

A comprehensive survey on blockchain-based healthcare industry: applications and challenges

Sara Ait Bennacer¹, Khadija Sabiri², Abdessadek Aaroud¹, Khalid Akodadi¹, Bouchaib Cherradi^{1,3}

¹LaROSERI Laboratory, Department of computer sciences, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco

²Fraunhofer Portugal AICOS, Rua Alfredo Allen, Porto, Portugal

³STIE Team, CRMEF Casablanca-Settat, El Jadida, Morocco

Article Info

Article history:

Received Sep 3, 2022

Revised Dec 18, 2022

Accepted Jan 27, 2023

Keywords:

Blockchain technology

Data management

Data security and privacy

Data sharing

Electronic health record

Healthcare

ABSTRACT

Blockchain has attracted a lot of interest since its publication because to its unique characteristics of immutability, decentralization, smart contract, and consensus mechanism. Today's healthcare systems are facing many issues in the era of digital health transformation and the growth of electronic health records. Blockchain has the potential to provide solutions to a variety of electronic health record (EHR)-related challenges, including data management, security, data sharing and patient privacy. This paper represents a blockchain-based healthcare industry survey; it includes many research publications in high-ranking scientific journals in recent years from 2016 to 2022. We adopt the preferred reporting items for systematic reviews and meta-analyses (PRISMA) approach and aspects. This work is based on five databases: Elsevier, Springer, IEEE Xplore, PubMed, and MDPI. The number of studies included in this study was 56. We found that researchers attempted to use blockchain technology to assist patients and healthcare providers in diagnosis and data processing, as well as including multiple entities. Our study discusses the potential of blockchain technology, its roles and benefits in healthcare, aiming to solve several problems such as data management, data sharing, access control, data security and privacy, which are missed in the conventional healthcare system.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Sara Ait Bennacer

LaROSERI Laboratory, Department of computer sciences, Faculty of Sciences

Chouaib Doukkali University

24000, El Jadida, Morocco

Email: aitbennacer.sara@gmail.com

1. INTRODUCTION

Blockchain technology, by providing more secure and efficient electronic medical records (EMRs), could provide a novel concept for healthcare data exchange. For healthcare treatment and diagnosis, electronic health record (EHRs) contain crucial and sensitive personal information [1], [2]. By positioning the patient at the heart of the healthcare system and enhancing the data management, sharing information, security, privacy, interoperability, and monitoring of the health data, blockchain technology can change the healthcare sector [3]. Immutability, decentralization, transparency, and traceability are just a few of the features that make blockchain technology appropriate for use in healthcare. The term "Blockchain" refers to a unique, decentralized and distributed ledger containing all the participating members' transaction records [4]. Blockchain is a distributed ledger system, enabling peer-to-peer (P2P) networked digital data transactions that can be distributed openly or privately to all users, allowing any data structure to be stored in a reliable and trustworthy manner [5], [6]. Blockchain concept [7] is what grants the trustworthy execution of transactions among multiple parties with

no need for a third party to verify or trust authority. According to Zheng *et al.* [8], blockchain technology has recently been applied in a wide range of industries, such as banking, e-healthcare, public serviceability, asset management, government policies, real estate, logistics, and supply chain management. The integration of blockchain applications the healthcare industry has been proven beneficial in terms of providing secure data and managing medical data. Furthermore, blockchain is successfully emerging traditional medical techniques, such as detecting and treating issues efficiently due to secure data sharing. There is no doubt that blockchain in the future is going to be utilized to personalize, legitimize, and secure healthcare by integrating information from medical records and distributing it safely and securely [9], [10].

In addition, machine learning technology may assist healthcare practitioners in developing accurate medication treatments that are tailored to individual features by processing vast amounts of data. Predictive modeling using historical EHR data may also advance personalized disease and raise the quality of diagnosis through machine learning [11]–[15]. The main contributions of this systematic literature survey are as follows:

- In this survey, we explore research that provides conceptual approaches, the experimental results, the prototypes, and the implementations of blockchain for managing EHRs, EMRs, or any type of health care management system. We outline the fundamental knowledge and concepts of the blockchain to help understand its potential in the healthcare domains. This listing of references presents the interesting research, authors' contributions, and emerging solutions for the integration of blockchain in healthcare.
- Further, we demonstrate the perspectives on different implementations and application domains supported by recent studies. This paper includes the major problems about health patients' data, providers, healthcare stakeholders and hospitals, which we define in data management, data sharing, confidentiality of medical information, user identity, electronic health record management, and data privacy and security.
- The survey also aims to highlight the main issues and develop outstanding research questions which should be considered by academics and experts in the field. This systematic review, specifically, outlines the future research scope's suggestions for the wider implications on blockchain in healthcare.

This literature survey is organized as follows; section 2 presents the research methodology; section 3 describes the blockchain technology background. While, section 4 provides the related work in blockchain healthcare application and section 5 is dedicated to presenting the blockchain implementation cases in the healthcare industry. Then, section 6 discusses and summarizes all the problems concerning the reviews cited below. Finally, we conclude our survey in section 7.

2. RESEARCH METHOD

The preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement was first released more than a decade ago [3]. The PRISMA statement was developed to help authors better report on systematic reviews and meta-analyses. Health decision makers consider systematic reviews as an essential resource for information that is synthesized in a systematic and transparent manner [16]. The authors' proposed approach in the study Briner and Denyer [17], and some aspects of the PRISMA statement in Moher [18] provided a comprehensive, systematic and scientific review of blockchain-driven applications for healthcare. The literature survey (Figure 1) includes the most recent research on the blockchain technology applied in the healthcare industry. The following activities determined the systemic survey presented.

2.1. Research questions

The research questions discussed in our study:

RQ1: What are the problems that the current healthcare system suffers from?

RQ2: What is the blockchain key benefit in healthcare applications?

RQ3: Why should healthcare providers be interested in adopting blockchain technology in their healthcare system?

RQ4: What are the authors' contributions to integrating blockchain into healthcare?

RQ5: What are the different blockchain architectural models, types, and approaches?

RQ6: How can blockchain support and manage the HER among different healthcare actors?

RQ7: What are the different blockchain developed applications in healthcare?

RQ8: What are the blockchain application challenges, emerging trends and limitations in the healthcare sector?

2.2. Search strategy

It was conducted according to five databases: Elsevier, Springer, IEEE, PubMed, and MDPI. These databases were chosen based on many journal articles, reviews and surveys on novel topics, such as blockchain technology. Papers identification using the Query '(blockchain OR blockchain technology) AND (healthcare OR health OR data management OR data sharing OR smart contract OR EHR OR EMR)'

2.3. Article selection

After we obtained the articles, we applied the inclusion and exclusion criteria below to designate the articles to be considered for our final survey. The inclusion criteria define the studies included in this study. The result present the total of articles used in this survey.

2.3.1. Inclusion criteria

The including criteria are presented as list:

- Studies published in English language.
- Studies published in journal articles, review and survey only.
- The main contribution of this research is the blockchain in the healthcare sector.
- Research paper (architecture, proposed system, uses cases, designs, framework, platform, scheme, model, approach, transaction location, and model storage) allied to the utilization of blockchain in the healthcare industry.
- Studies during the period 2016 to 2021.

