 4. Article filtering process overview, adopted [69].

refinement process, which is described below: Initially, when searching the selected databases, 318 papers were obtained. Of these, it was identified that 109 of them are stored in more than one database, therefore, duplicates are also eliminated, leaving only one copy of each paper in the records. Thus, for the next step, 209 papers remained to be analyzed. Next, the inclusion and exclusion criteria (I1 + E1 + E2) are applied in the 209 papers, including those published in the last five (5) years and, excluding records that do not correspond to published papers, conference or book chapters, and those written in languages other than English, leaving 186 articles. We applied the inclusion and exclusion criteria (I2 + I3 + I4 + E3 + E4) to 186 papers, reading their title and abstracts, and identifying 23 relevant works with the topic. The complete reading of these 23 articles was carried out and all the inclusion and exclusion criteria were applied again, 2 that referred to the same work were eliminated, and the 21 final papers were used as evidence to answer our RQ. The list of these documents appears in the References section at the end of this document. Next, we are giving an overview of the classification of the final 21 papers, detailing some characteristics to expand their description.

A. GENERAL ASPECTS

The first general aspect identified was the geographical location of the authors of the documents reviewed to establish, in percentage terms, the origin of the documents by country. The percentage of production for each country was calculated based on the affiliation of the authors of each document, following the approach of equivalent credit in authorship used by [70].

It is important to note that Figure 5 shows papers from 21 different countries, represented by 76 researchers, as it is vital to examine research from different social and organizational cultures and to evidence both academic and governmental efforts dedicated to this type of research. Likewise, it can be seen that slightly less than half (31/76) were written by at least one researcher from the USA (18 authors) or China (13 authors), leaders in technological and research processes worldwide. Also, it is noteworthy that a large number of countries from Asia and Europe are represented, indicating that our research topic is widespread in countries concerned with the adoption of cutting-edge technologies and with significant advances in BC technology. On the other hand, in Africa, there is only one representative and in South America there is none, evidencing the low adoption of this type of technology in these countries and the need to start with this type of work in these countries.

The second general aspect was the identification of the type of publication reviewed. Figure 6 shows the number of papers by type of publication (Journal Article and Conference Paper) versus the database from which they were obtained. In this sense, the number of Articles (14 papers) is the most frequent, which is positive, given that this type of document is the most rigorous in terms of review by editors and blind reviewers. followed by Conference Papers (7 Papers), this fact also can be considered positive, since this type of publication makes it possible to disseminate and learn about the latest advances in research in different areas of knowledge.

B. DESCRIPTIONS REGARDING BC, TYPES OF BC, CONSENSUS MECHANISMS, AMONG OTHERS

To schematize globally the results, in Table 2 we present a classification of the main results. We can see the 21 papers along with the architectural mechanism they use, the consensus mechanism used within the proposed BC, the type of BC (public, private, authorized, or consortium), the BC technology used (Ethereum, Hyperledger, or others), and the state of progress of their work (a proposal, experiment, prototype, PoC or finished).

Focusing on the **Consensus** column in Table 2, it is evident that there is no common factor at the time of its choice, as mentioned by [71] this field is constantly growing and its choice depends very much on the sector in which the BC technology is to be implemented. If we move on to the **Type BC** column, the most used among all the papers is Authorized (7/21), which contains the necessary balance when managing an HMS [55], [72], it also goes following the

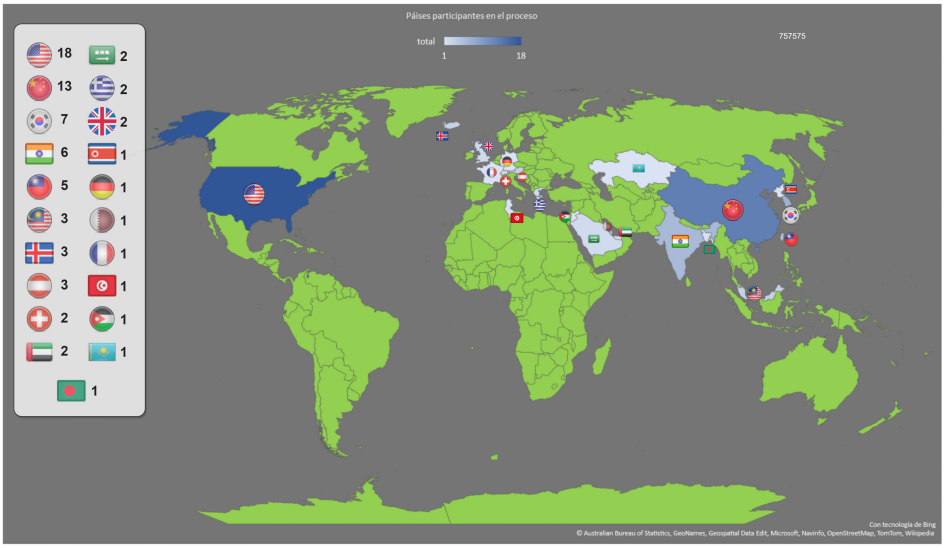


FIGURE 5. Countries represented in the final papers.

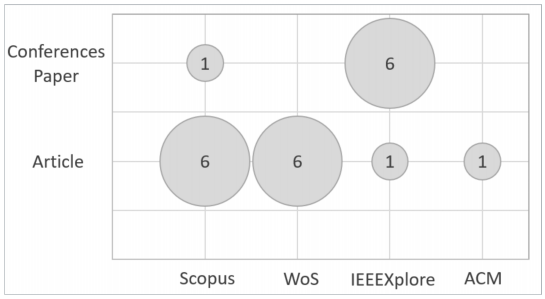


FIGURE 6. Number of articles by type of publication.

fact that only a public BC is used, due to the sensitivity of the data in this medium. In the **Platform**, the authors of the final papers focus on Hyperledger (9/21) and Ethereum (7/21), two platforms that due to their versatility and ability to adapt to different environments can be adapted to the healthcare field. In the **Stade** column, in the types of work that are under development, as is the case of work that presents an experiment, prototype, or PoC, different consensus mechanisms are used and the vast majority use Authorized BC. This denotes that the outlook for the adoption of the technology and its associated technologies in healthcare environments is not clear, generating one more decision to make on the road to implementing a BC solution. It is also noteworthy that 43% (9/21) of the papers present only proposals, evidencing the need for case studies in this environment. In the next section, we will focus on the **Architectural** Mechanism column.

V. ANSWER TO THE RESEARCH QUESTIONS

Taking into account the **RQ1: What architectural mechanism is being used to support the interoperability and security of HMS using BC?** And based on the search string used, we look for those architectural mechanisms that are being used in proposals that use BC in healthcare environments and whose main concerns are to achieve the interoperability and security of the entire ecosystem. In this respect, and as can be seen in Table 2, in the general column called **Architectural Mechanism**, the great majority of the works, 15 papers, use Frameworks as part of their solutions, followed by 3 solutions that use API, likewise, MDE is used by 2 papers and finally in one paper DSL, Metamodels, Gateways, and Intermediaries are used.

Due to the novelty and great breadth of architectural mechanisms in this area of research, we focus on those relevant to answering RQ1 but which also impact our solution presented in section VII.

Architecture modeling commonly uses high-level abstraction called views. **Frameworks** use viewpoints to create views that represent different perspectives of a system model. Specific frameworks being studied may have underlying goals to focus on distributed systems, enterprise architecture, or industry-specific systems [88]. For example, [73] develops a framework for cross-domain image sharing that uses a BC as a distributed data store to establish a ledger of radiological studies and patient-defined access permissions. A framework for BC based data sharing for primary care of oncology patients under cancer treatment is presented by [37]. Likewise, [72] proposes an Electronic Health Record Framework that uses BC technology to securely store the records and maintain a single version of the truth. The stakeholders will have to request permission to access a patient's history and commit the transaction to the distributed ledger. Due to the background presented in the field of SC, the work of SC is interesting [81], since it addresses the field of telesurgery, which provides considerable benefits to society, however, this system currently presents problems of security, privacy, and interoperability, limiting its application at a global level.

TABLE 2. Main aspects found in the final papers. Architectural mechanisms, consensus mechanisms, BC types, platforms, and state of progress of final papers. The checkmark (✓) denotes the existence of this feature within the paper.

Paper	Architectural Mechanism								Consensus	Type BC				Platform			State					
	DSL	Metamodel	API	Gateway	Proxy	Framework	Intermediary	MDE	Consensus Mechanism	Public	Private	Authorized	Consortium	Ethereum	Hyperledger	Other	Proposal	Experiment	Prototype	PoC	Finished	Case Study
[73]						✓			PoS								✓					
[55]						✓			PoA			✓	✓	✓				✓				✓
[74]							✓		DPoS	✓						✓					✓	
[75]						✓							✓				✓					
[37]						✓			PBFT			✓			✓				✓			
[76]			✓									✓			✓		✓					
[77]	✓	✓						✓						✓	✓	✓		✓				✓
[72]			✓			✓						✓			✓		✓			✓		
[78]				✓		✓											✓					
[79]																	✓					
[56]			✓			✓			PoW					✓					✓			✓
[80]						✓			PoW					✓			✓					
[81]						✓			DPoS					✓					✓			✓
[82]						✓			HPF			✓			✓		✓					
[83]									PoS			✓			✓					✓		✓
[22]					✓				PoS											✓		
[84]						✓		✓	Raft			✓			✓				✓			
[40]						✓			QuorumChain					✓			✓					
[85]						✓									✓				✓			✓
[86]					✓										✓				✓			✓
[87]						✓			DPoS					✓					✓			

For this reason, they propose HaBiTs, a framework based on BC and SC, which helps through immutability and interoperability to generate a secure ecosystem, avoiding the requirement of a trusted third party.

Software is typically used by people via a user interface. Increasingly, however, the software is not only used by people, but also by other software applications. This requires another type of interface, an **Application Programming Interface (API)** [89]. APIs offer a simple way for connecting to, integrate with, and extend a software system. APIs represent distributed internet applications that operate in a decentralized P2P network [56]. In some cases, their code is publicly open so that other users can access them. They also serve as a link for on-chain and off-chain data management [72]. They can also interoperate and integrate easily with any HMS, for processes such as data entry [76].

Continuing, we can highlight the work of [77], who proposes a reference model for SC, which allows developers to model and generate the structural code necessary to implement an SC, as a development methodology they propose a feature-oriented domain analysis to generate a **DSL** and thus model and deploy SC between BC platforms. They also present three case studies where they show the validity of the files generated by the DSL, also, in this same work they mention that the MDE, is an indispensable tool to manage the entire process of generating DSLs but it is not used.

