CEFET/RJ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO

A SYSTEMATIC REVIEW ON THE BLOCKCHAIN-ENABLED CLOUD OF SENSORS IN HEALTHCARE

André Ricardo Cavalcanti de Araújo

Dissertação de Mestrado apresentada ao Programa/Curso de Pós-Graduação Stricto Sensu em Engenharia de Produção e Sistemas do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ, como parte dos requisitos necessários à obtenção do título de Mestre.

Orientador: D.Sc. Igor Leão dos Santos

Rio de Janeiro
Setembro de 2022

A SYSTEMATIC REVIEW ON THE BLOCKCHAIN-ENABLED CLOUD OF SENSORS IN HEALTHCARE

Dissertação de Mestrado apresentada ao Programa/Curso de Pós-Graduação Stricto Sensu em Engenharia de Produção e Sistemas do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ, como parte dos requisitos necessários à obtenção do título de Mestre

André Ricardo Cavalcanti de Araújo

Banca Examinadora:

_____

Presidente, Professor Dr. Igor Leão dos Santos (Orientador – CEFET/RJ)

_____

Professor Professor Dr. Augusto da Cunha Reis (CEFET/RJ)

_____

Professor Dr. Pedro Senna Vieira (CEFET/RJ)

_____

Professor Dr. Claudio Miceli de Farias (UFRJ/RJ)

Rio de Janeiro
Setembro de 2022

Ficha catalográfica elaborada pela Biblioteca Central do CEFET/RJ

A663 Araújo, André Ricardo Cavalcanti de
A systematic review on the blockchain-enabled cloud of sensors in healthcare / André Ricardo Cavalcanti de Araújo. — 2022.
85f. : il. color. , enc.

Dissertação (Mestrado) Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, 2022.
Bibliografia : f. 70-85
Orientador: Igor Leão dos Santos

1. Sistemas de informação. 2. Blockchain (Base de dados). 3. Assistência médica. 4. Computação em nuvem. 5. Segurança de dados – Computação. I. Santos, Igor Leão dos (Orient.). II. Título.

CDD 658.4038

Elaborada pela bibliotecária Tania Mello – CRB/7 nº 5507/04

RESUMO

Resumo: Nos últimos anos, devido à popularidade das criptomoedas, a tecnologia blockchain tornou-se muito na moda e penetrou em diferentes domínios. Como as criptomoedas introduziram recentemente a tecnologia blockchain, as características dos aplicativos existem para estender essa tecnologia a um caso de uso não financeiro. Um campo de pesquisa em que o blockchain tem um tremendo potencial de impacto é a saúde, devido à necessidade de uma abordagem mais centrada no paciente para os sistemas de saúde. Além disso, combinado com outras tecnologias emergentes, como Internet das Coisas (IoT) ou Cloud of Sensor (CoS), onde as ameaças de segurança relacionadas incluem integridade de dados, atualização de dados, disponibilidade da rede, autenticação de dados, gerenciamento seguro, confiabilidade, segurança localização, responsabilidade e flexibilidade, é possível usar blockchain para conectar sistemas diferentes e aumentar a precisão de registros eletrônicos de saúde (EHRs), registros médicos eletrônicos (EMR) e registros pessoais de saúde (PHR). A tecnologia blockchain permite um ambiente descentralizado e distribuído sem a necessidade de uma autoridade central ou terceiro confiável (TTP). No blockchain, as transações são simultaneamente seguras e confiáveis devido ao uso de princípios criptográficos. Esta revisão sistemática da pesquisa em andamento nas aplicações da tecnologia blockchain na saúde visa revelar o uso potencial da tecnologia blockchain, combinada com nuvens de sensores, e destacar os desafios e possíveis direções de pesquisa. A metodologia desta pesquisa compreende os itens de relatório preferidos para as diretrizes de revisões sistemáticas e meta-análises (PRISMA). De acordo com a definição de palavras-chave relevantes e a execução de um protocolo de pesquisa bem projetado, foram identificadas publicações relevantes ao tema, usando as bases de dados científicas Scopus e Web of Science. Após análise bibliométrica dos artigos foi possível identificar a relevância do tema e as possíveis aplicações no setor de healthcare

Palavras - Chave: Blockchain; Healthcare; Cloud of Sensors, Edge Computing, Electronic Medical Records.

ABSTRACT

Abstract: In recent years, due to the popularity of cryptocurrencies, blockchain technology has become very trendy and penetrated different domains. Since cryptocurrencies recently introduced blockchain technology, the characteristics of applications exist to extend this technology to a non-financial use case. One field of research where blockchain has tremendous potential of impact is healthcare, due to the need for a more patient-centric approach to healthcare systems. In addition, combined with other emerging technologies, such as Internet of Things (IoT) or Cloud of Sensor (CoS), where related security threats include data integrity, data freshness, availability of the network, data authentication, secure management, dependability, secure localization, accountability, and flexibility, it is possible to use blockchain to connect disparate systems and increase the accuracy of electronic healthcare records (EHRs), electronic medical records (EMR) and personal health records (PHR). The blockchain technology enables a decentralized and distributed environment with no need for a central authority or trusted third party (TTP). In blockchain, transactions are simultaneously secure and trustworthy due to the use of cryptographic principles. This systematic review of the ongoing research in the applications of blockchain technology in healthcare aims to reveal the potential usage of blockchain technology, combined with clouds of sensors, and to highlight the challenges and possible research directions. The methodology of this research comprises the preferred reporting items for systematic reviews and meta-analysis (PRISMA) guidelines. According to the definition of relevant keywords and the execution of a well-designed research protocol, publications relevant to the topic were identified, using the scientific databases Scopus and Web of Science. After a bibliometric analysis of the articles, it was possible to identify the relevance of the topic and the possible applications in the healthcare sector.

Keywords: Blockchain; Healthcare; Cloud of Sensors, Edge Computing, Electronic Medical Records.

SUMMARY

FIGURE INDEX 7

TABLE INDEX 8

ACRONYMS LIST 9

1. INTRODUCTION 10

2. BACKGROUND 13

2.1 Electronic Medical Records (EMR) 13

2.2. The Healthcare Technology 15

2.3. Blockchain technology 17

2.3.1 Consensus algorithm technology 20

2.3.2 Cryptographic hash function technology 22

2.4. Clouds of Sensors 26

2.5. The blockchain-enabled cloud of sensors 31

3. RESEARCH METHODOLOGY 34

3.1 Definition of Research Questions 35

3.2 Conducting the Research 35

4 RESULTS OF SYSTEMATIC LITERATURE REVIEW 39

4.1 Classify papers 39

4.2 Analyze papers 41

4.3 Results and research gaps 45

4.4 Research Result 62

5. CONCLUSION 68

6. REFERENCES 70

FIGURE INDEX

Figure 1. Hash function operation example (By author) **23**
Figure 2. Blockchain transaction within blocks example (by author) **23**
Figure 3. Example of Blockchain network (by Author) **24**
Figure 4. Example of consensus algorithm (by Author) **25**
Figure 5. Three-tier cloud of sensors architecture (adapted from Santos, 2017) **29**
Figure 6. Scopus database string search (By author) **36**
Figure 7. ISI Web of Science database string search (By author) **36**
Figure 8. Remove duplicate articles and create a excel file on RStudio® (By author) **37**
Figure 9: Research flow diagram (By Author) **38**
Figure 10. Paper classification by segment area (By author) **39**
Figure 11. Research selection by year of publication (By Author) **45**
Figure 13. All publishing countries. (by author) **46**
Figure 14. Total Citations per country. **47**
Figure 15. Most Cited Documents **48**
Figure 16. Most relevant word for Word Cloud (by author) **49**
Figure 17. Most relevant word for Word Cloud replaced by unique word (by author) **49**
Figure 18. List of most cited word replaced by an unique word (By Author) **50**
Figure 19. Word growth over year **51**
Figure 19. Thematic Word Map graph with five groups and three words (By Author) **52**
Figure 20. Thematic Word Map correlation groups (by author) **53**
Figure 21. Thematic Word Map correlation groups (by author) **67**

TABLE INDEX

Table 1. Most cited paper after initial search. (by author) 37
Table 2. Segment distribution (absolute numbers) 40
Table 3. Papers listed by health characteristics classification (by author). 41
Table 4. All related papers used to final SLR results (by author). 44
Table 5. List of total publishing by countries. 47
Table 6. Classification of Articles (by Author) 59
Table 7. Articles by Technology Area (by Author) 60
Table 8. Articles by Focus usability area. (By Author) 61
Table 9. Types of sensor used (By Author) 61
Table 10. Articles that consider Fog technology per year (By Author) 61
Table 11. Internet of things technology surveillance domain (by Author) 62
Table 12. Articles regarding controlling and tracking medicine information (by Author) 64
Table 13. Articles regarding EMR information (by Author) 66

ACRONYMS LIST

BIOT	Blockchain IoT
BLE	Bluetooth Low Energy
BoS	Body of Sensor
BPIIoT	Blockchain Platform Industrial IoT
CGMs	Continuous Glucose Monitors sensor
CHD	Coronary heart disease diagnosis
COS	Cloud of Sensors
E -PHI	Electronic protected health information
EHR	Electronic Healthcare Records
EMR	Electronic Medical Records
H - IoT	Healthcare IoT
HIPAA	Health Insurance Portability and Accountability Act
IOMT	Internet of Medical Things
IOT	Internet of Things
MEC	Mobile edge computing
PHR	Personal Health Records
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta Analyzes
RHM	Remote Health Monitoring
SLR	Systematic Literature Review
SSN	Semantic Sensor Network
WBAN	Wireless Body Area Network
WoS	Web of Science
WSAN	Wireless Sensor and Actuator Networks
WSN	Wireless Sensor Network

1. Introduction

The future significance of the Internet of Things (IoT) is evident due to its application in everyday life. According to Souza,et al, (2020) IoT is a technological concept where different devices from our daily lives, such as mobile sensors, intelligent watches, appliances or even clothes, are connected to/through the Internet. This technology continues to grow rapidly due to evolution of hardware techniques such as improving bandwidth by incorporating cognitive radio based networks to address underutilization of frequency spectrum (Khan, et al, 2017; Akhtar, et al, 2016). Leveraging the wireless sensor and actuator networks (WSANs) (Rawat. et al, 2013) within the scope of the IoT, the novel cloud of sensors (CoS) paradigm (Santos, et al, 2015) emerged combining WSANs with cloud computing (Alamri, et al, 2013), making up a two-tier architecture. Since another paradigm has emerged: the edge computing (Bonomi, et al, 2012), it has proposed the virtualization of physical edge devices, to enable computation, storage, and networking capabilities at the edge of the network, i.e. among the sensor nodes and traditional clouds (Bonomi, et al, 2012). Thus, the current state of the art in CoS combines WSANs and cloud/edge computing paradigms in the form of a three-tier CoS architecture (comprising the sensor, edge and cloud tiers). Meanwhile several challenges exist in CoS, including how to solve related security threats including data integrity, data freshness, availability of the network, data authentication, secure management, dependability, secure localization, accountability, and flexibility. Blockchain technology has the potential to help overcome such issues.