2.3.2. Excluding criteria

The excluding criteria are listed:

- Studies not published in English language.
- Excluded conference proceedings, book chapters, magazine articles, theses.
- Eliminate duplicated papers.

2.3.3. Result

After removing duplicated and excluded papers because of irrelevance, the final studies comprised in this survey total of 56 articles. Figure 1 describes the preferred reporting items for systematic reviews and meta-analyses (PRISMA). The articles selection is demonstrated in the flow diagram, Figure 1.

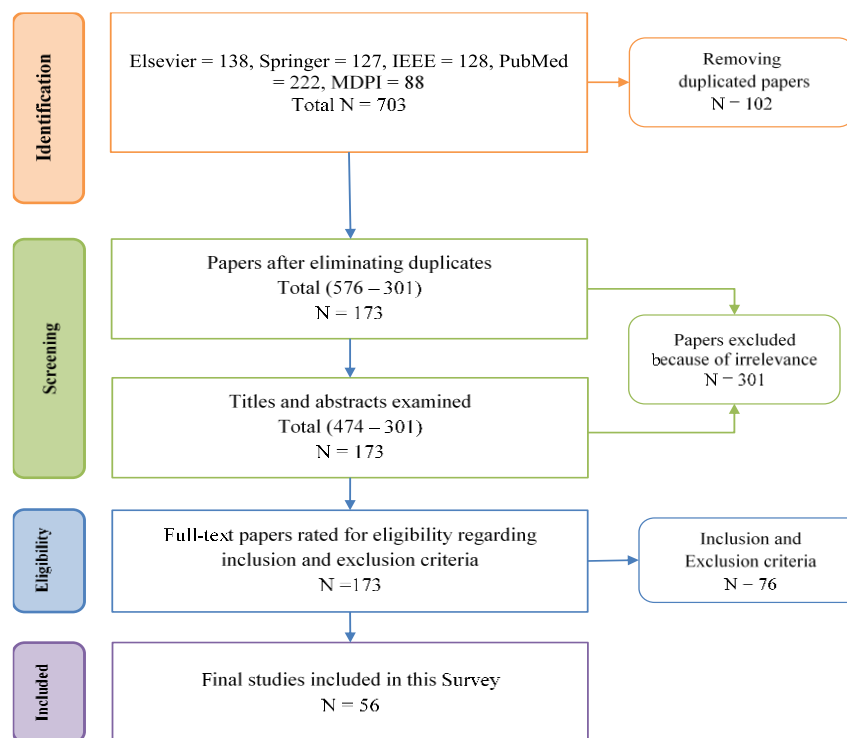


Figure 1. Survey search

3. BLOCKCHAIN TECHNOLOGY BACKGROUND

Several versions of blockchain have been released since the introduction of bitcoin a decade ago. The application of blockchain for digital assets was applied through financial transactions. Healthcare is one of the

industries that is getting the most attention and potential [19], [20]. In healthcare applications, the blockchain technology is redefining data management models and governance. This is primarily owing to its adaptability and capabilities to secure, segment, share medical data and services, in an original manner.

Blockchain technology is driving a number of existing developments in the healthcare sector [21]. Existing systems only share health resources within the medical and health care domain and are not entirely consistent with external systems. Nevertheless, the evidence reveals that there are many advantages to integrating these networks into higher quality, interconnected healthcare, including interconnection between different health informatics researchers and organizations [1]. The appropriate management and safe recovery of the massive amount of health data generated by the routine operations, making deals and delivering services, is a serious issue for the healthcare sector. The majority of health data is inaccessible, non-normalized throughout systems, and hard to interpret, manage, and share [22].

The healthcare industry faces a huge challenge in terms of data security. Most healthcare companies keep sensitive health data in a central location, which is vulnerable to malware and other cyberattacks due to an ageing legacy information technology (IT) architecture. Indeed, blockchain technology may be efficient in managing, processing personal health records, sharing, decreasing data security problems, and aiding the healthcare sector’s digital evolution [23]. Furthermore, the healthcare sector is now in the early phases of infrastructural development, computer programs, and strategic techniques that can safely, securely, and consistently bring together the many sets of data accessible to them [24].

This section shows the fundamental blockchain technology concepts to facilitate the understanding of remaining parts of this paper. Sharma *et al.* [7], a blockchain considers digital ledger types, which are copied simultaneously to different locations on a peer-to-peer network to securely store the data. Blockchains are a more specific form of distributed ledger technology (DLT) that outlines any database synchronously maintained in different locations [25]. Sharma *et al.* [7], the blockchain is an interconnected list of data blocks chained together within a distributed ledger by pointers, symbolized by a hash address that labels each block, and each data block has, in addition to its content, the pointer to the previous data block in the blockchain, as shown in Figure 2.

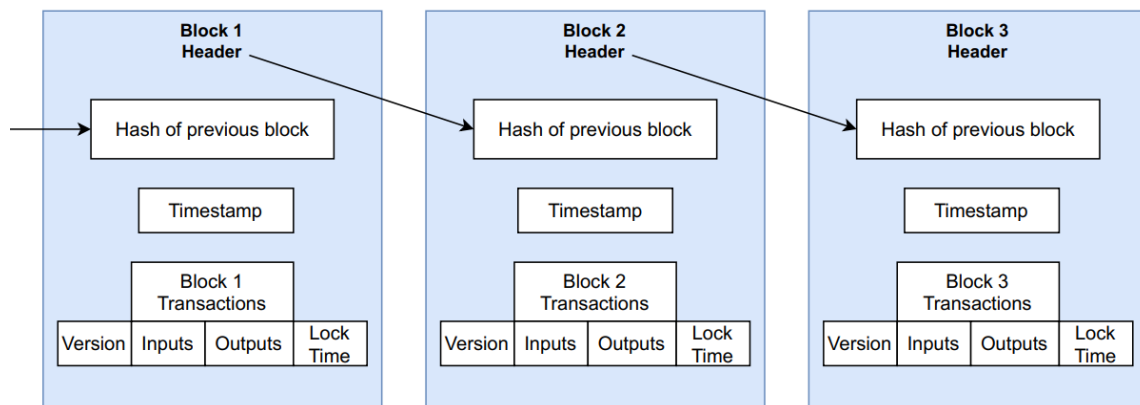


Figure 2. Representation of blocks in the blockchain

3.1. Blockchain benefits

In the health sector, as shown in Figure 3, blockchain technology has improved transparency, communication and more benefits among patients and healthcare professionals [26]. The healthcare area is concentrating its efforts on employing modern technology to improve the efficiency and effectiveness of healthcare systems [27]. In this section, we demonstrate the large blockchain benefits in the healthcare domain.

3.1.1. Decentralization

Henry *et al.* [28], a blockchain is a distributed system that takes the structure of a timestamped record ledger that is protected cryptographically against fraud and modification as opposed to traditional databases, which are controlled through a central entity. In the context of blockchain, decentralization describes the movement of decision-making and a centralized entity's control over a distributed network [29]. The main aspect of this technology is the decentralized storage system, which improves the security and data authentication kept in the system [30].