In conclusion of the above mentioned, in 15 papers Frameworks are developed as part of their solutions (Table 2), this is in accordance with the study of Anaya [90], which indicates that the natural evolution of software reuse has historically started by generating the source code from scratch. After this, by generating frameworks the evolution of a specific domain is evidenced, as we learn and know a little more in-depth in a particular domain. The next step in this evolution chain is the DSLs, of which we can see that two works are oriented towards this type of contribution, that is, if we already have several consolidated frameworks, we can automate the generation of code through DSLs, which streamlines the entire development process to improve productivity and some other aspects of software quality, such as maintenance and interoperability between systems. It also provides a higher level of abstraction and raises the level of crystalline automation.

To answer **RQ2: What architectural aspects are associated with the interoperability and security of HMS using BC?** Software architectures rarely address functionality. Rather, they address universal *Concerns* common to many different types of software applications. These concerns include so-called ''non-functional'' requirements, such as security, availability, modifiability, performance, reusability, interoperability, etc. The quality attribute is another common term for these general concerns. *Quality Attributes* are critical to producing a satisfactory software product since functionality does not matter when one or more of these quality attributes are not met. For example, one of the primary motivations for upgrading the operating system is to improve security. If an operating system turns out to be insecure, it will

quickly lose popularity no matter how much functionality it provides.

Despite their popularity, *Architectural Patterns* have some weaknesses. One is the fact that an architectural pattern generally addresses multiple quality attribute concerns (or strengths). This feature is problematic because the relationship between a given quality attribute and a pattern is not clearly defined: it depends on implementation decisions, detailed design decisions, and context. This, in turn, makes it difficult for an architect to confidently select a pattern that solves a specific problem at hand [91].

To overcome this weakness, a more detailed design concept that addresses one quality attribute at a time is needed. To address this new emerging need, the idea of *Tactics* has been proposed [11]. Unlike architectural patterns, a tactic is a design decision that influences the achievement of a quality attribute response (e.g., interoperability or security); therefore, they give more precise control to an architect. Tactics confer portability to one design, high performance to another, and integrability to a third [11], [92].

From data extracted from the 21 final papers, we found and organized some concerns related to interoperability and security, several tactics used for resolving these concerns, and a recurrent set of specific scenarios integrating these findings as a BC-based architectural design solution in the healthcare domain. This architectural knowledge could be a tool for software architects for decision-making and researchers, to advance unveiling this knowledge beyond the current state of the art.

To identify the tactics that we are going to use to answer RQ2, the 21 final papers were analyzed for interoperability and security tactics, the tactics found were extracted and classified, and compared with the set of preset tactics documented by Bass et al. [11], in this analysis, we found 12 security tactics and 4 interoperability tactics.

Table 3 summarizes the set of tactics found. The column labeled Code is a code for the identification of the tactic (ST for Security Tactic and IT for Interoperability Tactic, plus a consecutive number), the Paper(s) using that tactic, the category, and the subcategory (according to Figure 7 and Figure 8 explained below) the name of the tactic used and a description. The following explains how these tactics were related in Table 3.

1) SECURITY TACTICS

The summary of the security tactics can be seen in Figure 7, in this figure, it can be seen that the security tactics are classified into 4 subcategories: tactics for Detection, Resistance, Reaction, and Recovery from informatics attacks. In our case, all the identified tactics agree with the Resist attacks subcategory, while three of them: ST3, ST4, and ST5 also agree with the React to attacks subcategory. None of the tactics can be classified in the Detect attacks and recover from attacks subcategories.

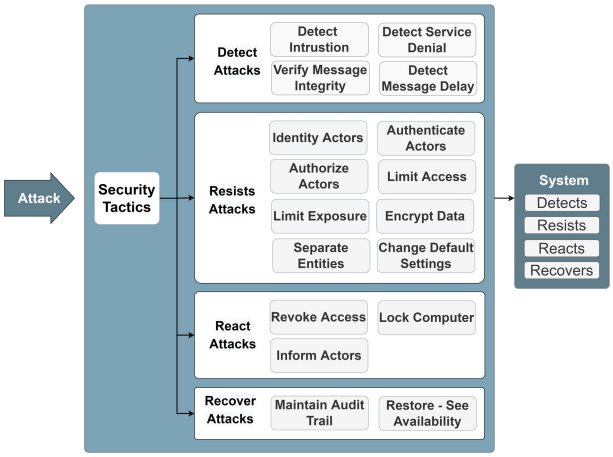


FIGURE 7. Summary of Security tactics. Adopted [11].

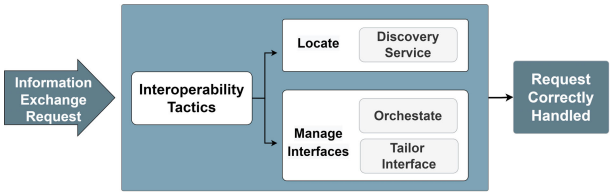


FIGURE 8. Summary of Interoperability tactics. Adopted [11].

2) INTEROPERABILITY TACTICS

Figure 8 shows the set of interoperability tactics. In this case, they are classified into 2 categories: Locate and Manage Interfaces. In our case, all tactics matched the Manage Interfaces subcategory.

Having analyzed the tactics, and relating them within an overall perspective of the RQ2 results. In Figure 9, you can visually see the main players revolving around BC technology related to software engineering. We have adopted the methodology specified by the International Organization for Standardization (ISO)/IEC/IEEE 42010-2011, Systems and Software Engineering-Architecture Description. In this case, a system-of-systems model is created, identifying the main stakeholders, who have some concerns, in this paper, we are going to focus on interoperability and security (dark blue color). To support these concerns, architectural *tactics* are used, including the main domains and subdomains to define and specify the BC technology components. It is worth noting that the codes and colors (white or grey) assigned to the tactics in figure 9 will be used in the analysis in section Synthesis and Discussion (section VI), in the same manner.

All of the above elements were mapped from the final 21 papers on the IEEE 42010 framework presented in [93]. On the right side of Figure 9, you can see some of the technologies associated with BC reviewed in the background. The 4 types of BC, which are used in permisioneess and permissioned domains. Within the process domain, we can find all the consensus mechanisms used by the authors of

TABLE 3. Tactics for interoperability and security found in final papers.

Code	Paper	Tactic Category	Tactic	Description
ST1	[37] [79] [83] [84] [40]	Resist Attacks - Encrypt Data	Proxy Re-encryption	It consists of performing encryption on previously encrypted data, with the purpose of improving the security and privacy of confidential data.
ST2	[79] [83]	Resist Attacks - Encrypt Data	NuCypher Network	NuCypher, enables encryption and reciprocation key management while using a BC-based proxy reciprocation mechanism to securely store and share patient health records. It also gives an access authorization design based on access policy creation.
ST3	[74] [37] [72] [56] [82] [22] [84]	Resist Attacks - Authenticate Actors React Attacks - Revoke Access	Membership Service	Manage identity, privacy and confidentiality in the network. A user is assigned a username and password that will be used to issue the certificate of enrollment and manage their identification.
ST4	[37] [78] [85]	Resist Attacks - Authenticate Actors React Attacks - Revoke Access	Certification Authority	It is the entity that generates and certifies through authenticated certificates for all ecosystem participants, constantly monitoring and controlling the different types of access and permissions.
ST5	[72] [84]	Resist Attacks - Identify Actors Resist Attacks - Revoke Access	Zero Knowledge	Zero Knowledge, is a means by which one part (tester) confirms the another part (verifier) without revealing any information other than the fact that this assertion is true, enhancing privacy.
ST6	[81] [22]	Resist Attacks - Encrypt Data	Attribute-Based Encryption	In ABE, a data owner can encrypt its data and specify access to the data as a boolean formula over a set of attributes.
ST7	[73] [86] [87]	Resist Attacks - Encrypt Data	Encrypt Access Keys	For the exchange of medical images, a pair of cryptographic keys is generated, one for the owner of the image and one for the entity or organization that wants to access the image, using these keys, access permissions are assigned and access is controlled.
ST8	[75] [76] [86] [87]	Resist Attacks - Limit Exposure	Create Anonymous Identity	Using various parameters that identify a patient, it is possible to create a unique identification, generating patient anonymity regardless of the patient's location.
ST9	[80]	Resist Attacks - Encrypt Data	Multilayer Encryption	Two or three layers of encryption are used to enhance data security, e.g. SHA 256 + AES-GCM AWS which is the default encryption of AWS and S3.
ST10	[75] [86] [87]	Resist Attacks - Authorize users	Authorize Users	Authorize Users, sets which system resources the authenticated user will be able to access. Authenticating does not mean that the user will be able to use all resources.
ST11	[75]	Resist Attacks - Authenticate Users	Authenticate Users	Authenticate Users, it is the process of identifying users and ensuring that they are who they say they are.
ST12	[76]	Resist Attacks - Encrypt Data	Encrypt Information	It is the conversion of data from a readable format to an encrypted format, using some encryption protocol or algorithm, e.g., SHA 256.
IT1	[86] [55]	Manage Interfaces - Tailor Interface	Data Translation	It consists data translation using known and universal standards for information management, e.g., use HL7 to ensure both situational and semantic interoperability.
IT2	[85]	Manage Interfaces - Tailor Interface	SNDC	SQL-to/from NoSQL Data Converter: Used for SQL to NoSQL data conversion.
IT3	[85] [55] [79] [81]	Manage Interfaces - Tailor Interface	IPFS	Interplanetary File System: IPFS provides a high-performance content address block storage model with content address hyperlinks, generating a hash that points to on-chain information.
IT4	[74] [78] [72] [22]	Orchestrate - Data Orchestrate	Data Orchestrate	It uses a control mechanism to coordinate, manage and sequence the invocation of particular services, in this case, to send data in or outside the chain.

the final papers. In the data domain, they are divided into on-chain and off-chain data, and in each of these, the different data are stored within the healthcare solutions. In the network domain, the types of networks used in these domains are mentioned. To complement this idea, the work of Wang et al. [94] proposes a novel BC-based solution for secure and auditable private data sharing in smart grids. Furthermore, it discusses the use of on-chain and off-chain SC for a trusted execution environment (TEE) with atomic operation guarantee for confidential processing of user data and reduction of computational overhead in the BC.