The blockchain technology could be implemented in several different areas, such as legal, finance, food industries, smart properties, banking, and supply chain network (Badr, et al., 2018; I. & Likic R. AO - Likic, 2018; Kumar & Tripathi, 2019; Wang, et al., 2019; Min, 2019). It is a technology and architecture system, first published by Nakamato, 2008, and was launched in 2009. This technology has gained widespread importance and acceptance in last few years, based on (i) guaranty of immutability and integrity of raw data, (ii) no need of third trusted party, and (iii) running decentralized and trustable transactions (Abujamra & Randall, 2019; Banerjee, et al., 2018; Zhang, et al., 2018; Galvez, et al., 2018). Blockchain works by storing information in

recording ledgers among peers bellowed into a distributed computer network infrastructure in a decentralized manner across computing devices that are members of this system.

Blockchain has the main purposes to provide security, immutability and trackability into information systems, based on cryptography algorithms. In spite of those characteristics, at the first moment, were typically relational for banking and financial applications, it can be used for trackability elements into several different areas, such as logistic and supply chain network. Blockchain works as a peer-to-peer distributed and decentralized technology, using a ledger to record all approved digital transactions (Christidis and Devetsikiotis, 2016). In addition, the blockchain ledger offers highly reliable storage capabilities as it is created using consensus algorithm mechanisms, cryptographic signatures, and hash chains (Zhao et al., 2017). Each transaction is according to the rules at smart contract and its approval is based on consensus among blockchain peers. All peers belonging to a blockchain (private, consortium or public) have a copy of the smart contract and the ledger (Tapscott, 2016).

Although the banking and finance sectors have had more research focus, based on the initial article about bitcoin (Nakamoto, 2009), the healthcare sector recently started to receive more attention as a blockchain enabled application, according to our research. Publication into this area started from 2015 (Yue, et al., 2016) regarding Electronic Medical Record (EMR) controls and how to secure the data. Several researchers have highlighted the potential of using blockchain technology to address existing challenges in healthcare applications (Abujamra and Randall, 2019; Banerjee, et al., 2018; Benchoufi and Ravaud, 2017; Chen, et al., 2018; Kuo, et al., 2017; Hölbl, et al., 2018; Agbo, et al., 2019; Dubovitskaya, et al., 2017; IEEE-SA, 2017; Tseng, et al., 2018).

The usage of blockchain can be applicable with healthcare management applications in public or private areas, monitoring and automated health claims adjudication and online patient information, achievement of healthcare records, sharing patients' medical data information, pharmaceutical and drug medicine counterfeiting, medical clinical trial, and precision medicine. (Casino, et al., 2019; Boulos, et al., 2018; Badr, et al., 2018; Benchoufi and Ravaud, 2017; Gordon and Catalini, 2018; Vazirani, et al., 2019). The utilization of cloud of sensors and blockchain technologies together, in the healthcare chain, could solve problems of scientific credibility of losing information, (data missing or dredging, endpoint switching and selective publication) in clinical trials (Nugent et al., 2016) as well as issues of patients' informed consent (Benchoufi and Ravaud, 2017; Benchoufi et al., 2017).

The adoption of blockchain-enabled CoS technology into hospital operations tends to increase the efficiency, reflecting on cost reduction because virtually all transactions with blockchain are safer, more transparent, traceable and efficient (Aste et al., 2017; Kshetri, 2018). Furthermore, blockchain adoption can enhance customers' trust, which will allow them to check the entire journey of goods across the operational chain in full confidence. In this regard, the traceability (Biswas et al., 2017) mechanisms of the blockchain will support products of fraud prevention and fraud across the whole chain. As a result, the hospital healthcare operation chains will gain efficiency and cost reduction.

Given the aforementioned challenge, the main objective of this dissertation is to perform a systematic review regarding blockchain, clouds of sensors and healthcare, among scientific reference databases. We also have two secondary objectives. First, to show the number of publications regarding the usage of blockchain, across a cloud of sensor networks, to support the healthcare operations, and discuss the relevant publications. Second, to indicate the potential challenges and future research directions of applications of blockchain in healthcare using clouds of sensors.

This dissertation is organized as follows. Technologies (EMR, Blockchain, Healthcare and Cloud of Sensors) where is presented the background information of those different areas and the combination among them; The research review, where is presented the methodology and the outcomes from systematic review; Research results, which include the bibliometric overview and analysis of data and the quality assessment results; The discussion of the results and research question answered; and the summed up with conclusion and discussion of future work.

2. Background

This section introduces the basic concepts and background on the main subjects approached by our work. Section 2.1 reviews Electronic Medical Reports, Section 2.2 reviews healthcare technology, Section 2.3 discusses blockchain technology, Section 2.4 introduces the Cloud of Sensors concept. Section 2.5 discusses the blockchain-enabled CoS.

2.1 Electronic Medical Records (EMR)

Medical information records or any data related to the health, diagnosis and treatment of patients are considered extremely sensitive and private information. Challenges associated with data stored, processing, privacy and security continue to rise concurrently, since the healthcare industry highly relies on the data. Health data privacy implies securely and privately processing of the patient data or the need for authorization to access the data. Besides, security refers to safeguarding sensitive data from intruders and listeners (Al Omar, Rahman, Basu, & Kiyomoto, 2017).

With the development of electronic information technology, electronic medical records (EMR) have been a common way to store the patients' data in hospitals. They are stored in different hospitals' databases, even for the same patient. Therefore, it is difficult to construct a summarized EMR for one patient from multiple hospital databases due to the security and privacy concerns. Meanwhile, current EMRs systems lack a standard data management and sharing policy, making it difficult for pharmaceutical scientists to develop precise medicines based on data obtained under different policies (Fan et al., 2018)

With the increased number of developments of information technology systems into hospitals or healthcare areas, a huge amount of information is processed, transferred and stored into electronic devices. According to ISO/TR 14639, the "information relevant to the wellness, health and healthcare of an individual, in computer processable form and represented according to a standardized information model" is called EHR or Electronic Health Records and it refers to an electronic way to structure patient's health records, collected and stored in a data repository, that can be shared by different digital formats. These records can contain several data groups, such as

allergies, laboratory exams results, medical appointments, vital signs, medical imaging and diagnoses (Roehrs, et al., 2017). Another type of patient record is named EMRs or Electronic Medical Records, and it distinguishes health records that are not integrated between healthcare providers. To differentiate from EHR, EMR has a special focus into the internal medical domain of health organizations (Roehrs, et al., 2017).

Also, according to ISO/TR 14639, PHR or Personal Health Records refers to a ‘‘representation of information regarding, or relevant to, the health, including wellness, development and welfare of that individual”. The owner of those records is the patient, and they can share, manage and also grant the permission to any other third parties. Although PHR data is oriented to the patient, it can be received from healthcare providers, be stored into a repository where the patient has access, and if permitted, it can be integrated with EHR (Roehrs, et al., 2017). Many publications discuss record keeping. The majority in the form of EHRs, while the minority propose or discuss electronic medical records (EMRs) and personal health records (PHRs). In this paper we combine these into the field of electronic medical records and use the acronical as EMR.

Consent data of patients are distributed across different controls as lifecycle events, which allow taking them away from one data provider to another (Cartwright-Smith, Gray, and Thorpe, 2016). This type of information is normally shared among peers such as clinics, hospitals, healthcare providers, researchers, insurance companies, healthcare centers and patient’s families. This implies a serious challenge to safeguard these valuable data as well as updating the medical history of the patient. This information between multiple units need to be saved and shared, as the patient’s treatment process could be hindered if multiple access control over numerous users is not enabled (Health, Staff, & Register, 2005; Meng, Tischhauser, Wang, Wang, & Han, 2018). The access to a full patient data history is very critical to continue his treatment, particularly for long-term treatment cases such as cancer patients, cardiovascular patients or HIV patients, and requires knowing the laboratory results, the medication doses or medicines’ negative side effects. The patient may also be required to visit different medical institutions for consultation or may even get transferred from one hospital to another, and to execute such an action, sharing of the patient’s clinical data is mandatory for the treatment purposes. Coordination becomes more difficult, especially when a patient moves to another region, city or a country and is unsure of the hospital or caregiver where he will be receiving the treatment. The data sharing features allows the medical

research institute to better understand, make the collaboration seamless between various healthcare providers and facilitate secure sharing with standard regulations (Yang, Li, & Niu, 2015).

Our current healthcare system is plagued with information silos and inefficient data interchanges between electronic medical record vendors, providers, insurance companies, research organizations, and patients. Electronic mail systems are still the primary mode of patient health data exchange due to factors like organizational bureaucracy, provider apathy, misaligned incentives, and inertia (Withers, 2018). Moreover, inconsistent and insecure data storage has led to massive breaches of patient data from large healthcare entities globally (Pierson, 2017). This led to significant public backlash and mistrust in the way patients' data are stored, interpreted, and potentially sold without their knowledge. Because of inefficient data sharing, physicians have incomplete pictures of patients' health profiles, which leads to slower treatment and poorer health outcomes (Wicks et al., 2010).

Current methods to protect and secure records have proven not to be as efficient as they should be, and dissemination of a patient's medical records can have real-world consequences (e.g. risks to patients' privacy in the form of malicious attacks, which can damage the reputation and finances related to those records) (Xia et al., 2017; Xu, 2016). In addition, only the encryption of EMR can be problematic if different encryption standards are used in different systems, causing interoperability issues (Xu, 2016; Abouelmehdi et al., 2017; Khan and Hoque, 2016; Vithanwattana et al., 2016).

2.2. The Healthcare Technology

Healthcare is defined by Cambridge Dictionary (https://dictionary.cambridge.org/, accessed in 31, July, 2021) as a set of services provided by an organization or country for the treatment of the physically and the mentally ill, or also defined as the activity or business of providing medical services. Hospitals, clinics and medical communities are also part of the healthcare system, it can be public, private and nonprofit systems. All of them have focused on patient health. The healthcare system has become complex year after year for over the last three decades (Plsek and Greenhalgh, 2001; Reibling et al,2019) due to differences regarding how countries fund, provide, and organize their health system.