The previous block's cryptographic hash, a time stamping and the transaction data are also included in each block. To construct a network or chain, it also holds information of all preceding blocks and transactions. If the data in any of the blocks alters, it causes a chain reaction that may prompt the entire blockchain to freeze. Once the blockchain has handled the data, every computer on the network will lock at the identical instant, generating an immutable data record. Each blockchain system designates who has the authority of adding blocks to the network and how this is accomplished [31], [32]. It is impossible to change or alter data, and the modifications or updates are not permitted after putting the information in a specific block in the chain [33].

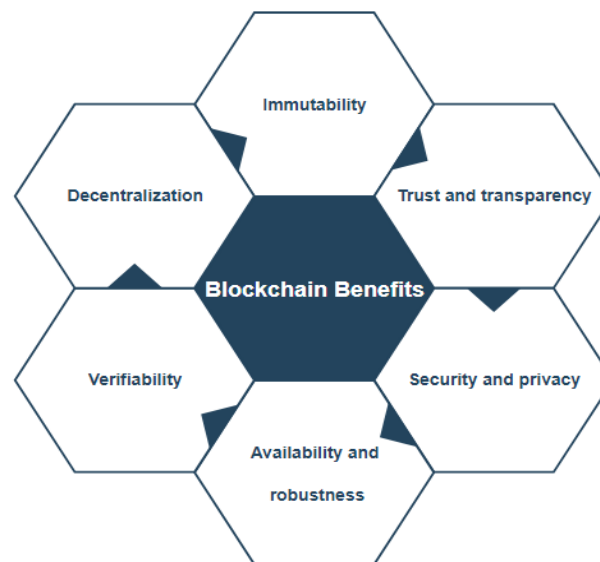


Figure 3. Blockchain benefits

3.1.2. Trust and transparency

The updated blockchain will be distributed to all participants after the new block was correctly inserted in the blockchain. If the data block is invalid, it is destroyed rather than being added to the blockchain. Consensus procedures are the validation mechanisms which participants utilize to verify the authenticity of a data block. Participants can rapidly achieve collective consent on the veracity of the data block by introducing consensus methods [34]. Potential users can see the recorded and stored data on the blockchain, and this can be quickly updated. The blockchain's transparency might prevent data from being tampered with or stolen [23].

3.1.3. Security and privacy

The term "Blockchain" refers to a technology that protects transaction information and data in a block from internal, peripheral, malicious, or unintentional threats. The security and information technology (IT) services, policies and tools are typically employed to detect and prevent risks, as well as provide a relevant response to the danger. Blockchain privacy can be defined as the ability of a stakeholder or a group to isolate oneself otherwise data and thereby be able to communicate in a discernible manner. It consist of the capacity to conduct transactions without revealing personal data. It also enables users to maintain compliance by careful self-divulgence [35], [36].

3.1.4. Availability and robustness

The blockchain technology is completely secure. It stores blocks of healthcare information that are similar across the network; it cannot be owned by a central authority, so it has no point of failure [37]. Utilizing the resources of all participating nodes and removing many-to-one traffic flows, the absence of centralized authority assures adaptability and robustness. Additionally, this technology gets rid of delays and solves the issue of a single failed phase [38].

3.1.5. Verifiability

The data are stored with integrity and accuracy on the blockchain and may be validated even without seeing the plaintext of such records. This capability comes in handy in the healthcare sector where records

must be verified, like managing the pharmaceutical supply chain and processing insurance claims [39]. All components of healthcare information are easily verifiable and accessible to everyone on the network, according to digital ledger technology, which allows different repetitions of sharing across all blockchain nodes. Blockchains provide data integrity and file synchronization by updating themselves automatically after a predetermined period [40].

3.2. Smart contract

Szabo [41], a smart contract is a self-checking, self-executing and tamper-proof computer program. Szabo [41] proposed the smart contract concept in 1994. It permits code execution without the intervention of external parties. The value, address, functions, and state of a smart contract are all included [42]. Smart contracts are extremely fundamental. The adoption of blockchain technology has emerged as a key direction of development as it allows peer-to-peer transactions to be conducted and a public database to be maintained in a secure and reliable manner. Smart contracts are irrevocable and trackable [43].

3.3. Consensus mechanism

Henry *et al.* [28], the mechanics of how such a system may operate rely on the overlay network structure imposed by the consensus protocol, that is, how participants select which transactions qualify for inclusion in the blockchain. In the network, every node manages its version of the blockchain, but in order for each node to obtain its copy, the distributed network must agree about the actual status of the blockchain. The algorithm that lays the foundation for security, accountability and trust is determined as a consensus protocol [44]. The description of the different consensus algorithms is outlined below:

Proof-of-work (PoW): the prover (requestor) and verifier are two separate parties (nodes) in a PoW system (provider). The prover completes a computational job that deploys many resources to reach an objective and then delivers it to a verifier or a group of verifiers for confirmation. The basic notion is that the imbalance in resource requirements among proof production and validation works as an inherent disincentive to any system misuse [45].

Proof-of-stake(PoS): is a consensus mechanism for selecting the validator that takes over the next block according to its economic participation in the network. The age of that stake, PoS comes in a variety of flavors, ranging from minor to major modifications to the basic protocol. The most obvious way in which they vary is in the method they use to avoid the protocol's double-spending and centralization [46].

Delegated proof-of-stake (DPoS): the most popular version of PoS is (DPoS), in which stakeholders choose validators instead of becoming validators themselves. Unlike PoS, which is based on the principle of direct democracy, DPoS is based on the principle of representative democracy [44].

Practical byzantine fault tolerant (PBFT): the traditional problem of byzantine generals in distributed computing is extended and solved by PBFT. It argues that when numerous anonymous players in a network achieve a consensus in sending their rulings to a trusted leader and unanimously agreeing on them, there may be enemies among those participants who transmit a false message. It has the ability to cause network damage and Byzantine failure [44], [47], [48].

3.4. Blockchain deployment models

The blockchain can be deployed in three main ways models; public, private and the consortium [44], [49]–[51]. **Public:** everyone with access to a public blockchain may read, contribute, and validate transactions. The transactions are visible to anyone on the network, but the identities of the participants are anonymous due to public-key cryptography: their public keys identify participants. Although a member's identity may not be linked with the blockchain, it is possible to compile a network of related transactions by connecting them to a well-known public key. Moreover, should an opponent be apt to attribute a member's real identity to their public key, the full history of their transactions can be widely viewed in the blockchain.

Private: a single organization manages private blockchains, which are not accessible to the public. Data is suitable for implementing data privacy regulations and other compliance requirements reasons since it is not available to the public. This method, however, is not a distributed, decentralized ledger and, like a centralized system, is vulnerable to insider threats and privacy violations. These systems identify participants, but transactions are encrypted and inaccessible apart from the organization.

Consortium: is managed by a group that regulates who can access, add and approve transactions on the blockchain. They are sometimes mislabeled as private blockchains because they may be locked down from the public. Consortium blockchains, which are more centralized than public blockchains, offer the benefits of private blockchains without putting total authority over the blockchain in the hands of a single person or other organization. Because the privileges of blockchain described above are paramount to biomedical and healthcare applications, the healthcare sector is now one of the key areas of emerging blockchain applications [52].