VI. SYNTHESIS AND DISCUSSION

We wanted to perform a global analysis of the two previous RQs, where, after the analysis of the reviewed articles, we propose a categorization into 7 different scenarios, in which BC is being used to impact the interoperability and security of HMS. To propose these scenarios, patterns of similarity were identified (e.g., which mechanism is used for the solutions or how BC is used in each solution), and the architectural tactics were reviewed in RQ2. Help researchers in the field and BC application architects and designers to have a clearer picture when approaching possible solutions in the health sector. In addition to being able to use this knowledge to plan the overall design of the software so that details can be added to define the big picture and create a solid foundation for the project. Also how to contribute with some techniques to achieve the desired quality attributes, which in our case are the interoperability and security of the planned solutions.

As previously mentioned, in these high-level diagrams, we will include the related architectural mechanisms in

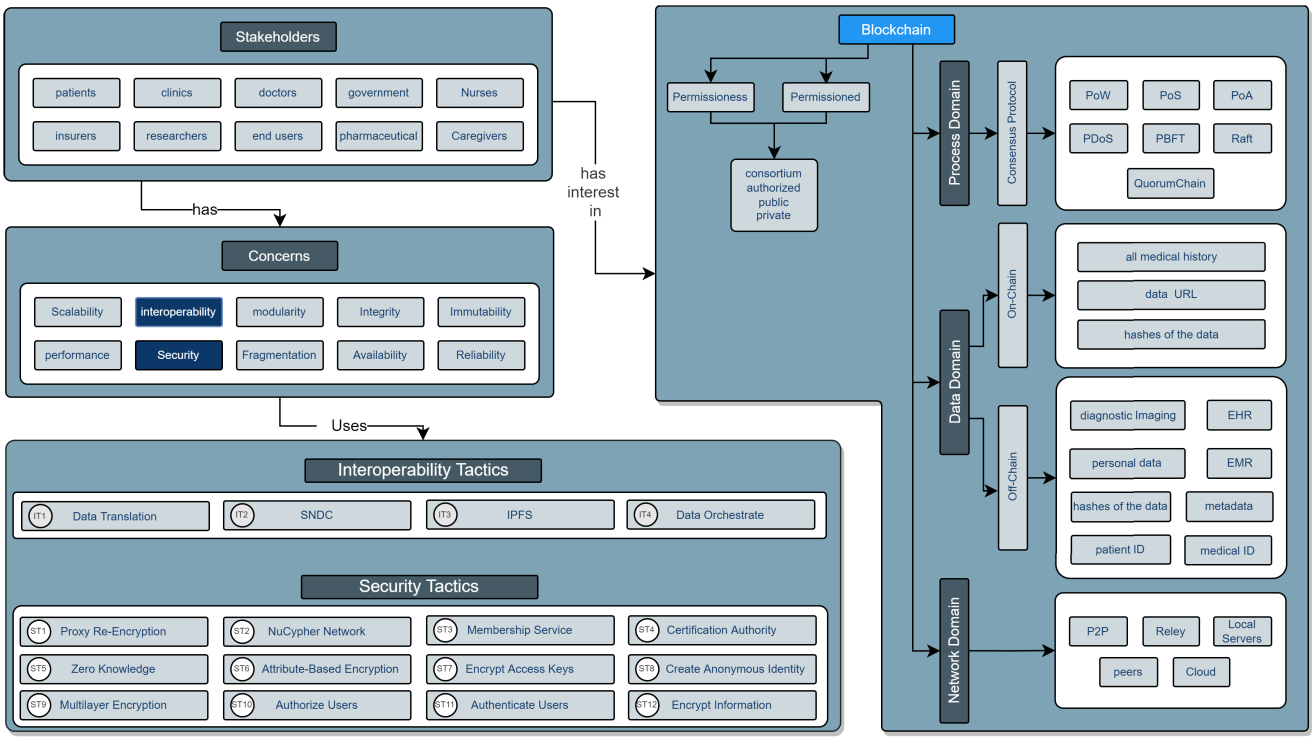


FIGURE 9. Domains and participants in the entire BC ecosystem. Adopted ISO 42010.[6]

TABLE 4. Classification and description of the seven scenarios in the final papers.

Name	Paper	Description
A	[73] [75] [40] [81] [83] [84] [37] [79]	Discusses the use of BC as a data warehouse and on-chain and off-chain data storage. As security tactics, membership (ST3) services can be used to complement on and off-chain data management and networks to manage data encryption and decryption (ST4).
B	[55] [74] [85]	Evidence of the use of an intermediary (relay or proxy) that manages the data between the actors of the healthcare ecosystem. As security tactics, the use of a CA (ST4).
C	[80] [56] [87]	It puts the cloud at the center of healthcare system interoperability and uses other resources such as an API to manage transactions. Even a separate cloud is used to manage security using tactics such as multi-layer encryption (ST9) and other elements such as API and transaction loggers.
D	[78] [86]	It uses the cloud to store data on-chain and a Gateway that manages transactions with the external world. Again a CA for security (ST4) and the creation of anonymous identities (ST8).
E	[76] [72]	It uses an API as an intermediary between on and off-chain data. As a security tactic, the zero knowledge protocol (ST5) is proposed.
F	[82] [77]	The central focus is on SC as connectors of transactions between BC systems. The security tactic of this framework is the SC themselves and membership service (ST3).
G	[22]	Uses one BC as a proxy or connector of the entire healthcare ecosystem within a hierarchy of several BC (known as BC of BCs BoB). As a security tactic, an attribute-based encryption system is proposed (ST6).

the response to RQ1 (green blocks in the diagrams) and the architectural aspects discussed in the response to RQ2 (the tactics were taken from Table 3). We rely on the methodology for describing architectural aspects of Mezaros et al. [95]. This methodology includes a general diagram, a summary, the problem statement, a discussion of concerns from the interoperability and security perspective, and an explanation of some tactics (not all are included due to the length of the paper), all of the above relating the final 21 items.

Table 4 shows the name of the 7 scenarios (named with letters from A to G), the papers that matched each of the scenarios raised, and a description of each scenario.

Diagram interpretation: The diagrams show blue boxes for on-chain data, red boxes for off-chain data, and green boxes for architectural mechanisms (RQ1). In the white boxes with dotted lines, the security (ST) and interoperability (IT) tactics (RQ2). A number (as a superscript) is associated to indicate the number of times the tactic is used in this scenario. Additionally, we distinguish as stakeholders: Patients, physicians, nurses, hospitals, insurers, manufacturers, and suppliers, among others. We also refer to a medical center as a hospital or clinic.

A. ON AND OFF-CHAIN DATA MANAGEMENT

1) OVERVIEW

It presents the interaction of healthcare ecosystem users with on-chain and off-chain data. Figure 10 is the graphical representation of the use of the BC as a data warehouse and

[6]https://www.iso.org/standard/50508.html

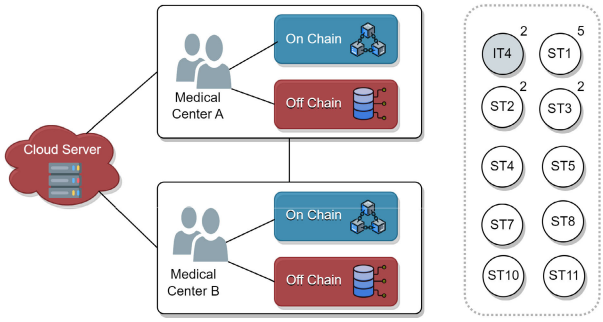


FIGURE 10. High-level representation for scenario A.

off-chain data storage, in addition, the optional use of the cloud as data storage in a BC to improve interoperability is described.

2) PROBLEM

The BC is a constantly growing data structure. The size of the BC is a problem being actively studied, where it is a limiting factor even for simple transactional data stores [73]. The problem increases with the handling of big data. To mention one case, Ethereum, which relies on a block gas limit, makes big data storage practically impossible. On the other hand, considering the sensitive nature and cumbersome handling of healthcare data [37], it makes it necessary to consider its off-chain storage to maintain its privacy and comply with the legal requirements of personal data protection [81].

3) INTEROPERABILITY

Healthcare requires intensive mastery of data of different types and sizes, with large amounts of information generated, accessed, and disseminated daily. Unfortunately, patient records are generally siloed in institution-centric EHRs, resulting in fragmentation with consequences ranging from inefficient care coordination to a lack of critical information during emergencies.

4) ANALYSIS

One possible scenario for improving interoperability is the use of a universally accessible BC, which may consist of data manageable within the BC, including data in a cloud-based BC (Cloud Server Figure 10), [37], [84]. Thus, because participants need only communicate with the BC using recognized interoperability standards (e.g., FHIR) and a single point of connection, document formats, and exchange protocols to follow (each with a security risk and potentially costly to address), a universal and accessible BC minimizes overall risk to the participating entity while enriching information exchange and patient trust [83].

5) TACTICS

It is possible to support patient identity management, we can use a membership server (ST3), which acts as a certificate authority (ST4) to generate the cryptographic keys and their encryption (ST7) so that actors can communicate with confidence [37]. The NuCypher network (ST2) [79], a BC network used to manage encryption and decryption keys, is a decentralized BC-based key management system of access control and encryption service and enables data exchange between users and nodes by proxy reciprocity (ST1) over the network [83]. By delegating rights among multiple nodes, it ensures reliability and availability and avoids a single point of failure. In addition, for off-chain data management on a cloud server, it is possible to use hash pointers using the Interplanetary File System (IPFS) (IT3), which is a decentralized file system whose hash is available to all authorized entities in the BC.

B. CENTRALIZED ON-CHAIN AND OFF-CHAIN DATA MANAGEMENT

1) OVERVIEW

In Figure 11, the central point of the scenario is the use of a Server Relay that is used as an intermediary between all the participants in the network, performs data encryption and re-encryption tasks, and off-chain and on-chain data management.

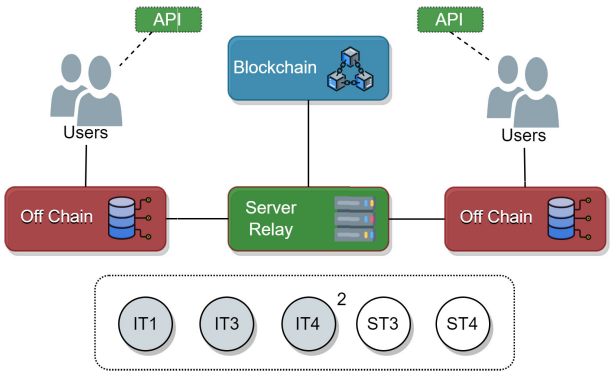


FIGURE 11. High-level representation for scenario B.