A health unit can be considered as an establishment that provides, promote and also maintain direct or indirect health services condition of an individual (Gomes et al., 2016; Viera, 2019) and also can be considered a healthcare facility. To define the quality of healthcare, it can be seen as the extent to which health services for populations and individuals increase the probability of desired health outcomes and care consistent with current professional knowledge (Gomes et al., 2016; Viera, 2019). To compare and to analysis of health networks through operations management models it may not be as effective as in an industrial environment, where the material flows, and process activities are well defined. Products are replaced by patients, medical doctors, nurseries who can freely move through the process as they wish and production is replaced by a much less deterministic trajectory of care. (Antonelli and Bruno, 2015; Viera, 2019).

The healthcare system has a variety of 'agents' coexisting together (Scarlat et.al 2011). They can be an organization agents, such as hospitals, drugs suppliers, medical equipment suppliers, food and linen suppliers, specialized cleaning and sterilizing suppliers, logistics and IT companies; also can be people agents such as doctors, patients, nurses, administrative personnel, pharmacists, patient's families and IT specialists); and practical agents like medical knowledge, practices, protocols and rules, regulations, technologies, standards. This diversity of agents acts within two functional structures: the healthcare supply chain and the clinical chain (Maracine and Scarlat, 2009; Scarlat and Maracine 2009; Bali, 2005).

The healthcare supply chain consists of the interaction of vendors, manufacturers of various medical products, group purchasing organizations, distributors, hospital internal chains, IT tools and logistical practices in a wide variety of situations. Alongside all these components, the most distinctive characteristic of the healthcare supply chain is its dependency on the point of care, which is the consumption driver in the clinical chain. On the other side, the clinical chain is a collection of medical and clinically related activities supporting the healthcare continuum (prevention – diagnosis – treatment – recovery). These activities can occur in what we call the point of care, i.e. the place where the patient and the healthcare professional interact (e.g. operating rooms, hospital wards, outpatient clinics, doctors' offices, patients' homes or workplaces).

The process of exchanging information among healthcare agents into the healthcare industry and its associated institutions there were no guidelines or rules. There were basically no generally accepted safety standards, nor were there any requirements for the protection of health

information across those agents. The primary provision regulated the guidelines set out in the Health Insurance Portability and Accountability Act (HIPAA) which was passed in 1996 (Pirc, J, et. al, 2016). The HIPAA consists of several sections, or rules, that must be followed in order to remain compliant. The important rule that we would like to discuss, and the usability of blockchain is expected, is the security rule as it provides the governance with respect to the technology and protection of electronic protected health information (e-PHI), and we referenced this document as EMR. In accordance with the HIPAA Security Rule Summary, the Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical and physical safeguards to protect e-PHI. Specifically, covered entities must ensure the confidentiality, integrity, and availability of all e-PHI created, received, maintained or transmitted; it must identify and protect against reasonably anticipated threats to the security or integrity of protected information, must protect against reasonably anticipated, impermissible uses or disclosures of e-PHI and must ensure compliance to the HIPAA Security Rule of all employees. (Pirc, J. et. al, 2016)

The HIPAA Security Rule defines confidentiality as meaning that the e-PHI shall not be made available or disclosed to any not authorized person to access it and follows the definition of confidentiality as described in the HIPAA Privacy Rule. The Security Rule also defines other key areas that must be considered while operating in the healthcare industry, such as Risk Analysis and Management that conducting regular risk analysis as part of the defined security management process, also define administrative safeguards that must designating an official security officer, putting in place the proper security management process, to oversee items such as risk analysis and conducting regular workforce training. Another rule is for physical and technical safeguards as the first one ensuring access to facilities as well as access to workstations areas and devices that may have access to e-PHI and the second must assure access control, auditability, integrity controls, and secure transmissions when accessing e-PHI. Another rule is to adopt a reasonable and appropriate policies to comply all security rule requirements as well as maintain a document retention policy definite elements. (Pirc, J. et. al, 2016).

2.3. Blockchain technology

Blockchain is a technology and a system architecture that runs over a communication network (which we call the blockchain infrastructure), first published by Nakamoto (Nakamato S. 2008), and was launched in 2009. This technology has gained widespread importance and acceptance in the last few years, based on two features. The first feature is its guarantee of immutability (Any records will be reserved forever, and can't be changed unless someone who has control more than 51% node in the same time (Niranjanamurthy et al, (2018)), integrity (preventing resources to be modified without authorization resources), transparency (data's record by Blockchain system is transparent to each node, each of these nodes can further update the data as well which makes it transparent and trustworthy), security (protecting personal data from unauthorized third-party access or malicious attacks and exploitation of data), and trackability (capable to being tracked) for the native data, i.e. the data that is created solely by the customer of an application in the network or its agents and is stored in the blockchain. The second feature is its decentralized (does not have to rely on centralized nodes, the data can be recorded, stored and updated on multiple system) nature, i.e. there is no need of a centralized trusted third party to validate transactions among peers in the network (Abujamra & Randall, 2019; Banerjee, et al., 2018; Zhang, et al., 2018; Galvez, et al., 2018). Where a transaction can be defined as an agreement between two entities to exchange services, goods, financial instruments, to order actions and command. Thus, the blockchain also guarantees immutability, integrity, transparency, security, and trackability for the transactions that occur inside it.

Current blockchain systems are categorized roughly into three types: public blockchain, private blockchain and consortium blockchain (Buterin, 2015). In public blockchain, all records are visible to the public and everyone could take part in the consensus process. Since the public blockchain is open to the world, it can attract many users and communities are active. As for private blockchain, only those nodes that come from one specific organization would be allowed to join the consensus process. Also, private blockchain is regarded as a centralized network since it is fully controlled by one organization. Differently, only a group of pre-selected nodes among organizations would participate in the consensus process of a consortium blockchain. The consortium blockchain is constructed by several organizations and is partially decentralized since only a small portion of nodes would be selected to determine the consensus. As for consortium blockchain, it could be applied into many business applications. Currently Hyperledger (Hyperledger project,2015) is developing business consortium blockchain frameworks. Ethereum

also has provided tools for building consortium blockchains. (Zheng et al., 2017)

By giving the required tool to establish consensus among spread entities without depending on a single reliable party, the blockchain technique will ensure the data security, the control over sensitive data, and will facilitate healthcare data supervision for the patient as well as different actors in medical area (Dorri, S. et al., 2017; Sachs, 2016). As per Brodersen et al. (2016) Blockchains can be defined as "cryptographic protocols that allow maintaining a shared ledger of information via a network of computers (nodes) collectively and a complete trust is not required amongst the nodes". The blockchain methodology has helped understand numerous issues relating to the current health information technology paradigms, involving immutably assuring expressed identities, security (specifically data integrity) and privacy, improving healthcare-related security for both patients and providers and creating highly robust audit trails. The private sector has been experimenting by applying blockchain technology across the industries, including healthcare, owing to benefits like distributed ledger technologies (Fairley, 2017).

Blockchains have the potential to revolutionize the way health data is stored, handled, and efficiently exchanged between healthcare entities while maintaining these entities' incentives. For example, after a patient receives a lab result, the data – instead of being stored centrally on the lab's servers – can be stored encrypted on the blockchain network. The data itself can be tagged with the creator of the data (i.e., the lab) so any parties who access data in the future can see who generated it. This allows for the preservation of commercial incentives for the lab as they will still be able to bill insurance companies and receive funding based on their work. However, the control of the data is now given to the patient, who can actively decide to share it with a new family doctor or send it to a university for research purposes. This reduces concerns surrounding lost or corrupt data, slow exchange of data, and unknown reselling of data. (Hughes et al, 2019).

Blockchain uses a ledger to record all approved digital transactions (Christidis and Devetsikiotis, 2016). A ledger holds a complete list of transaction records and each peer of the blockchain infrastructure (private, consortium or public) has a copy of the same ledger (Tapscott, 2016). A blockchain also has smart contracts, where a smart contract has discussed and approved rules among peers and it needs to be tested to (i) satisfy the contractors' specifications, (ii) comply with the laws of the legal systems involved, and (iii) do not include unfair contract terms. The peers that contain the ledgers and smart contracts are bellowed into a decentralized infrastructure across computing devices that are members of the blockchain infrastructure (network). In a

decentralized network, there is a random process to select someone to record the transactions. However, random selection is vulnerable to attacks. Therefore, if a node wants to publish a block of transactions, a lot of work has to be done to prove that the node is not likely to attack the network. In this case it must have a consensus strategy to validate the transaction.

2.3.1 Consensus algorithm technology

In blockchain, how to reach consensus among the untrustworthy nodes is a transformation of the Byzantine Generals Problem (Lin, I. C. et al., 2017; Cachin and Vukolic, 2017) that is knowledge by a group of generals who command a portion of the Byzantine army to circle the city. Some generals prefer to attack while other generals prefer to retreat. However, the attack would fail if only part of the generals attacked the city. Thus, they have to reach an agreement to attack or retreat. How to reach a consensus in a distributed environment is a challenge. It is also a challenge for blockchain as the blockchain network is distributed. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. Some protocols are needed to ensure ledgers in different nodes are consistent, this mechanism is called consensus algorithm. There are a few types of consensus algorithm, and the usability and relevance will depend on the type of application or transaction. (Syed, T. A. et al., 2019).

Proof of work (PoW) is a consensus strategy that each node in the network is responsible to calculate a hash value from the block header. It is considered not energy efficient due to a lot of energy spend to solve the work. The headers block contains a nonce and miners would change the nonce frequently to get different hash values (Syed, T. A. et al., 2019). Consensus requires that the value, from result of calculate math problem, be equal to or less than a certain value. When a node reaches the target value, it transmits the block to all other nodes and all of them must mutually confirm the hash value correctness. If the block is validated, new block will be attached to their own blockchains. In the decentralized network, valid blocks can be generated simultaneously when multiple nodes find the appropriate nonce at almost the same time. In this scenario a branch can be generated, and it is unlikely that two simultaneous forks will generate the next block simultaneously. In this scenario a chain that becomes longer after that is considered authentic.

Proof of stake (PoS) is an energy-saving alternative to PoW. Those peer in PoS have to prove the ownership of the amount of currency. It is believed that people with more currencies would be less likely to attack the network. The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Compared to PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come consequently. (Syed, T. A. et al., 2019)

Delegated proof of stake (DPOS) is an evolution of PoS. The difference between PoS and DPOS is that PoS is directly democratic while DPOS is representative democratic. An representative stakeholders elect their delegates to generate and validate blocks. With significantly fewer nodes to validate the block, the block could be confirmed quickly, leading to the quick confirmation of transactions. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by delegates. Additionally, users need not to worry about the dishonest delegates as they could be voted out easily.