4. BLOCKCHAIN APPLICATIONS IN HEALTHCARE

4.1. Blockchain layer approach

The technology components that underlie the layers of blockchain are transactions, blockchain, consensus, applications, and smart contracts. These elements are categorized in various that are equivalent to the blockchain ecosystem. Blockchain technology in healthcare applications is conceptually organized into five layers, as illustrated in Figure 4, and Table 1 describes the blockchain layer approach.

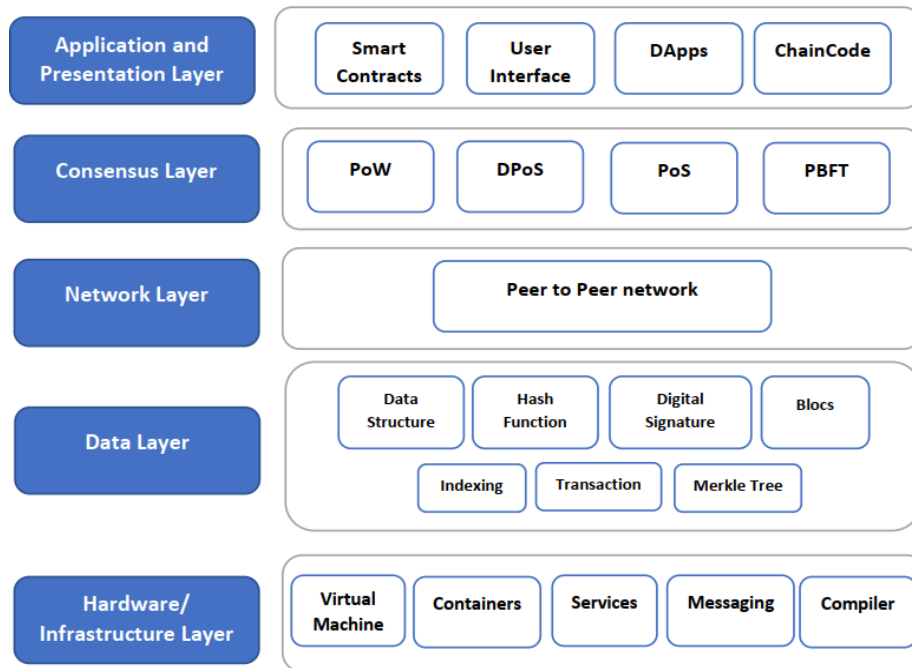


Figure 4. Blockchain layer approach

Table 1. Blockchain layer approach description

Layer	Description
Application and presentation	It focuses on developing Dapp blockchain solutions for usage through diverse applications and industries. It comprises smart contracts, user interface, ChainCode
Consensus	It is the set of algorithms which support a distributed or decentralized network to unitarily decide, when necessary, the protocol that considers the size of a publicly accessible ledger.
Network	The blockchain runs over a peer-to-peer network, where peers share information around the state of the network; it is responsible for the communication among the nodes.
Data	The data layer is the management of information stored both on the blockchain (on-chain) and within the database (off-chain) itself.
Hardware/ infrastructure	This layer includes the virtualization and virtual resource creation like storage, network and servers.

4.2. Data management

A recent work by Dubovitskaya *et al.* [53] has developed a system to enable the management, sharing and aggregation of EHR data in a secure and reliable manner. They have adopted a patient centric solution to managing their healthcare records across a number of hospitals; furthermore, the method ensures the patient's confidentiality and security concerning their health data management requirements, including the patient-specified access control strategy. They recommend a blockchain-based system with authorization for EHR data sharing and integration.

Azaria *et al.* [54] put forward a system MedRec for medical data access and permission management to solve the problematic data management, the permission management, digital rights management, data sharing, and data integrity. The authors applied 3 types of smart contracts, registrar contract (RC), patient-provider relationship contract (PPR), and summary contract (SC), to navigate the potentially considerable number of record representations

In another research published, Du *et al.* [55] mooted a medical information-sharing platform based on blockchain; they produced a process for anonymous information sharing, and a new two-layer consortium blockchain. This method improves the security and reliability of medical records sharing between users. Thus, the information as well as the transaction logs is stored in a distributed way to avoid any tampering or abuse. Pham *et al.* [56] demonstrates a remote healthcare system based on smart contract system; they posit a processing system for storing information from medical devices in an efficient and parsimonious manner according to the health situation of patients. Specifically, they screen the sensor data before making a decision on whether or not to write the data to the blockchain.

Khatoun [57] presents a smart contract system for managing medical data and streamlining complex medical operations; She develops a smart contract-based access system for permitting patient-provider interaction, and then the study employs Ethereum-based healthcare management tools. Sharma *et al.* [7] integrated smart contracts into the applications based on the internet of medical things (IoMT) in e-healthcare, and they propose an efficient approach by reducing the intermediates during the exchange of medical or patient records. Also, they interpret a scenario for IoMT related services.

Griggs *et al.* [58], posit exploiting blockchain-based smart contracts to simplify secure analysis and management of medical sensors; they mainly exploit the health insurance portability and accountability act (HIPAA) compliant manner. The suggested approach describes the system that would deploy a consortium-managed permission-based blockchain to run smart contracts that can measure the information captured by a patient's IoT health device against personalized triggers. They established a mechanism in which the sensors communicate with a smart device that calls the smart contracts and records all events on the blockchain. As for Wang *et al.* [59], developed a dynamic consent medical blockchain system, DynamiChain, based on a ruleset management algorithm. The solution is envisioned to provide a successful example for future blockchain-based medical systems to be extended to other disease areas or medical databases, then, a situation in which the healthcare company specializing in exercise management provides health management activities using data collected from the data provider's hospital.

4.3. Data sharing

Antwi *et al.* [60] specify a secure and privacy-preserving protected health information (PHI) sharing (BSPP) protocol based on the proposed e-health blockchain procedure of the recommended protocol, thus, they develop the basic components of blockchains, such as data architecture and the consensus mechanism. The authors use the scheme on juice to evaluate their results. Jiang *et al.* [61] introduce BloCHIE, a blockchain-based platform for healthcare information exchange. Their approach is about two fairness-based transaction packing algorithms: FAIR-FIRST and TP&FAIR; they apply BloCHIE in a minimal viable-product way, for their manipulation, to prove the practicability of BloCHIE.

Shen *et al.* [62] put forward a patient-driven healthcare data-sharing framework, named MedChain. They examined a MedChain data-sharing framework for flexible managing distinct types of information derived from healthcare data. Roehrs *et al.* [21] presented the prototype implementation and evaluation of OmniPHR architecture model, either the openEHR interoperability standard, then they evaluated the implementation of a model using the data set of over the 40 thousand patient adults anonymously identified by two hospital databases.

Liang *et al.* [63] proposed in this study a blockchain-based system, controlled by the mobile user, for personal health data sharing and collaboration. The authors' approach consists of a comprehensive user-centric case for personal healthcare data being shared. They apply an access control scheme using the Hyperledger Fabric membership service and channel pattern component. The framework implements a user-centric model for personal health data treatment using blockchain networks, guaranteeing the data ownership of individuals, and data integrity. Radhakrishnan *et al.* [64] a blockchain-based information management system, MedBlock, a secure blockchain-based system. The objective is sharing the electronic health information records across authorized users; it consists of six modules, clients, endorsers, schedulers, committers, databases and ledgers. They implement a strategy of access control and encryption that is straightforward and effective to assure the security and confidentiality of information with more minor time and cost energy. Furthermore, this paper proves that the collaboration of data sharing via blockchain can help hospitals understand the medical history of patients before consultation. They apply an efficient blockchain-based sharing and privacy preservation scheme that can secure the privacy of users' data by combining an access control protocol and encryption technology.