2) PROBLEM

Privacy and continuous information management among traditional systems operate independently, where sensitive patient data are recorded and maintained in centralized systems that produce redundant data. In addition, due to the lack of consistency in these systems, the atomicity and integrity of the data are not maintained. Most medical records are valuable for research, but cannot be made public due to security and privacy requirements [85]. Moreover, standalone interoperability between SQL databases (e.g., Oracle or MySQL) and off-chain data using NoSQL databases (e.g., MongoDB or CouchDB), is an ongoing challenge [40].

3) INTEROPERABILITY

The most complicated challenge is HMS interoperability and data exchange with various organizations, which is inescapable for e-government. Also, seamless synchronization and secure communication for interoperability between

various healthcare institutions is an issue that needs to be addressed, as it is crucial to ensure the quality of healthcare services and modern research [85]. Standardization and international cooperation for the dissemination of standards are indispensable to improve the interoperability of e-health services [74].

4) ANALYSIS

An intermediary (server relay in Figure 11) can be applied to enable seamless interactions between separate components in the system while supporting both on-chain and off-chain storage. When applied to BC-based data storage and resolving the tension created by its public and immutable aspects, it is possible to use an intermediary, where simple patient metadata pointing to confidential data or big data, as the case may be, can be exposed on demand to gain access to the actual data [85]. This will also enable fully distributed applications [55] and facilitate the administration of access control policies [85].

5) TACTICS

The Certification Authority (CA) (ST4) provides unique credentials for each element used in the ecosystem. All devices are necessarily registered with the CA, where the CA is the sole authority to generate different certificates and signatures for components and users. Moreover, an application programming interface (API) (in Figure 11) is used to support the integration of hospital and clinic HMS systems online [55], and offline data (IT4). They are also used for data conversion and translation (IT1) installed in the HMS and a relay server connected to the BC to ensure data integrity [74].

C. THE CLOUD AS THE KEY ELEMENT

1) OVERVIEW

Figure 12 shows the cloud as a central element since it is possible to perform on-chain and off-chain data management and security in the cloud, to support the interoperability of the healthcare ecosystem. It is also possible to use APIs as interoperability mechanisms.

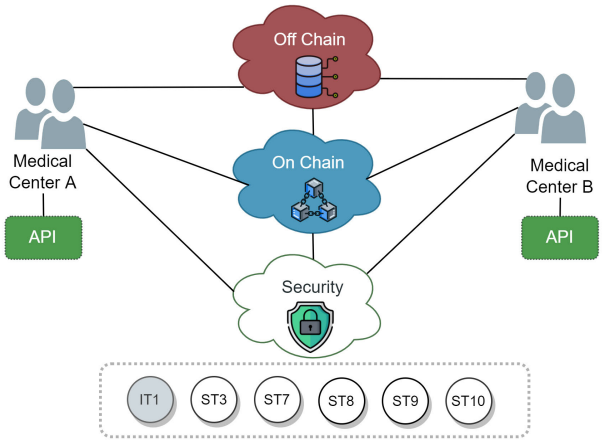


FIGURE 12. High-level representation for scenario C.

2) PROBLEM

EHRs have proven to be indispensable, but several problems remain. One of the most pressing is how to share patient information freely and efficiently [87]. A functional record exchange should require very little user input or time to implement. A system that requires a larger upfront investment in infrastructure, such as data centers or a formalized IT department, is very expensive and Return On Investment (ROI) is difficult to achieve. Hospitals and clinics can share data internally, but there is an inability due to a lack of infrastructure or unwillingness to share data between systems [80].

3) INTEROPERABILITY

The interoperability of healthcare data could improve the quality and efficiency of personal data for healthcare, improving the safety of the medical treatment and promoting the development of new treatments and medicines [87]. This is also of concern to all industry stakeholders who want to manage the entire healthcare process efficiently and with transparency [56].

4) ANALYSIS

We believe that a cloud-based solution enables IT professionals to design data warehouses and security frameworks that can be scaled and manipulated as needed through virtual machines. Rather than using expensive local hardware within data centers, along with BC to provide unadulterated audit trails through transparency and traceability. It is possible to use a mix of cloud web services to communicate and exchange data and relational databases in the cloud for big data storage (e.g., diagnostic imaging) [56]. By using a document repository in the cloud, documents can be stored transparently, securely, reliably, and persistently; in addition, we can also respond immediately to document retrieval requests [87]. Along with the above, we can include an API server, which is a set of decentralized and distributed applications, responsible for managing messages between users and the BC through the SC, in short, it is an intermediary for patient record management [56].

5) TACTICS

We believe that a cloud-based solution enables IT, professionals, to design within the security cloud, there is a decentralized entity in charge of digital identity management, to effectively protect a person's identity across different systems. In this case, multilayer encryption (ST9) is a tactic that uses three layers of encryption to enhance data security, e.g. SHA 256 + AWS of AES-GCM which is the default encryption of AWS and S3. Along with the above, clear and consistent authorization processes (ST10) of all users handling the medical record must be handled clearly and consistently.

D. INTERMEDIARY ELEMENTS BETWEEN PATIENTS AND DATA

1) OVERVIEW

Figure 13 shows the use of architectural mechanisms to manage communication and data provenance between BC and

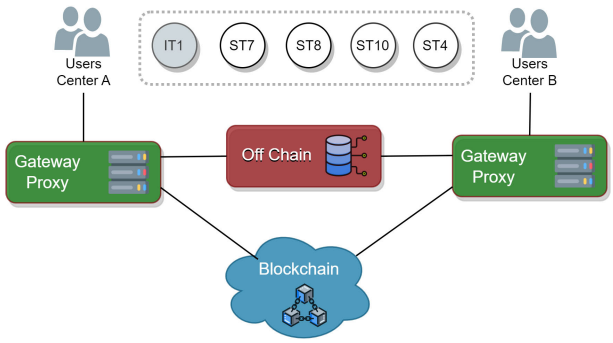


FIGURE 13. High-level representation for scenario D.

off-chain data, such as the use of a Gateway and a Proxy. In addition, they are complemented with a CA to manage authentication and data privacy.

2) PROBLEM

The creation and sharing of EHRs have developed significantly over the past decade, along with multiple associated technologies that aid in better healthcare delivery [78]. However, EHRs are distributed across multiple HMS databases, posing technical and clinical challenges that can jeopardize patient safety [86].

3) INTEROPERABILITY

Recent advances in healthcare research have led to improved interoperable and scalable networks, applications, and services for efficient EHR exchange, however, the global view of healthcare outcomes, over-prescribing, and billing integrity cannot be easily addressed with traditional e-health architecture solutions as they focus more on the needs of clinical, hospital and laboratory uses [78]. The use of BC technology, coupled with an authorization consensus mechanism, can provide a fully decentralized platform while balancing other needs such as privacy and interoperability [86].

4) ANALYSIS

Figure 13 shows the use of an architectural mechanism (proxy or Gateway) that ensures interoperability and data provenance. In the case of the Proxy [86], it can be responsible for transparently intercepting messages and enriching them with provenance metadata managed by the BC SC. Due to the high sensitivity of the data and the number of requirements, such as the size of the healthcare data, it is chosen to store this data off-chain, in this case, only the digital evidence (hash) of the data is stored, guaranteeing privacy. On the other hand, Gateways [78], before each party issues an EHR to document activity, adaptations to a common block syntax are required for healthcare providers and patients to publish those blocks. While BC can use traditional healthcare platforms to enhance processing now they must be enhanced by gateways to tailor requests and responses with BC and ensure interoperability and integrity of information gateways [78].

5) TACTICS

Within this scenario, it is possible to implement on-chain or off-chain (IT2) data storage coordination services, depending on the policies defined for each type of data. Likewise, achieving anonymous patient identity (ST8) is one of the most commonly used security tactics when working with the identification of sensitive diseases and high-cost drugs [87].

E. API AS A COMMUNICATION CENTER

1) OVERVIEW

Figure 14 presents API as an architectural mechanism for achieving interoperability and accessibility of on-chain and off-chain data.

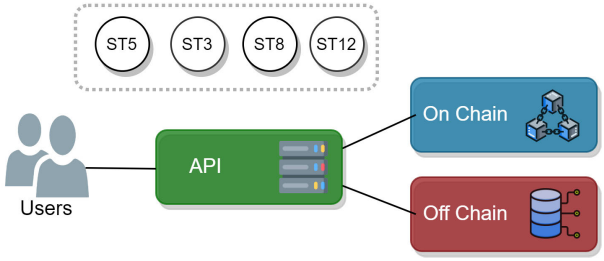


FIGURE 14. High-level representation for scenario E.

2) PROBLEM

The ongoing COVID-19 pandemic has exposed the need for a better data platform to manage health information centered on the patient, who may be isolated at home or in a hospital facility [76]. Common problems in medical services are mainly associated with the physician referral process, data transfer between healthcare institutions, and portals for patients to access their medical information. Specific problems arise, such as sharing health records between institutes or hospitals, problems with misuse of data once shared, lack of security, etc. [72].

3) INTEROPERABILITY

Healthcare data management currently needs a technological upgrade to provide accurate, reliable, and verifiable data for clinicians and researchers to decide on the best medicines and for the public to have their reliable health information history as they go about their daily lives [76]. The use of BC along with API helps improve interoperability and integration with multiple HMS to accelerate their technological adaptation, increasing efficiency in healthcare delivery. Traditionally, healthcare interoperability has focused on data exchange between commercial institutions, such as multiple HMS. Lately, the emphasis has been on patient-driven information exchange, where the exchange of medical information is mediated and driven by the patient [72].

4) ANALYSIS

In addition to the medical record, it becomes essential to have real-time data to achieve constant monitoring of patient

health, so API technology can constantly support this requirement by being able to communicate with other technologies such as IoT sensors, combined with BC to ensure interoperability and security. Having APIs that manage information Write (e.g., registering medical entities that are authorized to create and support transactions) from all participants in the healthcare ecosystem [76] and Read enables third parties to access the recorded data to perform various research actions, such as big data analytics, autonomous learning, and artificial intelligence [76]. These APIs can be integrated into various analytics systems allowing access to data being recorded in real-time from the healthcare organization's internal systems as the patient goes through their consultation processes [72].