Practical byzantine fault tolerance (PBFT) is a replication algorithm to tolerate byzantine general faults (Miguel and Barbara, 1999). PBFT is a consensus algorithm that could handle up to 1/3 malicious byzantine replicas. A new block is determined in a round. In each round, a primary would be selected according to some rules. And it is responsible for ordering the transaction. The whole process could be divided into three phases: pre-prepared, prepared and committed. In each phase, a node would enter the next phase if it has received votes from over 2/3 of all nodes. So PBFT requires that every node is known to the network. Like PBFT, Stellar Consensus Protocol (SCP) (Mazieres, 2015) is also a Byzantine agreement protocol. In PBFT, each node has to query other nodes while SCP gives participants the right to choose which set of other participants to believe.

Ripple is a consensus algorithm that utilizes collectively trusted subnetworks within the larger network. In the network, nodes are divided into two types: server for participating consensus process and client for only transferring funds. Each server has an Unique Node List (UNL). UNL is important to the server. When determining whether to put a transaction into the ledger, the server would query the nodes in UNL and if the received agreements have reached 80%, the transaction would be packed into the ledger. For a node, the ledger will remain correct as long as the

percentage of faulty nodes in UNL is less than 20%.

Tendermint is a byzantine consensus algorithm. A new block is determined in a round. A proposer would be selected to broadcast an unconfirmed block in this round. It could be divided into three steps: 1) Prevote step. Validators choose whether to broadcast a prevote for the proposed block. 2) Precommit step. If the node has received more than 2/3 of prevotes on the proposed block, it broadcasts a precommit for that block. If the node has received over 2/3 of precommits, it enters the commit step. 3) Commit step. The node validates the block and broadcasts a commit for that block. if the node has received 2/3 of the commits, it accepts the block. Unlike PBFT, nodes have to lock their coins to become validators. Once a validator is found to be dishonest, it would be punished.

2.3.2 Cryptographic hash function technology

A mathematical representation of an algorithm is the cryptographic hash function that allows arbitrary size mapping data to a bit string that has a static size (a hash), that is also calculated to act as a unidirectional function, i.e. a function that is infeasible to invert (Miller, Juels, Shi, Parno, & Katz, 2014). Attempting a brute-force search for possible inputs is the only method to reconstruct the input data over an ideal cryptographic hash function's output to check if a match is produced, or if there is a need to use a rainbow table for matched hashes (Christidis & Devetsikiotis, 2016). According to B. Schneier, unidirectional hash functions are called 'the modern cryptography workhorses' (Schneier, 2014). The message is most of the time the input data, while the output (the hash or hash value) is commonly known as the message digest or just the digest. The model cryptographic hash function can be characterized as: quick to compute the hash value, deterministic, changeable with original message changing, infeasible to generate a message from its hash value and non-redundant (impossible to determine if two different messages would generate the same hash value) (Lei et al., 2017; Thomas & Martin, 2006).

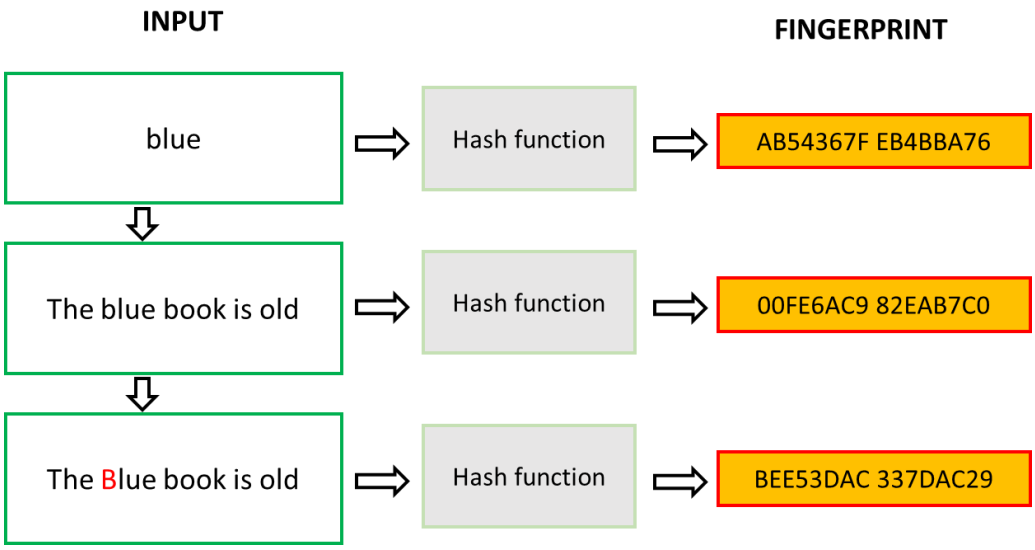


Figure 1. Hash function operation example (By author)

Each block into the blockchain network is responsible for validating the next transaction, due to the use of a hash algorithm to create a hash code for the last transaction. This sequential dependency has created a chain of blocks. In order for a transaction to be validated, there is a need for consensus based on characteristics of the network. If there is an attempt to modify outside the standards of a previous block, there will be no consensus and the transaction will fail (Badr, et al., 2018; Brogan, et al., 2018; Boulos, et al., 2018; Casino, et al., 2019). That process guarantees the immutability, trackability and security of data into blockchain network

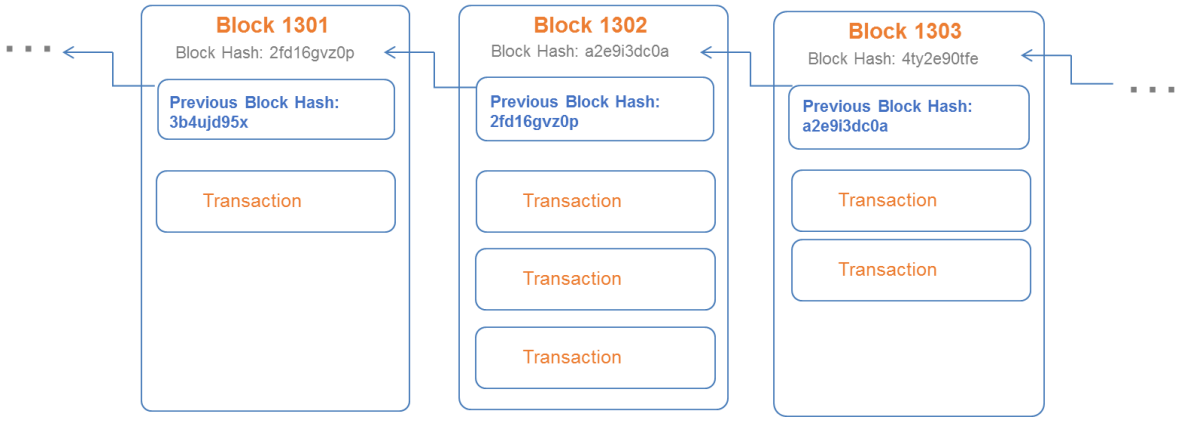


Figure 2. Blockchain transaction within blocks example (by author)

The blockchain ledger offers highly reliable storage capabilities as it is created using consensus algorithm mechanisms, cryptographic signatures, and hash chains (Zhao et al., 2017). Each transaction is based on a smart contract and its approval is based on consensus among blockchain peers. Each *peer* is part of the blockchain network and can be represented by part of the healthcare system, such as hospitals, medicals, pharmacies, patients, banks, drugs resellers, governor entities. The peer´s ring network representation from the Figure 3 is a didactic explanation because every peer is interconnected with each other into a blockchain network.

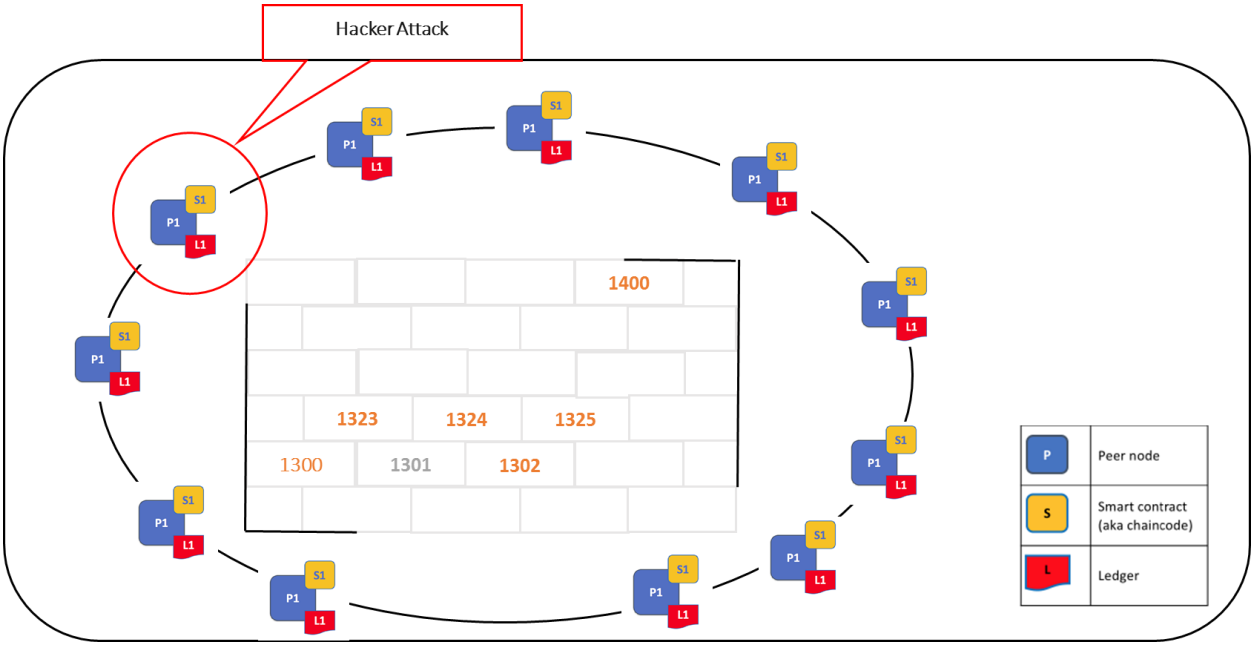


Figure 3. Example of Blockchain network (by Author)

Every peer has the same copy of ledger (red color item) and smart contract (yellow color item). The wall represented in the Figure 4 is the chain of blocks and they are represented as a consecutive horizontal sequential couple of blocks, from left to right, and from button up. Assuming that we are now preparing the transaction for block number 1401, we are in 1400´s block. According to the functioning of the blockchain, the 1400´s block, after it has been validated, a transaction hash code was generated from 1399´s bock, all transactions were validated and stored into ledger, according to the smart contract terms, and it has been copied to all *peers* members of

the network. This *hash* will be used to validate the next 1401 block transaction by generating another *hash code*. We will assume that this network is composed of 11 *peers* (P1 through P11). If a hacker tries to modify the number 1301 block, initially described in the Figure 4 as *peer* (P4), by modifying any information regarding the block number 1301.