4.4. Data security and privacy

Giordanengo [20] implemented a blockchain-based SHS framework to provide a secure and privacy-preserved healthcare system. This paper approves that a secured and smart healthcare system (S2HS) works by deploying blockchain technology in the SHSs to overcome the issues and challenges faced by the classical SHS; further they proposed the architecture of this system. Saini *et al.* [19] propose and develop an access

control model for internet of things (IoT) enabled smart healthcare devices and the medical system through blockchain-based smart contract, they implemented a scheme on a private Ethereum blockchain. This study exploits a methodology that covers the entire medical system scenario; furthermore, the authors moot a distributed and proactive smart contract-based access control system, a use case is demonstrated as the chosen distributed and patient-centric smart contract-based access control framework.

Ali *et al.* [65] explained about a blockchain-based remote health monitoring (RHM); this study manipulates Tor hidden data off-chain delivery services, in which they aim to share sensitive patient data with physicians securely, with the data not passing through third-party services. The article presents a security analysis conducted on the solution, based on multiple attack scenarios. Tripathia *et al.* [66] concerns a proposed new decentralized access control system built on the Tangle, allowing users to control access to their assets; this work is verified by application and is tested with AVISPA tools, which confirm security in the presence of the intruder.

Cheng *et al.* [67] combined the cloud storage together with cryptography for analyzing the blockchain security authentication feasibility in medical cyber physical systems (MCPS), realized the sharing of medical data and employed a BAN logic protocol. The authors suggested a secure storage model for the medical data. Using the network entity model, a security authentication scheme is established, and a blockchain-based network model of MCPS is demonstrated. Dwivedi *et al.* [24], suggest a framework of modified blockchain models adapted for IoT devices that leverage their distributed nature and the added privacy and security properties of the network. The authors developed a patient-centric access control for electronic medical records that is secure and private by combining the advantages of private key, public key, blockchain and many other cryptographic light-weight primitives. Additionally, while taking into account the resource limitations of IoT, this article builds the architecture and offers a solution to the majority of security and privacy risks. Radhakrishnan *et al.* [64] proposed a multilevel authentication-based scheme to preserve the Blockchain from attacks. Based on functionality, they connect the associated healthcare providers to store and share the EHR using the blockchain. This system is categorized into four layers: user management layer, EHR generation, view layer, EHR storage layer, and EHR access management layer.

5. BLOCKCHAIN IMPLEMENTATIONS IN HEALTHCARE

5.1. Clinical trials

According to Nugent *et al.* [68], researchers, clinicians, and patients are regularly denied access to data from clinical trials, resulting in a lack of faith in the process and underlining the need for structural transformation. The authors have shown that a smart contract based on the Ethereum blockchain may be used to increase the transparency of clinical trial data management. This study has proven that the cryptographic assurances provided by current protocols should go beyond “proof-of-existence” and be used for complicated clinical trial data management that is immune to tampering according to blockchains' tamper-resistant properties. Benchoufi and Ravaud [69] improve that the blockchain technology offers a high potential for clinical research; it facilitates the structuring on methodologies in a more transparent and verifiable way and, once a set of crucial metadata is established, it can contribute to the more transparent and mainly algorithmic proof of the integrity of clinical trials. Choudhury *et al.* [70] proposed a modern data management system based on permissioned blockchain technology to decrease the administrative cost, time, and effort of maintaining data integrity and privacy in framework studies. They show how our architecture, which makes use of smart contracts and private channels, allows for secure data transfer, protocol implementation, and an audit trail.

5.2. Pharmaceutical industry

Zakari *et al.* [71] demonstrated a blockchain-based approach to improve pharmaceutical supply chain security. They implemented a prototype called LifeCrypter. The aim was to measure the blockchain technology value, and how this prototype may protect patients' lives by deploying a patient-empowering blockchain solution. For all participants, the smart contract allows for free and trustless trading, with the potential to set rules for deals that are transparent and self-enforcing at all stages. In this study, Sylim *et al.* [72] announce that the drug expenses costs of the people and to governments is significant. The Philippine Food and Drug Administration (FDA) invites the public to verify drug approval certificates and report any counterfeiting incidents. A specific task unit of the Philippine National Police responds to such reports. Blockchain technology is a digital ledger that is said to be immutable and fault-tolerant due to periodic sequential hashing and a consensus process. They create a pharmaco-surveillance blockchain system and test it in a simulated network. Tseng *et al.* [73] recommend using the Gcoin blockchain as the foundation for creating transparent drug transaction data. Furthermore, the medication supply chain regulatory model may be changed from inspection and examination alone to monitoring net, with every component participating in the drug supply chain being capable of participating concurrently in preventing counterfeit pharmaceuticals and protecting

public health, including patients. The Gcoin blockchain is proposed as a framework for the drug data flow to provide transparent medication transaction data.

Gatteschi *et al.* [74], the insurance companies, like many other sectors, have already initiated the study and the integration of blockchain technology with important investments by large and small companies. In this work, Chen *et al.* [75], the traditional insurance plans are frequently conducted on paper contracts, which makes privileges and payments susceptible to mistake and regularly need human oversight; the fundamental complexity of traditional insurance includes consumers, agents, insurers, and reinsurers, and further insurance's primary product-risk. The blockchain, as a distributed ledger, increases insurance sector performance in four ways: fraud prevention, claims processing, data analysis using the IoT, and reinsurance. Heston approves the potential of the Estonian medical record blockchain project to ensure medical records privacy although making them publicly available to medical providers and insurance companies determines their success.

5.3. Medical IoT devices

Dilawar *et al.* [76] define the internet of medical things (IoMT) as a group of connected devices that supply health-related services on the internet. Khezr *et al.* [5], the healthcare equipment such as heart monitors, body scanners, and wearable devices can use IoMT technology to collect, analyze, and transmit data in real time via the Internet. Dorri *et al.* [77] suggest a blockchain framework for improving communication and data exchange security in an IoT environment. Their framework is especially aimed towards smart home applications. As for Dilawar *et al.* [76], the goal of their research was to evolve and validate a tamper-resistant mHealth system based on blockchain technology, which allows for trustworthy and robust computing over a decentralized network. They created a smartphone app-based mHealth system for the cognitive behavioral treatment of insomnia. Rahman *et al.* [78] provide a new technique, strategy, and system for measuring dyslexia symptoms and generating metric data for a single user, a community, or a group generally. Jo *et al.* [79] integrate in this research IoT with blockchain-based smart contracts for structural health monitoring (SHM) to create a modern, efficient, robust, and secure distributed network for increasing operational safety subterranean infrastructure.