5) TACTICS

One of the tactics used to ensure privacy is the zero-knowledge protocol (ST5), in which one party (the tester) confirms to the other party (the verifier) without revealing any information other than the fact that the particular assertion is true. Also, these services use a robust user authentication system (ST11) to identify individual users.

F. INTERACTION THROUGH SMART CONTRACTS

1) OVERVIEW

Figure 15 shows that SC can be the ideal technology for the support of solutions in healthcare environments, due to their status as trust generators, as they avoid the need for a trusted third party in the transactions to be carried out.

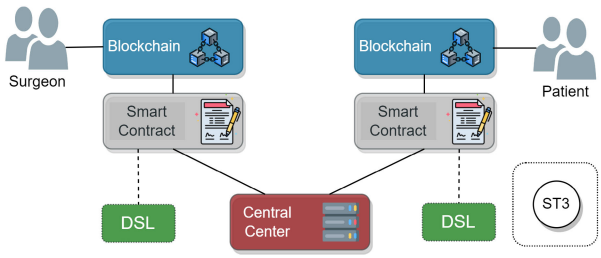


FIGURE 15. High-level representation for scenario F.

2) PROBLEM

Telesurgery has great potential to deliver real-time healthcare surgical services to remote or distant locations with high quality. However, the existing telesurgery system has security, privacy, and interoperability issues, which limits its applicability to healthcare facilities worldwide in the future [82]. On the other hand, SC generation is a latent challenge, due to different factors such as the maturity of the technology or the lack of standards [77].

3) INTEROPERABILITY

All healthcare facilities cannot afford modernization or digitalization to offer remote services to their patients. Therefore, patients and healthcare experts have to travel to health centers for diagnosis, which increases travel time and expenses. Therefore, a critically ill patient cannot go to the nearest health center. In this process, there is a lack of visibility and an inability to track transactions or data stored on servers, both by experts and patient caregivers [82].

4) ANALYSIS

Telesurgery allows surgeons or experts from different locations to work in collaboration, so it is necessary to sign a contract of trust with the healthcare center. This procedure was manual in the traditional system, which requires intermediaries to supervise and execute it. However, BC has the concept of SC as a trust contract, which eliminates the need for intermediaries to supervise and execute it [77]. An SC is a piece of code written in a language (e.g., solidity) or other BC-specific languages to establish trust between all connected parties [82]. This process improves the interoperability of the entire telesurgery ecosystem and creates a climate of trust between all participants. A DSL would allow the SC to be specified at a high level of abstraction, enabling independence from specific technologies and facilitating the reuse of the contract implementation [77].

5) TACTICS

A SC is a portion of code that execute autonomously and automatically due to predefined boolean triggers. These contracts are used to establish trust between all parties connected through BC and also eliminate the need for an intermediary to share data. CAs (ST4) is an indispensable tactic in these types of scenarios where identity verification of surgeons and patients is crucial and sensitive.

G. BLOCKCHAIN OF BLOCKCHAINS BoB

1) OVERVIEW

As can be seen in Figure 16, the BC is being used in different ways in healthcare environments, in this case, it is used as an upper layer of a BoB, acting as a proxy for other lower BCs. This upper layer somehow converges the other layers and coordinates transactions between patients and other actors in healthcare environments.

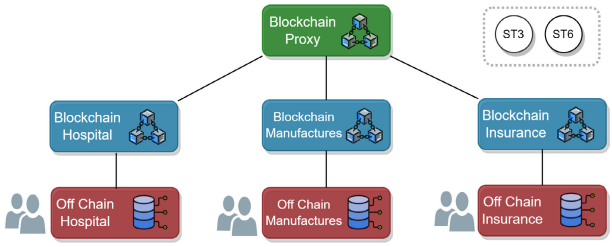


FIGURE 16. High-level representation for scenario G.

2) PROBLEM

Recently, healthcare management systems and devices were primarily stand-alone, disconnected systems. However, modern (customized and non-standardized) healthcare devices can continuously connect and exchange data with other

systems, offering interoperability and improved service delivery, but at the same time can act as enablers of cybersecurity threats [86]. The multitude of domains and stakeholders involved in a healthcare ecosystem and the need to share information also pose significant privacy and security challenges. At the outset, stakeholders must agree on what data can be exchanged within a domain (e.g., within hospitals) or across domains (e.g., between government and hospitals). And because assuming that all stakeholders will agree on a common policy at the same time is unrealistic, technology solutions must be dynamic [86].

3) INTEROPERABILITY

The healthcare ecosystem involves several interconnected stakeholders with different security and privacy needs. Sharing medical data, sometimes generated by remote medical devices, is a challenging task. All healthcare facilities cannot afford to modernize or digitize to provide remote services to their patients. In this process, there is a lack of visibility and an inability to track transactions or data stored on servers, both on the part of experts and patient caregivers [86].

4) ANALYSIS

In Figure 16, a hierarchical architecture can be seen, where, at its top layer, a BC proxy allows independently managed trusted authorities to interoperate. End users from different healthcare domains, such as hospitals or device manufacturers, can securely access and exchange medical data, provided that a commonly agreed domain access policy is enforced. At the lower layer, one or more domain authorities allow each domain (e.g., a hospital) to enforce its policy. In this architecture, SC is used to enforce decentralized policies [86].

5) TACTICS

It is proposed to use an attribute-based encryption ABE (ST6), basically, it is that a data owner can encrypt his data and specify access to it as a boolean formula over a set of attributes. There are two types, key-policy ABE, the encryptor has no control over who has access to the data it encrypts, except for its choice of descriptive attributes; therefore, it must rely on the key issuer to correctly grant or deny access to the appropriate users. Unlike Ciphertext-Policy ABE (CP-ABE), attributes are used to describe user credentials and the cipher can determine a policy on who can decrypt [22].

H. TRADE-OFFS

Trade-offs are common phenomena in software development. Although several solutions in the literature cover non-functional requirements, such as interoperability, as well as security requirements, such as fine-grained access control, balancing them is not an easy task.

The following are some trade-offs derived from the analysis presented in the previous section and which are intended to expose some scenarios in which a balance between interoperability and security is required, all based on the 21 final papers.

1) DATA SHARING

Security concerns are justifiably the primary considerations when using BC technologies to share health information. Historically, the dominant principle for protecting health-related data has been to keep the records themselves generally inaccessible, except to those directly involved in a patient's care. BCs privacy model, however, is more similar to that often used when conducting medical research: the data records themselves are widely accessible, but the patients to whom they relate are secret or anonymous. In this scenario, we must take steps to minimize the risk that an analysis of BC transactions, perhaps combined with external information, could link a public key definitively to a patient [73].

2) DECENTRALIZATION OF INFORMATION

On the one hand, BC eliminates a central point of failure, unlike conventional networks that handle centralized databases. However, because these networks are highly restricted, they may simply reject all network traffic from unauthorized addresses, forcing any attack to be transmitted through one of the few healthcare facilities or providers authorized to communicate with them. Such filtering is not possible in BC in a healthcare environment, where an open network exists without a central authority to limit participation. The attack surface is much larger; each healthcare facility must adequately secure its endpoints within URLs, and each node operator must be sure to guarantee the secrecy of its private keys. However, we note that, due to the decentralized architecture, the exposure of a single private key is unlikely to affect as large as several people as a breach in centralized networks. The ultimate reliance on asymmetric cryptography also means that the loss of private key results in the inability to manage the corresponding resource, requiring some recovery process outside of BC to restore ownership. As with privacy, decentralization results in a more complex security model, probably overall more prone to breaches than a centralized scheme [73].

3) NEED FOR AN INTERMEDIARY

While healthcare BC generally operates without the intervention of an intermediary, a regulated operating authority can still be instituted. When there is occasional non-convergence in BC reconciliation, as demonstrated in the 2014 Bitcoin (e.g., instances of inconsistent and non-converging transaction records), the e-health services industry cannot simply rely on the faith of the underlying BC protocol to resolve these drawbacks, given that time is of the essence in most healthcare services, especially in precise care scenarios [78].

4) API GATEWAY

Before each party issues an EHR to document activity, adaptations to a common block syntax are required for healthcare providers and patients to publish those blocks. While BC can use traditional health platforms to augment processing. They must now be enhanced through adaptive gateways so

that requests and responses can become part of BC. Existing data systems can provide data to influence SC behavior and help to define how communications and data transfer will occur between traditional applications/data and BC through API Gateway calls [77].

5) GATEWAYS

In a healthcare data management system, it is very important to ensure interoperability between different EMR vendors. However, current Architectures offer EHR data-centric storage, and they are vulnerable to cyber-attacks and have some security issues. If this system is hacked, it will inevitably lead to a public crisis. In the framework presented in [87], a secure and confidential gateway is used to store and share a patient's EHR or any CA-compliant clinical document. When an inpatient's EHR is uploaded, the EHR is linked to the correct patient through a patient-matching solution, making it easy for patients to access their aggregated EHR. Therefore, patients can have better collaboration with healthcare providers [87].

VII. AN MDE FRAMEWORK FOR BLOCKCHAIN INTEROPERABILITY AND SECURITY

In this chapter, taking into account the gap that exists in the literature regarding the security and interoperability of BC platforms, and which were evidenced with the RSL, we propose a novel framework consisting of a high-level architecture, whose main objective is the development of a DSL for the specification of SC independent of the BC platform used, to contribute to the interoperability and security of the healthcare environment. In addition, we propose an experiment developed under the MDE methodology, to contextualize this architecture and validate each of the elements required in this solution.

An important aspect of modeling and implementing SC is to define the business process and the rules governing the agreements under which the corresponding actions are executed. Unfortunately, these models use a combination of technical and business-centric terminologies that are different depending on the underlying BC platform targeted by the SC. Most SC are simple programs that define a set of rules that govern the contractual agreement process between the contracting parties (A contractual agreement is a self-executing and verifiable software code). Despite being simple, the development of SC is challenging. This is due to the complexity and heterogeneity of the underlying platforms used to create and implement SC [96]. Different BC platforms use different terminologies and require contract models to be specified according to the syntax defined by the platform.