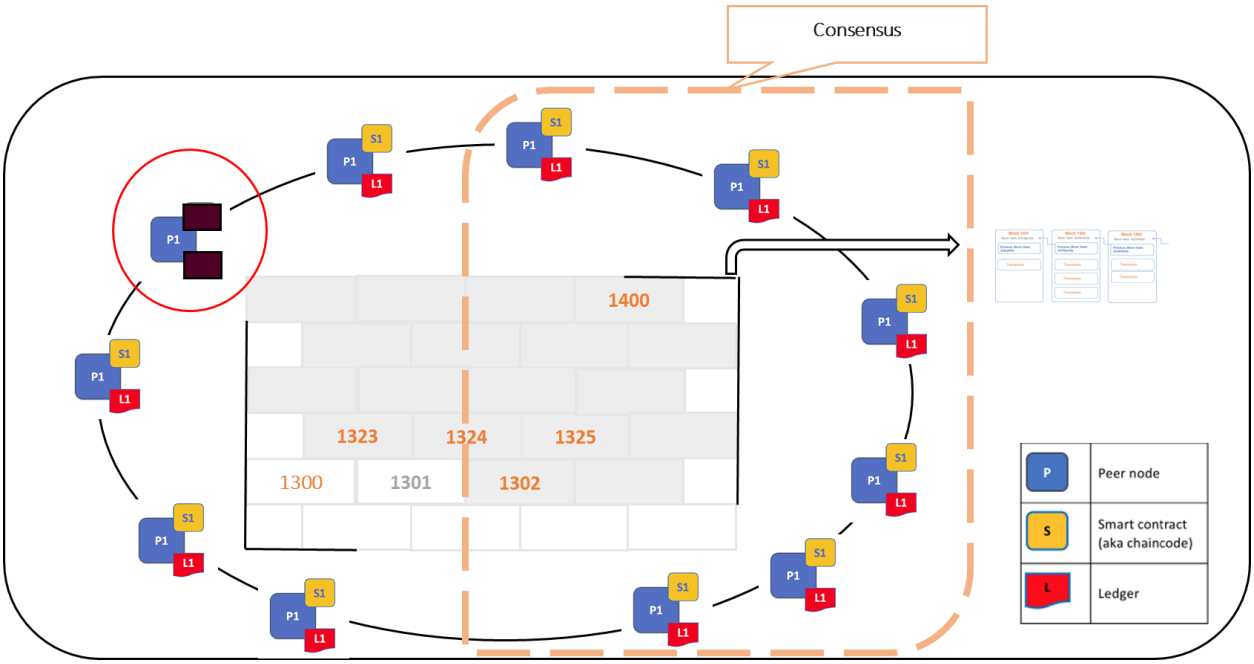


Figure 4. Example of consensus algorithm (by Author)

As the entire chain will have different information compared to that *peer*, from the number 1301 to the number 1400 inclusive, at the next time the block chain attempts to carry out the transaction validation of block 1401, the consensus algorithm will only validate the transaction if it obtains the consensus of 50% + 1 of the *peers* on the network, using any of consensus algorithm defined early. If six *peers* obtain the same consensus value, the transaction is validated between those *peers* that have made consensus and a copy of *ledger* is sent to all eleven *peers* members of the chain, overwriting the value that each had previously. That is, the *peer* P4 will not be able to affect the transaction, so it cannot modify a block that has already been transacted and written to the *ledger*.

The combination of cryptography and consensus technology given to blockchain to be considered a disruptive technology, the potential uses of blockchains transcended the initial idea of the financial industry (Nofer et al., 2017). Because blockchains allow the secure exchange of data in a distributed manner, the technology could affect the structure and governance of supply

chains as well as relationship configurations and information sharing between any type of actors. If integrated with field-sensing technologies such as the Internet of Things (IoTs), Edge Computing, Fog computing or Cloud of Sensor (CoS), blockchains could create permanent, shareable and actionable records of information digital footprints throughout the entire industry segments including healthcare. Such improved visibility would provide product traceability, authenticity and legitimacy – all of which are crucial to the pharmaceutical industry, medical accomplishment and healthcare operations.

2.4. Clouds of Sensors

With the high-speed networks and a rapid growth of smart devices, the Internet of Things (IoT) technology has gained wide acceptance and popularity as the main standard for devices for low-power lossy networks (LLNs) having constrained resources. It represents a network where ‘‘things’’ or embedded devices having electronic sensors are interconnected through a private or a public network (Khan and Salah, 2018).

These IoT devices can be controlled remotely and it is up to performing the desired functionality, such as exchange information among the devices and takes place through the network which employs the standard protocols of communication. The type of smart connected devices or ‘‘things’’ range from simple wearable accessories to large machines, each containing sensor chips, such as the electrical appliances including home power outlets, washing machines, microwave ovens and refrigerators can be controlled remotely through IoT service. The network for security cameras installed for surveillance of a location can be monitored remotely anywhere in the world using the IoT technology (Khan and Salah, 2018).

Apart from personal use, IoT and sensor devices serve the community needs as well. Various smart devices which perform diverse functionalities such as monitoring surgery in hospitals, detecting weather conditions, providing tracking in logistic or supply chain areas and connectivity in automobiles, and identification of animals using biochips are already serving the community specific needs (Rouse, et al, 2016). The data collected through these devices may be processed in real-time to improve efficiency of the entire system.

The future significance of IoT is evident due to its application in everyday life. It continues to grow rapidly due to evolution of hardware techniques such as improving bandwidth by incorporating cognitive radio-based networks to address underutilization of frequency spectrum (Khan, et al, 2017) (Akhtar, et al, 2016). In the literature, the Wireless Sensor Networks (WSNs) and Machine-to-Machine (M2M) or Cyber-Physical Systems (CPS) have now evolved as integral components for the broader term IoT.

By the evolution of interconnected devices and fast network speed growing, several sectors of industry, academia and society have been witnessing the wide spreading of a multitude of new paradigms, which are revolutionizing the field of Information and Communication Technologies (ICT) (Aleksic, 2014). The novel cloud of sensors (CoS) paradigm (Santos, et al, 2015) is one of such paradigms that has gained importance. The CoS combines wireless sensor and actuator networks (WSANs) (Rawat. et al, 2013) with cloud computing (Alamri, et al, 2013), making up a two-tier architecture.

Several IoT services, such as computation resources, storage capabilities, heterogeneity, high processing, and others that brought a technological revolution, are provided by cloud computing. Formally, a cloud is a large-scale (ideally unlimited) set of virtualized computing resources that owners can dynamically reconfigure to serve a variable load, seeking optimum resource utilization (Alamri, et al, 2013), (Liu and Wassel, 2011). Accordingly, virtualization is a key feature that grounds the cloud computing paradigm. The authors Liu and Wassel, 2011 define virtualization in terms of hiding from clients the variety of types of infrastructures, platforms and data available at the back end, facilitating application delivery.

The cloud provides the virtualization of computing resources at various levels (Mubeen et al.,2017), such as network, server, storage, and almost all the human life domains have adopted cloud computing (Bilal et al., 2016). However, cloud computing has drawbacks in terms of high delays which have an adverse effect on the IoT tasks that require a fast or real-time response. Furthermore, it does not match industrial control systems which require a low delay response time (Mubeen et al.,2017). According to Elmisery et al., 2017, the Cisco Company announced, in 2012, an infrastructure paradigm called edge computing, which is a new computing concept, to tackle the limitations of cloud computing. They asserted that edge computing is applicable at three networking levels: First, there is a collection of data from the devices in the sensor (sensors, vehicles, roadways, and ships) level ; Second, there are multiple devices connecting to a network

and sending all the data; Third, there are collection of data from the devices that should be processed in less than a second along with decision making (You and Learn, 2015)

The edge computing term shifts capabilities of the cloud near to the end user, and provides storage, computation, and communication to edge devices, this facilitate and enhance mobility, security, privacy, low latency, and network bandwidth so that edge computing can perfectly match latency-sensitive or real-time applications (Hu et al.,2017). On the one hand, edge computing infrastructure consists of several edge nodes, edge device networks, and even virtualized data centers or IoT sensors or devices that are connected to these nodes (Zhang et al.,2016). These are connected to the cloud for the purpose of implementing large storage and rich computing (AAzam et al., 2016). The distribution of functions among the cloud and the edge nodes is a crucial factor, due to millisecond to sub-second latency offered by edge, even faster than real-time interaction, supports multi-tenancy and performs better in low-latency applications. The concept of edge computing has been designed to satisfy the applications that require low latency with a real-time response such as healthcare IoT systems (Cerina et al.,2017; Li et al.,2015; Bilal et al., 2017).

The edge computing level are composed by physical heterogeneous devices in terms of their capabilities and can be either resource-poor devices such as access points, routers, switches, base stations, and smart sensors, or resource-rich machines like a “cloud-in-a-box”, such as Cloudlets (Yi, et al, 2015). Edge devices perform several tasks, for instance, collecting the data and performing preprocessing, filtering the data and reconstructing it into a more useful form, uploading only the necessary data to the cloud. In addition, edge nodes can monitor smart objects and sensor activities, keeping check on their energy consumption. The edge consumes locally the portion of data generated by sensors that require real-time processing (from milliseconds to tenths of seconds). Then, it transmits the rest of such data to the cloud, for operations with less stringent time constraints (from seconds to minutes) (Bonomi, et al, 2012). Therefore, edge computing allows real-time delivery of data, especially for latency sensitive services. On the other hand, the closer to the cloud, the longer the time scale, and the wider is the geographical coverage. The cloud provides the ultimate and global coverage and serves as a repository for data for a duration of months or years, besides allowing more complex data analytics, based on historical data.