According to these works, there are three significant issues in the healthcare field: data management, the different responsibilities that exist among users of health data, and rights assigned to these roles to control access to the information. Thus, the problematic of data sharing, sharing healthcare and medical data, was among the most important and necessary steps toward improving healthcare provider quality and performance of the system. Participants will share their medical records with other healthcare institutions for better patient care. Also, both accidentally and by malicious users, data security and privacy are often compromised. Consequently, several institutions have suffered a significant reputation and money losses.

6. DISCUSSION

This survey analysis highlights research trends by presenting the most relevant studies on innovative healthcare applications that employ blockchain technology. Many of the systems studied provide insufficient implementation information, such as the type of blockchain applied, the consensus process utilized, and the deployment of smart contracts, yet only a minority has developed, tested, or deployed their systems. Furthermore, none of the published available systems discusses the problem concerning blockchain governance. All the systems that specified the type of blockchain were hybrid, public, or they implemented their own platform, indicating that an entity or group governs the blockchain. This process requires prescribing read and written regulations, as well as approving mining nodes and users.

According to the first research problematic, data management, Kuo *et al.* [52] mention the lack of interoperability between healthcare systems due to a multitude of EHR systems with different interfaces. Azaria *et al.* [54] offer simple access, an immutable log, and a wide range of services. It also eliminates the possibility of a single point of failure, while the smart contract, encryption, auditability, obscurity, and scalability are not regarded; for complicated scenarios, including healthcare data, the architecture must be improved. Roehrs *et al.* [21] one important constraint is that the data had to correspond to the model's requirements, and data that could not meet the requirements would not be provided. Patients and healthcare professionals are responsible for checking and inputting various data, such as the patient's demographics and the healthcare provider's diagnosis.

Concerning data sharing, Radhakrishnan *et al.* [64] presented MedBlock which enables quick access and sharing, reduces the traffic load, and ensures excellent data security; it lowers the idea of decentralization because the data are kept in local databases. Jiang *et al.* [61], the off-chain storage and on-chain verification is both guaranteed and proven to be practical and effective. Rahman *et al.* [78] on the access control, data auditing, privacy protection, private searching, and time-controlled revocation are all features of the system. However, there are a few difficulties with changing the uniform resource locator (URL). Because blockchain only store

records, the location of data may change; as a result, the previous URL cannot be altered and a new URL must be created.

Additionally, data security and privacy are addressed by Saini *et al.* [19], which shows that the combination of blockchain with clouds to offer decentralized access control faces scalability and performance problems, despite the proposed scheme's appealing characteristics. The latency that emerges during EMR processing and retrieval may be greatly decreased by employing edge computing. As a result, more research is required to solve this problem. Moreover, the authors did not demonstrate the consensus algorithm process. Dwivedi *et al.* [24], to handle user wallet assaults, the proposed blockchain-based healthcare system employs a multilayer authentication mechanism that adds another layer of protection. The blockchain-based healthcare system necessitates a large amount of storage, which is still a tough challenge; further, in this work, they did not point out the consensus algorithm as well as the smart contract.

The lack of stakeholder information is one of the serious obstacles to blockchain adoption, which will need to be given more attention. blockchain has witnessed remarkable growth across all industries since its introduction in 2008. The use of blockchain in healthcare is still in its early phases of research, but it has the potential to completely change the sector. Healthcare executives, governments, technology developers, and other stakeholders must work together to address the multiple issues that have long existed and to solve the numerous problems that the healthcare sector has been dealing with for decades.

7. CONCLUSION

In recent years, blockchain applications have been in wide demand, and several issues must be overcome. Therefore, the blockchain technology is set to evolve to become more scalable, efficient and sustainable. Considered independently, the features they provide are not new, and most of the systems they are based on have been well known for years. The combination of these properties, however, makes an outstanding choice for a wide range of purposes, which accounts for the critical interest level from various sectors. The study's objective was to determine the state of blockchain research and application in the healthcare sector. To achieve this goal, we have defined the research questions, and by applying the predefined method, we have narrowed the reviewed literature to 56 papers. We examined five pertinent databases for articles released between 2016 and 2022. These were then given further analysis. This paper identifies the key application areas in healthcare where blockchain technology can have a serious impact. In addition, this article examines the various blockchain-based healthcare requirements and solutions. According to the referenced articles, we determine the three severe issues in the healthcare industry, in interaction with patients, doctors, hospitals, and stakeholders, which implies the integration of blockchain technology to solve them.




REFERENCES

- [1] A. H. Mayer, C. A. da Costa, and R. da R. Righi, "Electronic health records in a blockchain: a systematic review," *Health Informatics Journal*, vol. 26, no. 2, pp. 1273–1288, Jun. 2020, doi: 10.1177/1460458219866350.
- [2] S. Yaqoob *et al.*, "Use of blockchain in healthcare: a systematic literature review," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, 2019, doi: 10.14569/IJACSA.2019.0100581.
- [3] R. Sarkis-Onofre, F. Catalá-López, E. Aromataris, and C. Lockwood, "How to properly use the PRISMA statement," *Systematic Reviews*, vol. 10, no. 1, Dec. 2021, doi: 10.1186/s13643-021-01671-z.
- [4] H. D. Zubaydi, Y.-W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, "A review on the role of blockchain technology in the healthcare domain," *Electronics*, vol. 8, no. 6, Jun. 2019, doi: 10.3390/electronics8060679.
- [5] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: a comprehensive review and directions for future research," *Applied Sciences*, vol. 9, no. 9, Apr. 2019, doi: 10.3390/app9091736.
- [6] A. Gaggioli, "Blockchain technology: living in a decentralized everything," *Cyberpsychology, Behavior, and Social Networking*, vol. 21, no. 1, pp. 65–66, Jan. 2018, doi: 10.1089/cyber.2017.29097.csi.
- [7] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B.-G. Kim, "Blockchain based smart contracts for internet of medical things in e-healthcare," *Electronics*, vol. 9, no. 10, Oct. 2020, doi: 10.3390/electronics9101609.
- [8] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.
- [9] M. Kaur, M. Murtaza, and M. Habbal, "Post study of blockchain in smart health environment," in *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*, Nov. 2020, pp. 1–4, doi: 10.1109/CITISIA50690.2020.9371819.
- [10] H. Cao and H. Cao, "Solutions to the endless addition of transaction volume in blockchain," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 6, 2022, doi: 10.14569/IJACSA.2022.0130601.
- [11] O. Daanouni, B. Cherradi, and A. Tmiri, "Predicting diabetes diseases using mixed data and supervised machine learning algorithms," in *Proceedings of the 4th International Conference on Smart City Applications*, Oct. 2019, pp. 1–6, doi: 10.1145/3368756.3369072.
- [12] O. Terrada, A. Raihani, O. Bouattane, and B. Cherradi, "Fuzzy cardiovascular diagnosis system using clinical data," in *2018 4th International Conference on Optimization and Applications (ICOA)*, Apr. 2018, pp. 1–4, doi: 10.1109/ICOA.2018.8370549.