To address this problem, in this paper, we follow the MDE methodology, which allows for defining improved productivity and some other aspects of software quality, such as maintainability and interoperability between systems. In addition, it provides a higher level of abstraction and raises the level of automation. Consequently, as can be seen in Figure 17 shows a diagram of the proposed architecture, this is a principle mechanism proposed as a Domain Specific Language (DSL) [14], it seeks to contribute to solving the difficulties to address interoperability of HMS through BC technology. A DSL would allow SC to be specified at a high level of abstraction, enabling independence from specific technologies and facilitating the reuse of contract implementation through an MDE approach [15]. In addition, there would be multiple advantages for designers and programmers of SC, independent of the platform on which they are executed. A DSL will allow the designer to abstract SC from different BC implementations with different consensus mechanisms. Additionally, it will contribute to the generation of mature and grounded standards for the modeling of SC used in BC.

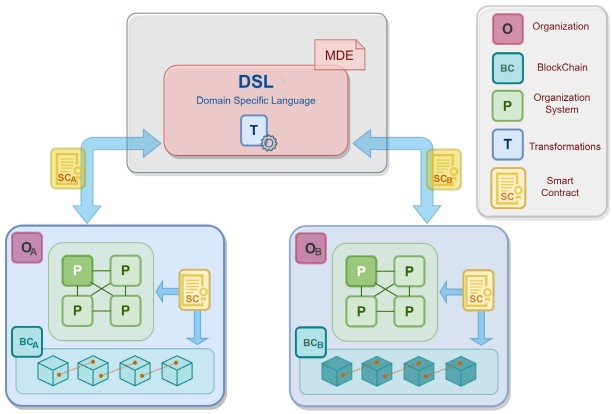


FIGURE 17. General architecture of the proposed experiment.

In Figure 17, we see the lower part of two healthcare organizations (e.g., hospitals), within each of these organizations there are several nodes (colored green) represented with the letter P (the dark green one represents the node that is used as a communication gateway with the other systems), this network of nodes runs SC to manage the information found in the BC (which can be different in each of the organizations).

When one of these organizations needs to communicate with another, it does it by sending an SC to our DSL, which receives the SC, then is validated and applies the MDE process (explained below) required to generate a new compatible SC with the BC of the other organization.

At the central point of the architecture, there is our MDE mechanism, which consists of a DSL that serves as a translator (via an API, Web server, and others) of SC from two or more BC platforms. The DSL will facilitate the generation of SC regardless of the BC platform used and will translate them into the required target platform. In this sense, utilizing MDE to provide a higher level of abstraction and raise the level of automation, which will facilitate the process of the designing and development of SC for architects and developers of BC solutions.

A. EXPERIMENT DESCRIPTION

In Figure 18, we can see the representation using a 4-level architecture, of the entire MDE process required to perform

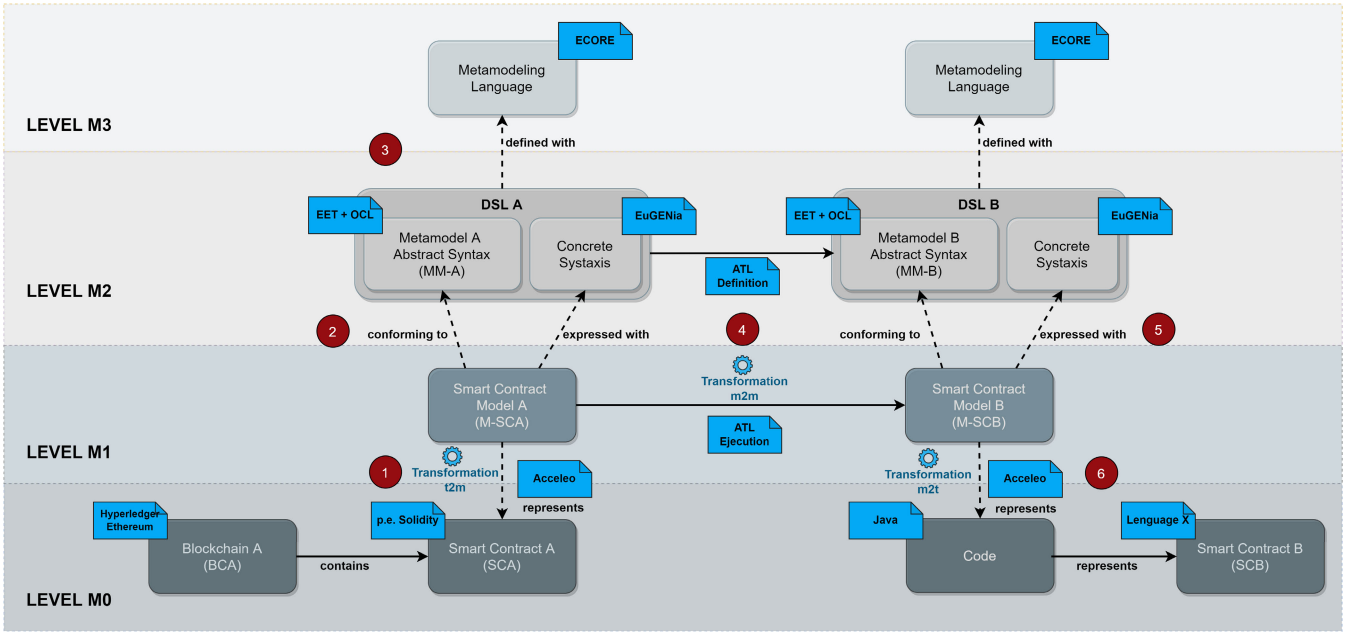


FIGURE 18. Description of the MDE process for the proposed experiment. Based on the 4-level architecture [15].

an experiment designed to translate an SC called SCA, which was generated on a BC platform (e.g., Hyperledger), into another SC called SCB required to be deployed on another target BC platform (e.g., Ethereum). The process depicted in Figure 18 is described below:

Note: the blue boxes mention each of the software tools used in the MDE process.

1) The first thing is to perform a text-to-model transformation (t2m) of the SCA, this process will generate a model (M-SCA) that represents SCA.
2) The M-SCA model is generated by a DSL A, which conforms to a Metamodel A (MM-A) and is expressed with the concrete syntax of the DSL A.
3) In turn, the DSL A is defined with a Metamodeling language (which defines itself).
4) A model-to-model transformation (m2m) is applied to the M-SCA Model to be represented in the SC Model B (M-SCB).
5) Steps 2 and 3 are repeated, but now with M-SCB.
6) A model to text transformation (m2t) is applied to the M-SCB model to generate the SC B (SCB) to be implemented in the BC B (BCB) platform.

This experiment seeks to look at the feasibility and determine if we are working at the right abstraction levels for the generation of SC between different BC platforms. In addition, it will allow us to make adjustments to the process and strengthen the components that are well-defined.

The software tools selected (blue boxes in Figure 18) for the experiment are based on recommendations and significant experience of experts in the area of MDE [15], [64], most of them are compatible with the Eclipse Project[7] and are open source (but allow commercial extensions). Eclipse has made available a set of interesting tools for MDE, which allows a fertile blossoming of initiatives on this platform and comprises popular components for all required modeling tasks.

Eclipse Modeling Framework (EMF) is the core Eclipse technology for MDE. EMF is a good MDE representation tool for several reasons. First, EMF allows the definition of metamodels based on the metamodeling language called Ecore. Second, EMF provides generator components to produce from metamodels (i) a specific Java-based API to manipulate models programmatically and (ii) modeling editors to create models in tree-based editors. Third, EMF comes with a powerful API covering different aspects, such as serializing and deserializing models to/from XMI, as well as powerful reflection techniques. Fourth, based on EMF, several other projects are defined that provide additional functionality to build model-based development support within Eclipse, among these projects we can mention tools such as Acceleo, OCL or EuGENia [15].

VIII. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we conducted a Systematic Literature Review on mechanisms and architectural elements aimed at improving the interoperability and security of HMS using BC. We have systematically analyzed, compared, and discussed 21 papers, corresponding to the same number of interoperability and security solutions in the field of BC technology. By methodologically exploring each of the solutions, this study provides interesting reflections, the first thing is to expose in a clear way the architectural mechanisms used to support solutions using BC in healthcare environments, among these are Frameworks, Gateways, Proxies,

[7]https://www.eclipse.org/modeling/emf/

API, DSL's, MDE, among others. The second thing is to analyze, describe and classify architectural tactics used to solve interoperability and security concerns of HMS using BC. As a third point, we generate 7 high-level scenarios, which represent 7 ways to address the architectural level solutions using BC in the healthcare field, in each of these we describe its context, a problem, analyze interoperability and security concerns, and then describe and analyze some trade-offs used to balance the interoperability and security of the healthcare ecosystem using BC. As a fourth point, We present a MDE Framework for blockchain interoperability and security. This framework consists of a high-level architecture that has as a central element the creation of a DSL that will be used for the translation of SC independently of the BC platform, to validate this architecture, we design an MDE experiment, which will allow us to validate the whole MDE process, This experiment seeks to look at the feasibility and determine if we are working at the right abstraction levels for the generation of SC between different BC platforms. In addition, it will allow us to make adjustments to the process and strengthen the components that are well-defined.

Our results allow us to conclude that the conditions are met to investigate the architectural elements using BC, around the interoperability and security of healthcare environments, allowing a multitude of new use cases. Thus, we expect that interest in this area of research will increase considerably. This work is aimed at making the BC ecosystem more practical, facilitating the work of developers and researchers. We hope that this study will provide a solid and reliable starting point for developers and researchers to work in the research area of software architecture, interoperability, and security of HMS using BC. Finally, we can say that Model-Driven Engineering (MDE) is being used in this type of solution to optimize productivity and improve software quality, maintenance, and interoperability of the entire healthcare ecosystem.

In the near future, we will perform characterization of the different types of SC, for the generation of the metamodels required in the development process of our DSL, then we will proceed with the development process of all the components of the DSL. After this, and to make adjustments and improvements to our experiment, put it in a real context, make measurements, and evaluate our mechanism, we will generate two case studies, the first one is related to the process of patient referral between hospitals that use within their HMS the BC technology, the second study will be related to the management by BC and SC of a dataset of examinations of the functionality of the elderly, this dataset is the result of the 4ie project.[8] Each of these case studies will be evaluated following the Architecture Tradeoff Analysis Method (ATAM) [97], which will allow us to evaluate our software architecture based on the quality attributes of interoperability and security, considered in our system. In future installments, we will publish the results of the case studies and expand the discussion on the trade-offs to be had between interoperability and security of HMS using BC within the healthcare ecosystem.