Combining WSANs and cloud/edge computing in the form of a three-tier CoS architecture (comprising the sensor, edge and cloud tiers) potentially leverages mutual advantages. On the one hand, WSANs could benefit from the virtually unlimited resources, besides the low latency,

mobility and location-awareness support, of a cloud/edge environment to implement service management and composition for exploiting the smart sensors and their produced data. On the other hand, the cloud/edge computing paradigms can benefit from WSANs by extending their scopes to deal with real world objects in a distributed and dynamic way, enabling the delivery of a wider variety of new services in real world scenarios. The CoS architecture is shown in Figure 6. Three tiers compose this architecture: sensors tier (ST), edge tier (ET) and cloud tier (CT).

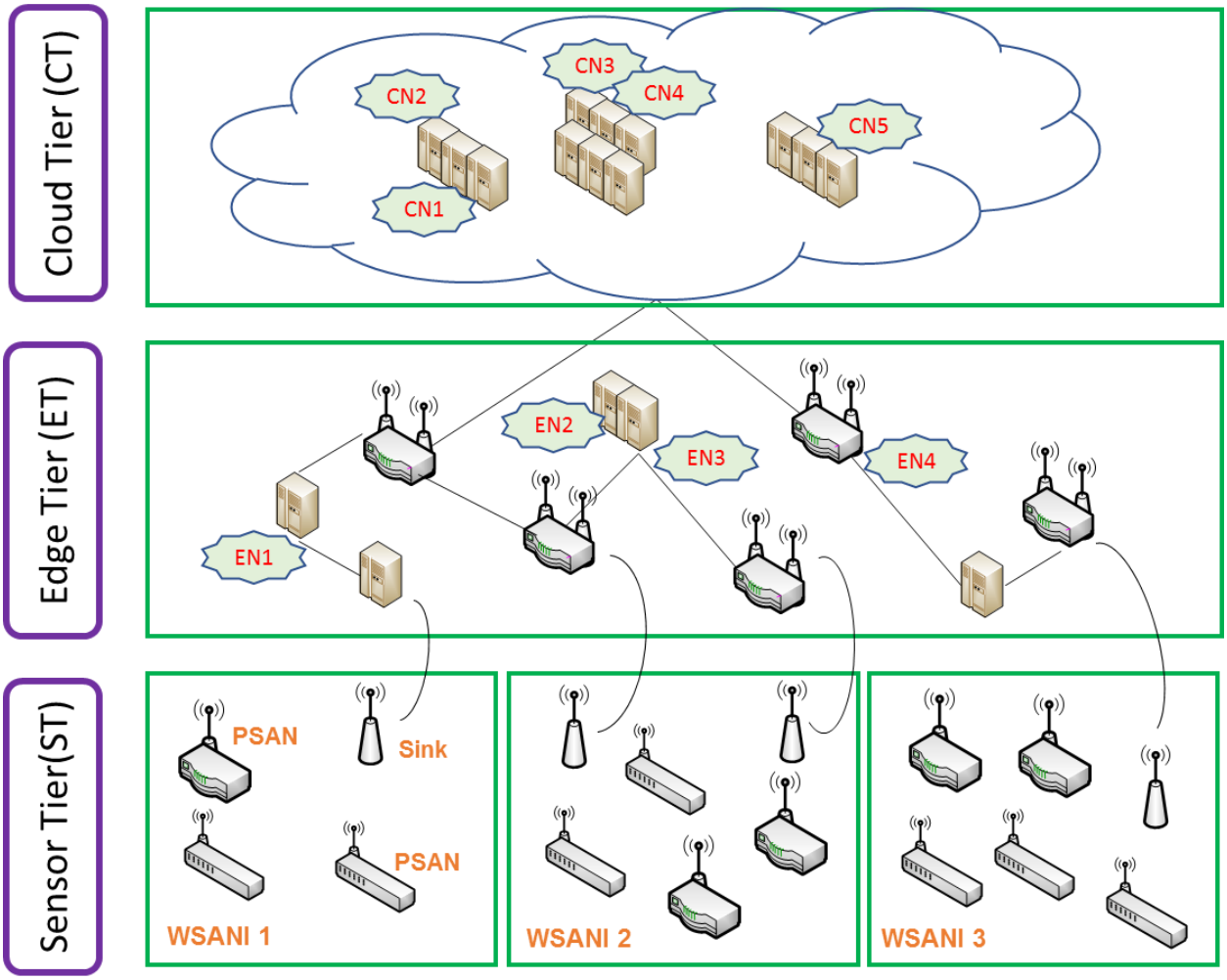


Figure 5. Three-tier cloud of sensors architecture (adapted from Santos, 2017)

The sensors tier comprises the physical wireless sensor and actuator network infrastructures (WSANIs), each of which is owned and administered by an infrastructure provider. Each WSANI comprises a set of physical sensor and actuator nodes (PSANs) deployed over a

geographical area, in our case a hospital, clinic or pharmaceutical store and connected by wireless links, so that every PSAN pertains to a single WSANI.

The edge tier comprises the edge nodes, which are typical physical edge devices. Such devices can be resource-poor devices such as access points, routers, switches, base stations, and smart sensors, or resource-rich micro-data centers and machines, such as cloudlets (Yi, et al, 2015). The cloud tier comprises the cloud nodes, which are multiple physical data centers (more powerful than physical edge devices) responsible for a global view of the CoS system. Cloud physical data centers can perform data-intensive computation, time-based data analysis and permanent storage of huge amounts of valuable data. The InPs can combine multiple physical data centers for providing services in the global scale, and each physical data center has a heterogeneous cost for providing its services (Santos, 2017).

In three-tier CoS architecture, is considered the existence of three main entities, namely the PSANs at the sensors tier, the edge nodes at the edge tier and the cloud nodes at the cloud tier. PSANs as being the physical devices of the sensors tier themselves, while is described the edge and cloud nodes as being virtual instances hosted by the physical devices of edge and cloud tiers, respectively. This device arrangement considers that the deployment of each edge and cloud node on their respective physical hosts is transparent to our CoS architecture and is handled by typical cloud and edge computing virtualization models. In addition, each edge and cloud node has information about the physical device that hosts it, so that we can associate the physical location of an edge or cloud node to the location of its physical host (Santos, 2017).

The fusion of electronic equipment and processes with mobile and embedded devices has the potential to improve efficiency, access and the quality of personalized service. Wearable and embedded devices (such as pacemakers, smart glucometers and activity trackers) combined with remote monitoring and telemedicine services will allow patients to receive care and maintain their health with minimal disruption to their daily activities. While the implementation of these cyber-physical systems can greatly benefit society, the safety and privacy of each patient must be guaranteed. (Brogan et al., 2018)

To achieve the vision of an increasingly distributed healthcare system, the usage of CoS and algorithmic processing of large volumes of data will train models that continuously monitor healthcare metrics and report or act on abnormalities in real time. The ongoing development of effective models and algorithms is critical to improving healthcare and should be an open and

controlled process within the medical community. As these shared models and algorithms improve over time, devices can wirelessly send and receive updates in a federated manner (Brogan et al., 2018).

2.5. The blockchain-enabled cloud of sensors

Achieving privacy and security in a wireless sensor network (WSN) or IoT takes extensive resources, but mismanaged and compromised healthcare information can 'hurt' the patient and the future prospects of mobile healthcare applications (Sahi et al., 2017). These threats emerge as healthcare organizations that use the technology may not have the expertise to adequately secure the patient data (Kotz et al., 2016). In addition, devices can be lost or connected to an unencrypted network can result in malware or other malicious attacks (Vithanwattana et al., 2016). Wearable technology is another technology that has healthcare applications with potential security implications. Specific privacy concerns arise from wearable technology in the form of health information sensitivity and legislative protection (Li et al., 2016). Sensors, devices, and smart technology have privacy concerns in the form of information disclosure, withholding information or services, modification of information, repudiation, non-auditability, and loss of authenticity/validity (Theoharidou et al., 2017).

A Wireless Body Area Network (WBAN) deployment can include wearable body sensors (Al-Janabi et al., 2017; Mohan and Singh, 2016), and related security threats include data integrity, data freshness, availability of the network, data authentication, secure management, dependability, secure localization, accountability, and flexibility (Al-Janabi et al., 2017; Mohan and Singh, 2016). Devices in a WBAN are also likely to be resource constrained (Zhang et al., 2016), and hence lightweight security solutions will be required.

Additional problems associated with wearable health technology are that the data can be corrupted, the device may break down or malfunctions, and the user themselves can tamper with the data for a benefit (Siddiqi et al., 2017). A successful compromise of critical devices such as implanted medical devices used to administer life-saving drugs such as insulin can result in serious or fatal health risks (Al-Muhtadi et al., 2017). Before healthcare applications and wireless

healthcare can seriously be considered in a large-scale applications, these security concerns and health risks associated with health related attacks need to be addressed (Al-Muhtadi et al., 2017).

In several IoT applications, a lot of data is exchanged between objects and with other entities. Among them, the data freshness is one of the most relevant in a distributed system based on sensing data, such as the CoS (Bouzeghoub, 2004). This importance increases particularly in the context of systems composed of a set of autonomous data sources, where the data integration with different freshness values can lead to semantic problems, hindering the execution of applications. There are several definitions of data freshness in literature (Bouzeghoub, 2004). Among these definitions stands out the one that quantifies the freshness of a given data based on the time elapsed since its acquisition.

For that, it's very important to deal with this data and propose security solutions to share it with others. Moreover, privacy is a great issue that should be considered while addressing sharing data problems in IoT. According to Conoscenti (et al, 2016), to ensure privacy in IoT systems, it is recommended to use peer-to-peer architecture, and specifically blockchain technology. In addition, as all the operations handled on IoT data are controlled by the blockchain, it is easy to detect any abuse in data (Conoscenti et al, 2016) . Blockchain might serve as a tool to deal with all these aspects. In this trend, several works have been proposed.

The problem related to security at Wireless Sensor Network continue to arise in the context of IoT with the IP protocol being the main standard for connectivity (Khan and Salah, 2018). The deployment architecture therefore needs to be secured from attacks which may hinder the services provided by IoT as well as may pose threat to privacy, integrity or confidentiality of data, with that characteristics are from blockchain. Since the IoT characteristics represents a collection of interconnected networks, and heterogeneous devices, it inherits the conventional security issues related to the computer networks. The constrained resources pose further challenges to IoT security since the small devices or things containing sensors have limited power and memory. Consequently, the security solutions need to be adapted to the constrained architectures.