- [13] S. Laghmati, B. Cherradi, A. Tmiri, O. Daanouni, and S. Hamida, "Classification of patients with breast cancer using neighbourhood component analysis and supervised machine learning techniques," in *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*, Sep. 2020, pp. 1–6, doi: 10.1109/CommNet49926.2020.9199633.
- [14] O. Terrada, B. Cherradi, A. Raihani, and O. Bouattane, "Atherosclerosis disease prediction using supervised machine learning techniques," in *2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, Apr. 2020, pp. 1–5, doi: 10.1109/IRASET48871.2020.9092082.
- [15] B. Cherradi, O. Terrada, A. Ouhmida, S. Hamida, A. Raihani, and O. Bouattane, "Computer-aided diagnosis system for early prediction of atherosclerosis using machine learning and k-fold cross-validation," in *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, Jul. 2021, pp. 1–9, doi: 10.1109/ICOTEN52080.2021.9493524.
- [16] V. Welch *et al.*, "Extending the PRISMA statement to equity-focused systematic reviews (PRISMA-E 2012): explanation and elaboration," *Journal of Clinical Epidemiology*, vol. 70, pp. 68–89, Feb. 2016, doi: 10.1016/j.jclinepi.2015.09.001.
- [17] R. B. Briner and D. Denyer, "Systematic review and evidence synthesis as a practice and scholarship tool," in *The Oxford Handbook of Evidence-Based Management*, Oxford University Press, 2012, pp. 112–129.
- [18] D. Moher, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *Annals of Internal Medicine*, vol. 151, no. 4, p. 264, Aug. 2009, doi: 10.7326/0003-4819-151-4-200908180-00135.
- [19] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5914–5925, Apr. 2021, doi: 10.1109/IJOT.2020.3032997.
- [20] A. Giordanengo, "Possible usages of smart contracts (blockchain) in healthcare and why no one is using them," *Studies in Health Technology and Informatics*, vol. 264, pp. 596–600, 2019, doi: 10.3233/SHTI190292.
- [21] A. Roehrs, C. A. da Costa, R. da R. Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *Journal of Biomedical Informatics*, vol. 92, p. 103140, Apr. 2019, doi: 10.1016/j.jbi.2019.103140.
- [22] A. Tandon, A. Dhir, A. K. M. N. Islam, and M. Mäntymäki, "Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda," *Computers in Industry*, vol. 122, Nov. 2020, doi: 10.1016/j.compind.2020.103290.
- [23] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: challenges and future perspectives," *Cryptography*, vol. 3, no. 1, Jan. 2019, doi: 10.3390/cryptography3010003.
- [24] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, Jan. 2019, doi: 10.3390/s19020326.
- [25] B. Sun, Q. Dang, Y. Qiu, L. Yan, C. Du, and X. Liu, "Blockchain privacy data access control method based on cloud platform data," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 6, 2022, doi: 10.14569/IJACSA.2022.0130602.
- [26] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, Feb. 2020, doi: 10.1016/j.jisa.2019.102407.
- [27] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: a secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, Dec. 2021, doi: 10.1016/j.comnet.2021.108500.
- [28] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: challenges and directions," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 38–45, Jul. 2018, doi: 10.1109/MSP.2018.3111245.
- [29] Y. Zhu, C. Lv, Z. Zeng, J. Wang, and B. Pei, "Blockchain-based decentralized storage scheme," *Journal of Physics: Conference Series*, vol. 1237, no. 4, Jun. 2019, doi: 10.1088/1742-6596/1237/4/042008.
- [30] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, Jun. 2019, doi: 10.1016/j.jnca.2019.02.027.
- [31] D. L. K. Chuen, Ed., *Handbook of digital currency*. Elsevier, 2015.
- [32] M. Attaran, "Blockchain technology in healthcare: challenges and opportunities," *International Journal of Healthcare Management*, vol. 15, no. 1, pp. 70–83, Jan. 2022, doi: 10.1080/20479700.2020.1843887.
- [33] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," *Journal of Medical Systems*, vol. 43, no. 10, Oct. 2019, doi: 10.1007/s10916-019-1445-8.
- [34] A. Adeyemi *et al.*, "Blockchain technology applications in power distribution systems," *The Electricity Journal*, vol. 33, no. 8, Oct. 2020, doi: 10.1016/j.tej.2020.106817.
- [35] T. T. Huynh, T. D. Nguyen, and H. Tan, "A survey on security and privacy issues of blockchain technology," in *2019 International Conference on System Science and Engineering (ICSSE)*, Jul. 2019, pp. 362–367, doi: 10.1109/ICSSE.2019.8823094.
- [36] R. Mohammed, R. Alubady, and A. Sherbaz, "Blockchain-base healthcare applications a survey," in *The Sixth International Conference on Internet Applications, Protocols and Services (NETAPPS2020)*, 2021, pp. 130–136.
- [37] S. Singh, A. Sharma, and P. Jain, "A detailed study of blockchain: changing the world," *International Journal of Applied Engineering Research*, vol. 13, no. 14, pp. 11532–11539, 2018.
- [38] M. R. Bataineh, W. Mardini, Y. M. Khamaysheh, and M. M. B. Yassein, "Novel and secure blockchain framework for health applications in IoT," *IEEE Access*, vol. 10, pp. 14914–14926, 2022, doi: 10.1109/ACCESS.2022.3147795.
- [39] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: a systematic review," *Healthcare*, vol. 7, no. 2, Apr. 2019, doi: 10.3390/healthcare7020056.
- [40] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing and Applications*, vol. 34, no. 14, pp. 11475–11490, Jul. 2022, doi: 10.1007/s00521-020-05519-w.
- [41] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, Sep. 1997, doi: 10.5210/fm.v2i9.548.
- [42] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 09, no. 10, pp. 533–546, 2016, doi: 10.4236/jsea.2016.910036.
- [43] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2018, pp. 1–4, doi: 10.1109/ICCCNT.2018.8494045.
- [44] A. Wahab and W. Mehmood, "Survey of consensus protocols," *arXiv:1810.0335*, Oct. 2018.
- [45] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: a survey," *arXiv:2001.07091*, Jan. 2020, [Online]. Available: <http://arxiv.org/abs/2001.07091>.
- [46] S. King and S. Nadal, "PPCoin: peer-to-peer crypto-currency with proof-of-stake," *Self-published paper*, vol. 19, no. 1, Aug. 2012.
- [47] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, Jul. 1982, doi: 10.1145/357172.357176.