In future directions, the metaverse is being studied from different approaches along with BC, for example, in the work of [98], which is a literature review that focuses on the study of Metaverse and BC, in this, it is mentioned that interoperability will be the main driver of the metaverse. In the same work, it is mentioned that there are multiple security challenges for the management of health data in the metaverse. There is also the risk of data leakage, manipulation, or loss if the metaverse relies on a central storage system. In this and many cases, BC technology could provide an important role in finding a trade-off between interoperability and security within the metaverse.

[8]http://4ie.spilab.es/

ACKNOWLEDGMENT

The authors express thanks to their respective research groups for enabling and supporting the development of this work: Quercus Software Engineering Group, University of Extremadura; the Research and Development Group in Software Engineering IDIS, Faculty of Electronic Engineering and Telecommunications, University of Cauca; and the Davinci Research Group, National Open and Distance University (UNAD).

REFERENCES

[1] *Universal Health Coverage*, World Health Organization, Geneva, Switzerland, 2022.

[2] V. P. Aggelidis and P. D. Chatzoglou, "Using a modified technology acceptance model in hospitals," *Int. J. Med. Informat.*, vol. 78, no. 2, pp. 115–126, 2009.

[3] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records," *J. Biomed. Inform.*, vol. 71, pp. 70–81, Jul. 2017.

[4] N. Spence, M. N. Bhardwaj, and D. Paul, "Ransomware in healthcare facilities: A harbinger of the future?" *Perspect. Health Inf. Manage.*, vol. 10, pp. 1–22, Jul. 2018.

[5] N. Thamer and R. Alubady, "A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research," in *Proc. 1st Babylon Int. Conf. Inf. Technol. Sci. (BICITS)*, Apr. 2021, pp. 210–216.

[6] T. Benson, *Principles of Health Interoperability HL7 and SNOMED*, 2nd ed. New York, NY, USA: Springer, 2012, pp. 1–316.

[7] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, vol. 5, p. 21260, Oct. 2008.

[9] C. Burniske, E. Vaughn, J. Shelton, and A. Cahana, *How Blockchain Technology Can Enhance EHR Operability*. St. Petersburg, FL, USA: Ark Invest, 2016.

[10] A. M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *J. Med. Internet Res.*, vol. 13, no. 3, p. e67, Sep. 2011.

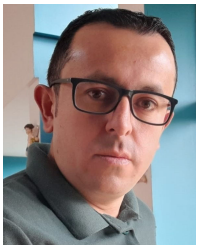
[11] L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice*. London, U.K.: Pearson, 2012.

[12] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Inf. Softw. Technol.*, vol. 55, no. 12, pp. 2049–2075, 2013.

[13] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. 12th Int. Conf. Eval. Assessment Softw. Eng.*, 2008, pp. 68–77.

[14] I. Kurtev, J. Bézivin, F. Jouault, and P. Valduriez, "Model-based DSL frameworks," in *Proc. Companion 21st ACM SIGPLAN Symp. Object-Oriented Program. Syst., Lang., Appl.*, 2006, pp. 602–616.
[15] M. Brambilla, J. Cabot, M. Wimmer, and L. Baresi, *Model-Driven Software Engineering in Practice*, 2nd ed. San Rafael, CA, USA: Morgan & Claypool, 2017.
[16] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.
[17] E. Dulce and J. Hurtado, "The role of the blockchain technology in the elderly care solutions: A systematic mapping study," in *Proc. Int. Workshop Gerontechnol.* Cham, Switzerland: Springer, 2021, pp. 23–34.
[18] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.
[19] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "Blockchain technology in the healthcare industry: Trends and opportunities," *J. Ind. Inf. Integr.*, vol. 22, Jun. 2021, Art. no. 100217.
[20] A. I. Aljazaery, H. T. S. Alrikabi, and M. R. Aziz, "Combination of hiding and encryption for data security," *Int. J. Interact. Mobile Technol.*, vol. 14, pp. 34–47, Jan. 2020.
[21] L. Ismail and H. Materwala, "BlockHR: A blockchain-based framework for health records management," in *Proc. 12th Int. Conf. Comput. Modeling Simulation*, Jun. 2020, pp. 164–168.
[22] V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, "A hierarchical multi blockchain for fine grained access to medical data," *IEEE Access*, vol. 8, pp. 134393–134412, 2020.
[23] O. O'Donoghue, A. A. Vazirani, D. Brindley, and E. Meinert, "Design choices and trade-offs in health care blockchain implementations: Systematic review," *J. Med. Internet Res.*, vol. 21, no. 5, May 2019, Art. no. e12426.
[24] A. R. Bartolomé, J. M. Moral Ferrer, D. Tapscott, A. Tapscott, A. I. D. Santos, V. Koulaidis, J. P. Schmidt, M. Sharples, J. Domingue, and N. Smolenski, "Blockchain en educación: Cadenas rompiendo moldes," *Learn., Media Social Interact.*, vol. 3, no. 2, pp. 95–97, 2018.
[25] J. Martinez-Gil, M. Pichler, T. Beranic, L. Brezocnik, M. Turkanovic, G. Lentini, F. Polettini, A. Lué, A. C. Vitale, G. Doukhan, and C. Belet, "Framework for assessing the smartness maturity level of villages," in *Proc. Eur. Conf. Adv. Databases Inf. Syst.* Cham, Switzerland: Springer, 2019, pp. 501–512.
[26] A. W. Abreu and E. F. Coutinho, "A pattern adherence analysis to a blockchain web application," in *Proc. IEEE Int. Conf. Softw. Archit. Companion (ICSA-C)*, Mar. 2020, pp. 103–109.
[27] H.-A. Lee, H.-H. Kung, J. G. Udayasankaran, B. Kijsanayotin, A. B. Marcelo, L. R. Chao, and C.-Y. Hsu, "An architecture and management platform for blockchain-based personal health record exchange: Development and usability study," *J. Med. Internet Res.*, vol. 22, no. 6, Jun. 2020, Art. no. e16748.
[28] I. Qasse, S. Mishra, and M. Hamdaqa, "iContractBot: A chatbot for smart Contracts' specification and code generation," in *Proc. IEEE/ACM 3rd Int. Workshop Bots Softw. Eng. (BotSE)*, Jun. 2021, pp. 35–38.
[29] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Informat.*, vol. 35, no. 8, pp. 2337–2354, 2018.
[30] H. Jin, X. Dai, and J. Xiao, "Towards a novel architecture for enabling interoperability amongst multiple blockchains," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2018, pp. 1203–1211.
[31] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 160–209, 1st Quart., 2022.
[32] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and A. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.
[33] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Comput. Surv.*, vol. 54, no. 8, pp. 1–41, Nov. 2022.
[34] M. Marwan, A. A. Temghart, F. Sifou, and F. AlShahwan, "A decentralized blockchain-based architecture for a secure cloud-enabled IoT," *J. Mobile Multimedia*, vol. 2020, pp. 389–412, Nov. 2020.
[35] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F. Wang, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Trans. Computat. Social Syst.*, vol. 5, no. 4, pp. 942–950, Dec. 2018.
[36] M. Snider, K. Samani, and T. Jain, "Delegated proof of stake: Features & tradeoffs," Multicoin Capital, Austin, TX, USA, Tech. Rep., 19, 2018.
[37] A. Dubovitskaya, Z. Xu, and S. Ryu, "Secure and trustable electronic medical records sharing using blockchain," in *Proc. AMIA Annu. Symp.*, 2017, p. 650.
[38] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.
[39] Y. Li, Y. Zhang, W. Huang, X. Zhang, R. Mo, and J. Song, "Privacy-aware real estate recommendation in cloud for elderly care based on historical consumption behaviors," *IEEE Access*, vol. 9, pp. 41558–41565, 2021.
[40] G. Dagher, J. Mohler, and M. Milojkovic, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.
[41] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private blockchains," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 172–181, Jan. 2020.
[42] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021.
[43] K. M. Kina-Kina, H. E. Cutipa-Arias, and P. Shiguihara-Juarez, "A comparison of performance between fully and partially decentralized applications," in *Proc. IEEE 26th Int. Conf. Electron., Electr. Eng. Comput. (INTERCON)*, Aug. 2019, pp. 1–4.
[44] X. Xu, C. Pautasso, L. Zhu, Q. Lu, and I. Weber, "A pattern collection for blockchain-based applications," in *Proc. 23rd Eur. Conf. Pattern Lang. Programs*, Jul. 2018, pp. 1–20.
[45] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, Jul. 2016, vol. 310, no. 4, pp. 1–4.
[46] V. Reniers, D. Van Landuyt, P. Viviani, B. Lagaisse, R. Lombardi, and W. Joosen, "Analysis of architectural variants for auditable blockchain-based private data sharing," in *Proc. 34th ACM/SIGAPP Symp. Appl. Comput.*, Apr. 2019, pp. 346–354.
[47] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.
[48] N. Szabo, "Formalizing and securing relationships on public networks," *1st Monday*, vol. 2, no. 9, Sep. 1997.
[49] B. Aldughayfiq and S. Sampalli, "Digital health in physicians' and pharmacists' office: A comparative study of e-prescription systems' architecture and digital security in eight countries," *OMICS, J. Integrative Biol.*, vol. 25, no. 2, pp. 102–122, Feb. 2021.
[50] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "BlockChain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018.
[51] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4585–4600, Jun. 2019.
[52] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "FogBus: A blockchain-based lightweight framework for edge and fog computing," *J. Syst. Softw.*, vol. 154, pp. 22–36, Aug. 2019.
[53] M. M. H. Onik and M. H. Miraz, "Performance analytical comparison of blockchain-as-a-service (baas) platforms," in *Proc. Int. Conf. Emerg. Technol. Comput.* Cham, Switzerland: Springer, 2019, pp. 3–18.
[54] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2009–2030, 3rd Quart., 2020.
[55] Y.-S. Lo, C.-Y. Yang, H.-F. Chien, S.-S. Chang, C.-Y. Lu, and R.-J. Chen, "Blockchain-enabled iWellChain framework integration with the national medical referral system: Development and usability study," *J. Med. Internet Res.*, vol. 21, no. 12, Dec. 2019, Art. no. e13563.
[56] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 310–317.
[57] H. T. Vo, Z. Wang, D. Karunamoorthy, J. Wagner, E. Abebe, and M. Mohania, "Internet of Blockchains: Techniques and challenges ahead," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1574–1581.