Patients are also more willing to take more proactive approaches to personalizing their healthcare (Zhang et al., 2017). This personalization of healthcare and treatment can come in the form of smart devices and smart sensors that record and send vital health data to their doctor to remotely view and assess chronic conditions (Zhang et al., 2017). Examples of these IOT technologies that apply to healthcare and empower patients to make more informed decisions about

their health are smart watches, contact lenses, fitness bands, microchips under the skin, and wireless sensors (Torre et al., 2016). These wireless systems sometimes do not put as much thought into security as other more sensitive systems such as databases, databanks, and IoT systems have a variety of vulnerabilities and attacks that can compromise Security. Attacks against wireless IoT systems can be categorized as active and passive attacks (Al Ameen et al., 2012). A passive attack is categorized as occurring when the data packets are routed through the system and an attacker can change the destination of packets or interfere with the routing protocols (Al Ameen et al., 2012). In addition, an attacker can eavesdrop or "sniff" the packets (intercept the packets as they travel through the network or wireless area) to uncover the data contained within (Al Ameen et al., 2012). Active attacks are when an attacker uses a vulnerability of a device or network to actively find, steal, modify, or obtain information about the user of the device or network (Al Ameen et al., 2012). Some of the attacks a malicious actor can use to obtain medical information from IoT devices are: data modification, impersonation attack, eavesdropping, and replaying, which all have the goal of obtaining private information from the victim (Al Ameen et al., 2012). Specific security vulnerabilities that attackers can exploit are general system security, administrator security, physical security, and information security (Al Ameen et al., 2012).

The three-tier CoS architecture characteristic, using the sensor tier (ST) to collect information and using the edge of the enterprise network, fog computing provides comparatively better performance in terms of reduced delay, store information, has lower latency and jitter, combined with blockchain technology, is a considerable opportunity to reduce the security issues for healthcare.

3. Research Methodology

The research methodology of this dissertation was crafted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyzes (PRISMA) that has gained the notoriety and importance since 2005, after an meeting in Canada and since them, it was incorporated in SLR methodology workflow. The method consisted in collecting articles, that is considered "data", that were used for systematic literature review (SLR) and bibliometric study that based the paper.

The search for the paper was conducted using two search engines: Scopus and ISI Web of Science. Elsevier's Scopus is the largest database of peer-reviewed literature and recovers journals from all major databases such as Science Direct, Emerald, PubMed, Taylor & Francis, among others. According to Chadegani et al., 2013, Scopus database is the largest searchable citation and abstract source. ISI Web of Science (WoS) from Thomson Reuters was the only citation database and publication that covers all domains of science for many years (Chadegani et al., 2013). The advantage of one database over another one depends on what explicitly will be analyzed, the scientific field and period of analysis (Chadegani et al., 2013). WoS is the oldest citation database, therefore it has strong coverage with citation data and bibliographic data going back to 1900 (Boyle and Sherman, 2006). Study of Vieira and Gomes (2009) reveals that 2/3 of the studies can be found in both databases and 1/3 only in one database. Another considerable advantage is that both databases provide ".bib" files providing full search data (such as references, article authors, etc.) that can be further analyzed in bibliometric packages. Nevertheless, even conducting the research in both databases it would not be possible to guarantee that all relevant literature was covered and so, it can be considered a limitation.

During the research period, three types of software were used. The first software was Mendeley®, which is mainly a software that organizes all references, making it easier to remove duplicates and cite papers, as it automatically generates references in the desired format. The second software used was RStudio® , which is a statistical and graphical tool for data science, converting the ".bib" output format from search database into bibliometric and graphical analysis. The third software used was MS Excel®, which is a spreadsheet to organize and generate tables.

3.1 Definition of Research Questions

After defining the scientific databases where to perform the search for articles, the next process step in the systematic mapping study, was defining some research questions based on our objectives which is to unravel the state-of-the-art in research on the application of blockchain technology in healthcare and its impact using the sensor network environment.

Question 1 - How bibliometric indicators behave in the literature regarding Blockchain, Clouds of sensors and Healthcare?

Question 2 - Which and how works propose the application of blockchain and Cloud of Sensors, in healthcare?

Question 3 - What are the existing research challenges regarding the blockchain-enabled cloud of sensors in healthcare?

3.2 Conducting the Research

The research methodology was conducted using Preferred Reporting Items for Systematic Reviews and Meta-Analyzes (PRISMA) method that came up with Moher et al. (2009). This research protocol has gained the notoriety after its developed in June, 2005 when it was presented in Ottawa, Canada, with 29 participants including review authors, methodologists and other professionals (Moher et al. 2009). The initial search was conducted using paper and articles Scopus and ISI WoS databases. The search string was defined an applied thru those databases and a “bib” output files was generated and downloaded. Those files were adjusted to avoid uncompleted information using Mendeley™ reference manager software, and were imported to R software to be analyzed and created a unique single file that was consolidated with duplicates information removed. The R™ software was used to created important analyzes but some items were necessary to de classified, to be sorted, to be counted, the MS Excel spreadsheet was used to generated more information.

The search term used was (("**Blockchain**" OR "**Smart Contract**" OR "**Ledger**") AND ("**Cloud***" OR "**Fog**" OR "**Edge**" OR "**Sensor**" OR "**Internet of ***") AND ("***health***"

OR "***medica**l" OR "**Hospital**" OR "**Pharmacy**" OR "**Clinic***")) in the article title, keywords and abstract. The usage of those words tried to cover the research target, but as a limitation, can be cited the fact that were refined including reviewed international journal articles and reviews (published in the English language), excluding book chapters, conference papers, master and doctoral dissertations, unpublished articles, textbooks, and notes. The initial search was conducted in March 27, 2022, and due an uncompleted year, all 2022 data's was not considered into this SLR and they were removed from initial search string, as are shown below.

```
TITLE-ABS-KEY ( ( "Blockchain" OR "Smart Contract" OR "Ledger" ) AND ( "Cloud*" OR "Fog"
OR "Edge" OR "Sensor" OR "Internet of *" ) AND ( "*health*" OR "*medical" OR "Hospital" OR "Pharmacy"
OR "Clinic*" ) ) AND ( LIMIT-TO ( DOCTYPE , "ar" ) OR LIMIT-TO ( DOCTYPE , "re" ) ) AND ( LIMIT-
TO ( LANGUAGE , "English" ) ) AND ( EXCLUDE ( PUBYEAR , 2022 ) )
```

Figure 6. Scopus database string search (By author)

The total search result into 577 articles and they were saved into ".bib" file (scopus_577_27.03.2022_all_fields.bib). Below the string search used in ISI Web of Science database with 594 articles resulted and saved into "bib" file (savedrecs_WoS_594_27.03.2022.bib)

```
TS=(("Blockchain" OR "Smart Contract" OR "Ledger") AND ("Cloud*" OR "Fog" OR "Edge" OR "Thing*"
OR "Sensor" OR "Internet of *") AND ("*health*" OR "*medical" OR "Hospital" OR "Pharmacy" OR "Clinic*"))
and Review Articles or Articles (Document Types) and English (Languages) and 2022 (Exclude – Publication Years)
```

Figure 7. ISI Web of Science database string search (By author)

All search results were saved into a ".bib" file with all information related. Among the papers found in this research, there was a list of most cited papers separated by Scopus and WoS databases. The Table 1 presented the top 10 most cited papers by initial research.

Paper	Citations Scopus	Citations WoS
XIA Q, 2017, IEEE ACCESS	483	360
CHAMOLA V, 2020, IEEE ACCESS	380	244
ESPOSITO C, 2018, IEEE CLOUD COMPUT	352	245
DWIVEDI AD, 2019, SENSORS	308	217
GRIGGS KN, 2018, J MED SYST	299	202

WANG S, 2019, IEEE TRANS SYST MAN CYBERN SYST	254	190
XIONG Z, 2018, IEEE COMMUN MAG	251	213
XIA Q, 2017, INFORMATION	247	182
BANERJEE M, 2018, DIGIT COMMUN NETW	237	157
KOUICEM DE, 2018, COMPUT NETWORKS	230	171

Table 1. Most cited paper after initial search. (by author)

Those " .bib" output files were used to generate the articles reference list information into Mendeley® software. After importing the all " .bib" data into a single directory in Mendeley® software, there were a total of 1171 total listed. Applied a Check for Duplicates tool available at Mendeley software, the number of articles was reduced by 731 total articles. The same list of ".bib" files were used by RStudio® statistical software and graphical tools for removing duplicate articles and to merge into one spreadsheet list of articles as described below.

```
--------- Merger 2 Bases --------
S <- convert2df("scopus_577_27.03.2022_all_fields.bib",dbsource = "scopus", format =
"bibtex")
W <- convert2df("savedrecs_WoS_594_27.03.2022.bib",dbsource = "isi", format =
"bibtex")
Database=mergeDbSources(S, W, remove.duplicated = TRUE)
View(Database)

----------- Save Excel --------
dim(Database)
library(openxlsx)
write.xlsx(Database, file = "Database_All_Artigo_731.xlsx")
```

Figure 8. Remove duplicate articles and create a excel file on **RStudio®** (By author)

Following the PRISMA methodology, once duplicated records were removed, the beginning of screening the relevant papers phase needed to start. All non-duplicated papers were imported into a reference management software (Mendeley®) and synchronized to collect the title and abstract information of those imported papers. Few of them had to be downloaded from the paper´s website.

During the screening of paper titles, 489 articles were discarded because they were not related to the blockchain, or related to the healthcare or medical industry, or sensor related. The remaining publications were inspected more detailed by full read paper revision to analyze if the paper meets the relevance criteria. All of 242 remaining papers were tried to be fully downloaded and classified but 40 of them were not available to be accessed. The rest of 202 papers were fully

downloaded, read and selected by this SLR relevance, all paper must have all three concepts together presented above, blockchain, health or medical and sensor information. As the result a list of related publication themes that had 118 articles to be analyzed for Systematic Literature review.