- [48] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proceedings of the Symposium on Operating System Design and Implementation*, 1999, no. February, pp. 1–14, doi: 10.1145/571637.571640.
- [49] T. Hardin and D. Kotz, "Blockchain in health data systems: a survey," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, Oct. 2019, pp. 490–497, doi: 10.1109/IOTSMS48152.2019.8939174.
- [50] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," arXiv:1707.01873, Jul. 2017, [Online]. Available: <http://arxiv.org/abs/1707.01873>.
- [51] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Jan. 2017, pp. 1–5, doi: 10.1109/ICACCS.2017.8014672.
- [52] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017, doi: 10.1093/jamia/ocx068.
- [53] A. Dubovitskaya *et al.*, "ACTION-EHR: patient-centric blockchain-based electronic health record data management for cancer care," *Journal of Medical Internet Research*, vol. 22, no. 8, p. e13598, Aug. 2020, doi: 10.2196/13598.
- [54] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.
- [55] M. Du, Q. Chen, J. Chen, and X. Ma, "An optimized consortium blockchain for medical information sharing," *IEEE Transactions on Engineering Management*, vol. 68, no. 6, pp. 1677–1689, Dec. 2021, doi: 10.1109/TEM.2020.2966832.
- [56] H. L. Pham, T. H. Tran, and Y. Nakashima, "A secure remote healthcare system for hospital using blockchain smart contract," in *2018 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6, doi: 10.1109/GLOCOMW.2018.8644164.
- [57] A. Khatoun, "A blockchain-based smart contract system for healthcare management," *Electronics*, vol. 9, no. 1, p. 94, Jan. 2020, doi: 10.3390/electronics9010094.
- [58] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, p. 130, Jul. 2018, doi: 10.1007/s10916-018-0982-x.
- [59] S. Wang *et al.*, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 942–950, Dec. 2018, doi: 10.1109/TCSS.2018.2865526.
- [60] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. Habib ur Rehman, and C. A. Kerrache, "The case of HyperLedger fabric as a blockchain solution for healthcare applications," *Blockchain: Research and Applications*, vol. 2, no. 1, Mar. 2021, doi: 10.1016/j.bcr.2021.100012.
- [61] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BlocHIE: a blockchain-based platform for healthcare information exchange," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, Jun. 2018, pp. 49–56, doi: 10.1109/SMARTCOMP.2018.00073.
- [62] B. Shen, J. Guo, and Y. Yang, "MedChain: efficient healthcare data sharing via blockchain," *Applied Sciences*, vol. 9, no. 6, Mar. 2019, doi: 10.3390/app9061207.
- [63] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct. 2017, pp. 1–5, doi: 10.1109/PIMRC.2017.8292361.
- [64] B. L. Radhakrishnan, A. S. Joseph, and S. Sudhakar, "Securing blockchain based electronic health record using multilevel authentication," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Mar. 2019, pp. 699–703, doi: 10.1109/ICACCS.2019.8728483.
- [65] M. S. Ali, M. Vecchio, G. D. Putra, S. S. Kanhere, and F. Antonelli, "A decentralized peer-to-peer remote health monitoring system," *Sensors*, vol. 20, no. 6, Mar. 2020, doi: 10.3390/s20061656.
- [66] G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS- A blockchain based approach for smart healthcare system," *Healthcare*, vol. 8, no. 1, Mar. 2020, doi: 10.1016/j.hjdsi.2019.100391.
- [67] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *Journal of Medical Systems*, vol. 44, no. 2, Feb. 2020, doi: 10.1007/s10916-019-1468-1.
- [68] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *F1000Research*, vol. 5, Oct. 2016, doi: 10.12688/f1000research.9756.1.
- [69] M. Benchoufi and P. Ravaut, "Blockchain technology for improving clinical research quality," *Trials*, vol. 18, no. 1, Dec. 2017, doi: 10.1186/s13063-017-2035-z.
- [70] O. Choudhury, N. Fairiza, I. Sylla, and A. Das, "A blockchain framework for managing and monitoring data in multi-site clinical trials," arXiv:1902.03975, Feb. 2019, [Online]. Available: <http://arxiv.org/abs/1902.03975>.
- [71] N. Zakari *et al.*, "Blockchain technology in the pharmaceutical industry: a systematic review," *PeerJ Computer Science*, vol. 8, Mar. 2022, doi: 10.7717/peerj-cs.840.
- [72] P. Syllim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention," *JMIR Research Protocols*, vol. 7, no. 9, Sep. 2018, doi: 10.2196/10163.
- [73] J.-H. Tseng, Y.-C. Liao, B. Chong, and S. Liao, "Governance on the drug supply chain via gcoin blockchain," *International Journal of Environmental Research and Public Health*, vol. 15, no. 6, May 2018, doi: 10.3390/ijerph15061055.
- [74] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: is the technology mature enough?," *Future Internet*, vol. 10, no. 2, Feb. 2018, doi: 10.3390/fi10020020.
- [75] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, "A survey of blockchain applications in different domains," in *Proceedings of the 2018 International Conference on Blockchain Technology and Application*, Dec. 2018, pp. 17–21, doi: 10.1145/3301403.3301407.
- [76] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, "Blockchain: securing internet of medical things (IoMT)," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, 2019, doi: 10.14569/IJACSA.2019.0100110.
- [77] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623, doi: 10.1109/PERCOMW.2017.7917634.
- [78] M. A. Rahman, E. Hassanain, M. M. Rashid, S. J. Barnes, and M. S. Hossain, "Spatial blockchain-based secure mass screening framework for children with dyslexia," *IEEE Access*, vol. 6, pp. 61876–61885, 2018, doi: 10.1109/ACCESS.2018.2875242.
- [79] B. Jo, R. Khan, and Y.-S. Lee, "blockchain and internet-of-things network for underground structure health monitoring," *Sensors*, vol. 18, no. 12, Dec. 2018, doi: 10.3390/s18124268.




BIOGRAPHIES OF AUTHORS

Sara Ait Bennacer    is a Ph.D. candidate in the Computer Science Department of the University of Chouaib Doukkali, Faculty of sciences El Jadida in Morocco. She received a Master's degree in Internet of things and mobile systems from the National School of Applied Sciences in Fez, Morocco, in 2019. Her research interests include the integration of the blockchain technology in the healthcare systems, data privacy and security. She can be contacted at e-mail: aitbennacer.sara@gmail.com.






Khadija Sabiri    received her Ph.D. degree in the cloudification legacy system to a cloud-native application from the Science Faculty of Ben M'sik in Casablanca-Morocco, then she moved to the University of Beira Interior in Portugal as Postdoc researcher as part of cloud computing competence center-C4 projects. Her overarching research is to explore rigorous software development methodologies and cloud-based technology solutions that increase and guarantee citizen rights, such as privacy, transparency. Furthermore, fundamental research is expected to be conducted on the use of Blockchains for better accountability of the public information system and decision support systems in use in local administration. She can be contacted at e-mail: khadija.sabiry@gmail.com.






Abdessadek Aaroud    is a Professor at the Faculty of sciences El Jadida in Morocco, and member of LAROSERI Laboratory, and head of the computer sciences department. His research interests are the specification and verification of real-time systems, the use of a reactive agent approach for modeling, and real-time temporal logic as a formal method. He can be contacted at e-mail: aaroud.a@ucd.ac.ma.



Khalid Akodadi    is a Ph.D. candidate in the Computer Science Department of the University of Chouaib Doukkali, Faculty of sciences El Jadida in Morocco. His research interests include semantic middleware, systems analysis and control, artificial intelligence, and neural networks. He currently works as a Technical Manager in 2M TV Channel. He can be contacted at e-mail: khalidakodadi@gmail.com.



Bouchaib Cherradi    is a Professor of computer science in CRMEF-El Jadida. He is associate member of Signals, Distributed Systems and Artificial Intelligence (SSDIA) Laboratory in ENSET Mohammedia, Hassan II University Casablanca (UH2C), and LaROSERI Laboratory on leave from the Faculty of Science El Jadida (Chouaib Doukali University), Morocco. His research interests include massively parallel architectures, cluster analysis, pattern recognition, image processing and fuzzy logic systems. He can be contacted at e-mail: bouchaib.cherradi@gmail.com.