[58] E. Mossialos, R. Baeten, G. Permanand, and T. K. Hervey, *Health Systems Governance in Europe: The Role of European Union Law and Policy*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[59] *Additional Guidance Regarding the Vigilance System as Outlined in Meddev 2.12-1 Rev. 8, Directorate- General for Internal Market, Industry, Entrepreneurship and SMEs. Unit GROW D.4Health Technology and Cosmetics*, Comission Europea, Brussels, Belgium, 2019.
[60] B. Appleton, "Patterns and software: Essential concepts and terminology," Motorola Cellular Infrastruct. Group, Chicago, IL, USA, Tech. Rep., 1997.
[61] D. Garlan, "Software architecture: A roadmap," in *Proc. Conf. Future Softw. Eng.*, 2000, pp. 91–101.
[62] *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*, IEEE Standard 610, pp. 1–217, 1991.
[63] *Revisión de Estándares de Interoperabilidad Para la Esalud en Latinoamérica y el Caribe*, Organización Panamericana de la Salud, Washington, DC, USA, 2016.
[64] J. García, M. Félix, O. G. Rubio, V. Pelechano, A. Vallecillo, J. M. Vara, and C. Vicente-Chicote, "Desarrollo de software dirigido por modelos conceptos, métodos y herramientas," Universidad Nacional de la Plata, La Plata, Argentina, Tech. Rep., 2010.
[65] M. Petticrew and H. Roberts, *Systematic Reviews in the Social Sciences: A Practical Guide*. Hoboken, NJ, USA: Wiley, 2008.
[66] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in Software Engineering*. Cham, Switzerland: Springer, 2012.
[67] T. Meline, "Selecting studies for systemic review: Inclusion and exclusion criteria," *Contemp. Issues Commun. Sci. Disorders*, vol. 33, pp. 21–27, Mar. 2006.
[68] T. Dyba, T. Dingsoyr, and G. K. Hanssen, "Applying systematic reviews to diverse study types: An experience report," in *Proc. 1st Int. Symp. Empirical Softw. Eng. Meas. (ESEM)*, Sep. 2007, pp. 225–234.
[69] O. Revelo-Sánchez, C. A. Collazos-Ordóñez, and J. A. Jiménez-Toledo, "El trabajo colaborativo como estrategia didáctica para la enseñanza-/aprendizaje de la programación: Una revisión sistemática de literatura," *TecnoLógicas*, vol. 21, no. 41, pp. 115–134, Jan. 2018.
[70] A. Serenko, N. Bontis, L. Booker, K. Sadeddin, and T. Hardie, "A scientometric analysis of knowledge management and intellectual capital academic literature (1994–2008)," *J. Knowl. Manage.*, vol. 14, no. 1, pp. 3–23, Feb. 2010.
[71] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.
[72] S. N. Dass and R. Chinnaiyan, "A blockchain based electronic medical health records framework using smart contracts," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2021, pp. 1–4.
[73] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Inform. J.*, vol. 25, no. 4, pp. 1398–1411, 2018.
[74] Y.-S. Bae, Y. Park, T. Kim, T. Ko, M.-S. Kim, E. Lee, H.-C. Kim, and H.-J. Yoon, "Development and pilot-test of blockchain-based MyHealth-Data platform," *Appl. Sci.*, vol. 11, no. 17, p. 8209, Sep. 2021.
[75] X. Du, B. Chen, M. Ma, and Y. Zhang, "Research on the application of blockchain in smart healthcare: Constructing a hierarchical framework," *J. Healthcare Eng.*, vol. 2021, pp. 1–13, Jan. 2021.
[76] O. Musa, L. S. Yun, and R. Ismail, "UPLX: Blockchain platform for integrated health data management," in *Proc. Int. Conf. Reliable Inf. Commun. Technol.*, in Lecture Notes on Data Engineering and Communications Technologies, vol. 72, 2021, pp. 10–18.
[77] M. Hamdaqa, L. A. P. Metz, and I. Qasse, "iContractML: A domain-specific language for modeling and deploying smart contracts onto multiple blockchain platforms," in *Proc. 12th Syst. Anal. Modeling Conf.*, Oct. 2020, pp. 34–44.
[78] W. Liu, S. Zhu, and T. Mundie, "Advanced block-chain architecture for e-health systems," in *Proc. IEEE 19th Int. Conf. E-Health Netw., Appl. Services (Healthcom)*, Oct. 2017, pp. 1–6.
[79] M. Abouali, K. Sharma, O. Ajayi, and T. Saadawi, "Blockchain framework for secured on-demand patient health records sharing," in *Proc. IEEE 12th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Dec. 2021, pp. 35–40.
[80] G. Carter, H. Shahriar, and S. Sneha, "Blockchain-based interoperable electronic health record sharing framework," in *Proc. IEEE 43rd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jul. 2019, pp. 452–457.
[81] A. Abugabah, N. Nizamuddin, and A. A. Alzubi, "Decentralized telemedicine framework for a smart healthcare ecosystem," *IEEE Access*, vol. 8, pp. 166575–166588, 2020.
[82] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Aug. 2019, pp. 1–5.
[83] R. H. Hylock and X. Zeng, "A blockchain framework for patient-centered health records and exchange (HealthChain): Evaluation and proof-of-concept study," *J. Med. Internet Res.*, vol. 21, no. 8, Aug. 2019, Art. no. e13592.
[84] Q. Wang and S. Qin, "A hyperledger fabric-based system framework for healthcare data management," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, 2021, pp. 132–137.
[85] Y. Liu, G. Shan, Y. Liu, A. Alghamdi, I. Alam, and S. Biswas, "Blockchain bridges critical national infrastructures: E-Healthcare data migration perspective," *IEEE Access*, vol. 10, pp. 28509–28519, 2022.
[86] A. Margheri, M. Masi, A. Miladi, V. Sassone, and J. Rosenzweig, "Decentralised provenance for healthcare data," *Int. J. Med. Informat.*, vol. 141, Sep. 2020, Art. no. 104197.
[87] H. Wu, Y. Shang, L. Wang, L. Shi, K. Jiang, and J. Dong, "A patient-centric interoperable framework for health information exchange via blockchain," in *Proc. 2nd Int. Conf. Blockchain Technol. Appl.*, Dec. 2019, pp. 76–80.
[88] A. Tang, J. Han, and P. Chen, "A comparative analysis of architecture frameworks," in *Proc. 11th Asia–Pacific Softw. Eng. Conf.*, 2004, pp. 640–647.
[89] M. Biehl, *API Architecture: The Big Picture for Building APIs*. Zürich, Switzerland: API-University Press, 2015.
[90] R. Anaya, "Un acercamiento a la reutilización en ingeniería de software," *Revista Universidad EAFIT*, vol. 35, no. 114, pp. 51–63, 1999.
[91] J. Ryoo, P. Laplante, and R. Kazman, "A methodology for mining security tactics from security patterns," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, 2010, pp. 1–5.
[92] A. C. Ordonez-Guerrero, J. D. Munoz-Garzon, E. R. D. Villarreal, A. Bandi, and J. A. Hurtado, "Blockchain architectural concerns: A systematic mapping study," in *Proc. IEEE 19th Int. Conf. Softw. Archit. Companion (ICSA-C)*, Mar. 2022, pp. 183–192.
[93] C. Lima, "Developing open and interoperable DLT/blockchain standards," *Computer*, vol. 51, no. 11, pp. 106–111, Nov. 2018.
[94] Y. Wang, Z. Su, N. Zhang, J. Chen, X. Sun, Z. Ye, and Z. Zhou, "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7688–7699, Nov. 2021.
[95] G. Meszaros and J. Doble, "A pattern language for pattern writing," in *Pattern Languages of Program Design*, vol. 3. Boston, MA, USA: Addison-Wesley, 1998, pp. 529–574.
[96] W. Zou, D. Lo, P. S. Kochhar, X.-B. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, "Smart contract development: Challenges and opportunities," *IEEE Trans. Softw. Eng.*, vol. 47, no. 10, pp. 2084–2106, Oct. 2021.
[97] R. Kazman, M. Klein, M. Barbacci, T. Longstaff, H. Lipson, and J. Carriere, "The architecture tradeoff analysis method," in *Proc. 4th IEEE Int. Conf. Eng. Complex Comput. Syst.*, Aug. 1998, pp. 68–78.
[98] T. R. Gadekallu, T. Huynh-The, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. B. da Costa, and M. Liyanage, "Blockchain for the metaverse: A review," 2022, *arXiv:2203.09738*.



EDGAR R. DULCE VILLARREAL received the degree in systems engineering from the University of Nariño, Pasto, Colombia, in 2008, the Specialist degree in networks and telematic services from the University of Cauca, Colombia, in 2009, and the master's degree in computer security from the International University of La Rioja, Spain, in 2017. He is currently pursuing the Ph.D. degree in electronics sciences with the University of Cauca. He is doing his doctoral internship with the Research Group Quercus Software Engineering Group, directly at the SPILab, University of Extremadura, Spain. He is also a full-time Professor in the specialization in cybersecurity at UNAD, Colombia. He is a Reviewer and an Evaluator of projects in the IEEE IBEROAMERICAN JOURNAL OF LEARNING TECHNOLOGIES. His research interests include cybersecurity, software engineering, and blockchain in healthcare environments.

JOSE GARCÍA-ALONSO (Member, IEEE) received the Ph.D. degree in software engineering from the University of Extremadura, Spain, in 2014. He is currently an Associate Professor with the University of Extremadura. He is also the Co-Founder of Gloin, a software consulting company, and Health and Aging Tech, an eHealth company. His research interests include software engineering, mobile computing, pervasive computing, eHealth, and gerontechnology.

ENRIQUE MOGUEL received the M.Sc. degree in computer science from the University Carlos III, Spain, in 2010, and the Ph.D. degree in computer science from the University of Extremadura, Spain, in 2018. He is a Researcher at Extremadura Supercomputing, Technological Innovation and Research Center. He is currently an Assistant Professor with the University of Extremadura. He is also the Co-Founder of Health and Aging Tech, an eHealth company. His research interests include software engineering, smart systems, eHealth, and quantum computing.

JULIO ARIEL HURTADO ALEGRÍA received the degree in electronics and telecommunications engineering from the Universidad del Cauca, in 1997, the Specialist degree in software development processes from the Universidad San Buenaventura, in 2002, and the Ph.D. degree in computer science from the Universidad de Chile, in 2012. His research interests include development processes, architectures, and software reuse. In recent years, he has been researching the development of computational thinking and aspects related to process design and situational collaborative methods in different scenarios of software construction.