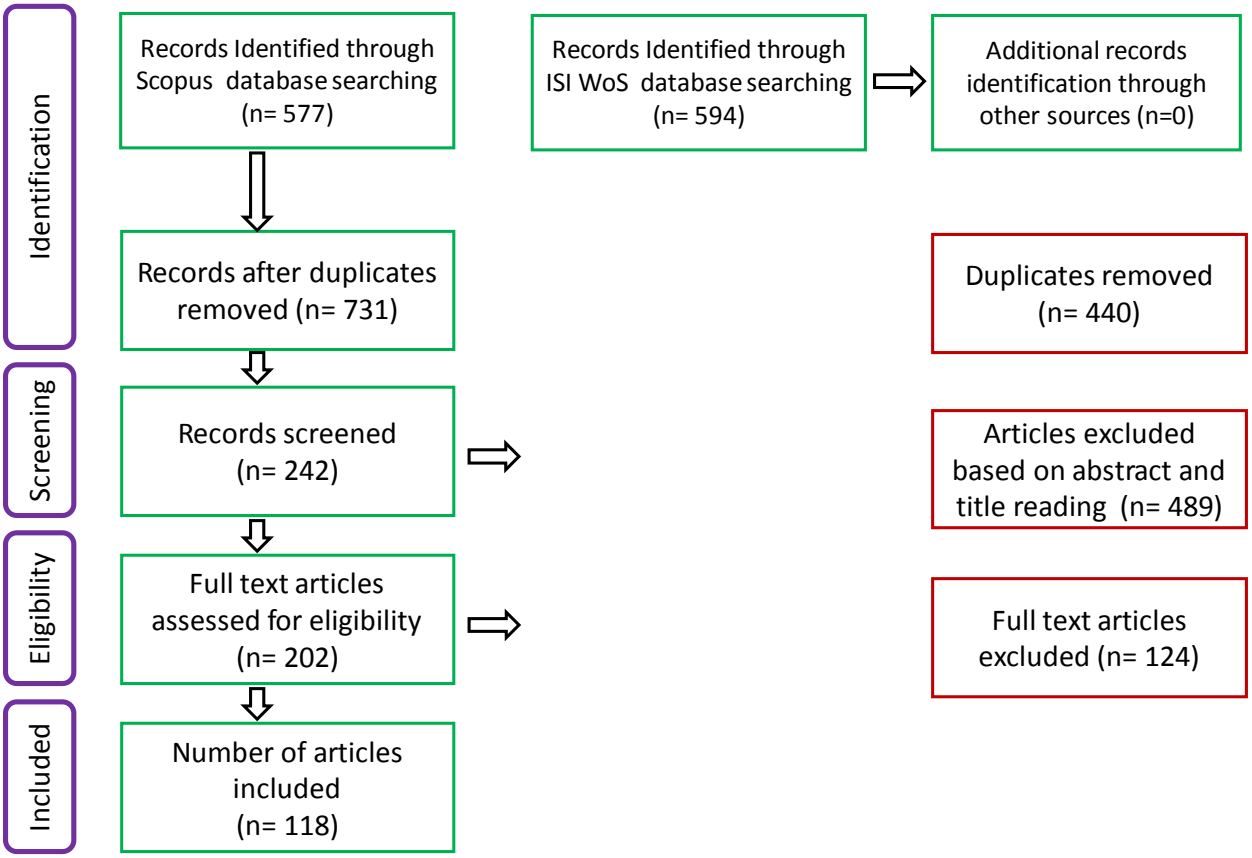


Figure 9: Research flow diagram (By Author)

4 Results of Systematic Literature Review

4.1 Classify papers

This section presents the classification of articles in different areas of research. As a single article can be classified in many research segments, the absolute number of papers is not equivalent to the sum of the articles. Figure 10 shows the classification of articles by research area.

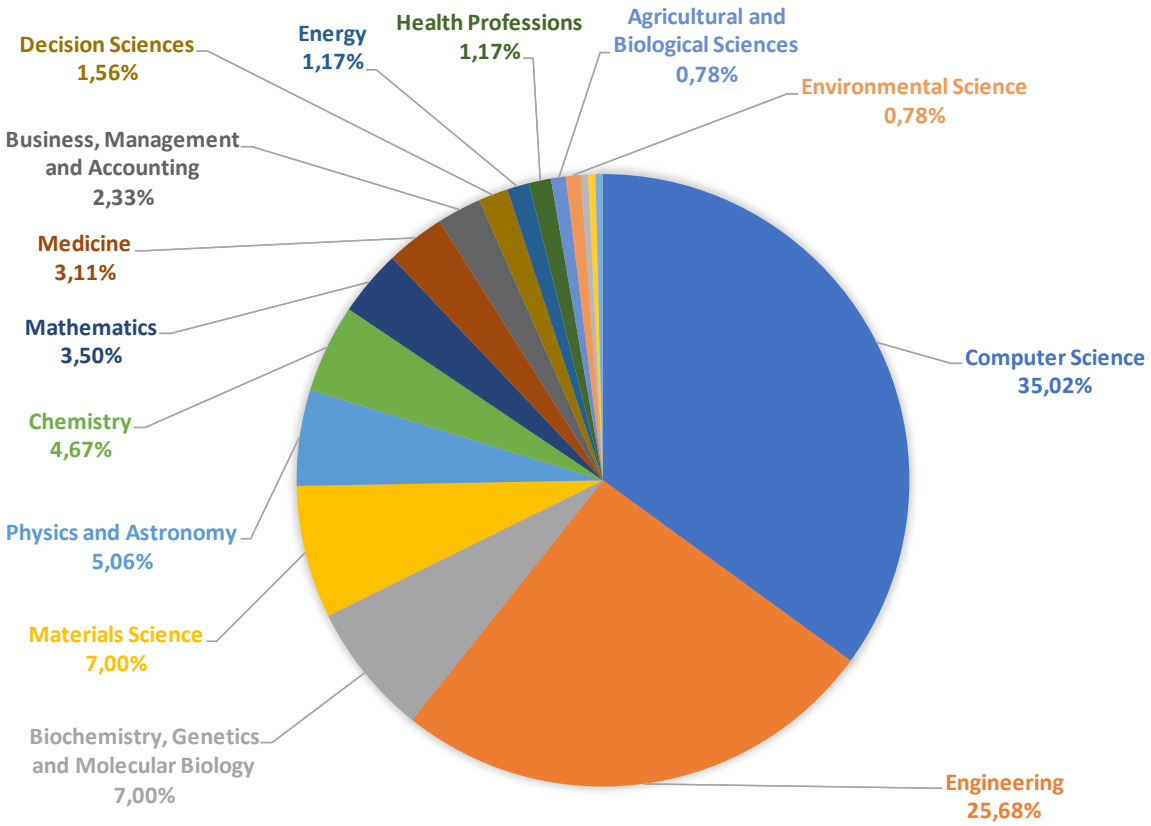


Figure 10. Paper classification by segment area (By author)

Among the applied papers the distribution by segment summarized by Table 2. It is noted that paper classification for Computer Science and Engineering and sectors are outstanding with 35,02% and 25,68% outcomes respectively.

Category	Quantity
Computer Science	90
Engineering	66
Biochemistry, Genetics and Molecular Biology	18
Materials Science	18
Physics and Astronomy	13
Chemistry	12
Mathematics	9
Medicine	8
Business, Management and Accounting	6
Decision Sciences	4
Energy	3
Health Professions	3
Agricultural and Biological Sciences	2
Environmental Science	2
Immunology and Microbiology	1
Chemical Engineering	1
Social Sciences	1

Table 2. Segment distribution (absolute numbers)

Concerning Table above, it is important to highlight a paper that could be classified in more than one category. The case of blockchain and sensor publications, they can be classified into the first 2 (two) most published segments (Engineering and Computer Science). Although there is not a segment described as Healthcare the Biochemistry, Genetics, Medicine, and Health Profession,

are most related thru healthcare sector, and if we could create a separated category together, they appear with 11,67% studies classified among these categories. This number of articles may represent a great demand or ease in publications in science and technology journals instead of medical journals. The table below shows the list of papers with healthcare characteristics.

Authors	Area	Approach
Zheng, X. et al.(2019)	Patient Tractability	Data Sharing
Griggs, K. N. K. N. et al.(2018)	Patient Monitoring	Body Sensor
Shahbazi, Z. & Byun, Y.-C. Y. C.(2020)	Patient Monitoring	Thermal Energy
Jamil, F. et al.(2020)	Patient Monitoring	Data Sharing
Satamraju, K. P. & Malarkodi, B.(2020)	Patient Monitoring	Healthcare 4.0
Chen, X. et al.(2020)	Patient Monitoring	Data Sharing
Fernández-Caramés, T. M. et al.(2019)	Patient Monitoring	IoMT
Bublitz, F. M. et al.(2019)	Patient Monitoring	AI
Ren, Y. et al.(2019)	Patient Monitoring	Security
Liu, X. et al.(2020)	Patient Monitoring	CHD
Dwivedi, A. D. A. D., et al.(2019)	Patient Monitoring	Body Sensor
Ali, M. S. M. S.et al.(2020)	Patient Monitoring	Torrent
Singh, R. et al.(2020)	Medical Transportation	Temperature Monitoring
Celesti, A. et al.(2020)	Healthcare	Tele-Medical
Tripathi, G. et al.(2020)	Healthcare	Security
Liang, X. et al.(2018)	Blockchain	Data Sharing

Table 3. Papers listed by health characteristics classification (by author).

4.2 Analyze papers

This section shows the results of all 118 papers extracted from the final full text read result. The table 4 list all related papers used to final SLR results.

#	Year	Author	Publisher
1		Wang, J. et al.	Future Generation Computer Systems
2	2019	Islam, N. et al.	Future Generation Computer Systems
3	2020	Islam, A. & Young Shin, S.	Computers and Electrical Engineering
4	2019	Syed, T. A. et al.	IEEE Access
5	2020	Ali, M. S. M. S.et al.	Sensors (Switzerland)
6	2019	Dwivedi, A. D. A. D., et al.	Sensors (Switzerland)
7	2020	Aujla, G. S. & Jindal, A.	IEEE Journal on Selected Areas in Communications
8	2019	Silva, C.-C. A. et al.	Wireless Communications and Mobile Computing
9	2020	Rathee, G. et al.	Multimedia Tools and Applications
10	2020	Tahir, M. et al.	International Journal of Distributed Sensor Networks
11	2020	Guo, R. et al.	International Journal of Distributed Sensor Networks
12	2020	Kumar, A. et al.	IEEE Access
13	2019	Padmavathi, U. & Rajagopalan, N.	International Journal of Innovative Technology and Exploring Engineering
14	2020	De Aguiar, E. et al.	ACM Computing Surveys
15	2019	Zheng, X. et al.	Journal of Medical Internet Research
16	2020	Hathaliya, J. J. & Tanwar, S.	Computer Communications
17	2020	Sharma, A. et al.	Electronics (Switzerland)
18	2020	Mistry, I. et al.	Mechanical Systems and Signal Processing
19	2019	Nguyen, D. C. et al.	IEEE Access
20	2020	Farouk, A. et al.	Computer Communications
21	2018	Rifi, N. et al.	Wireless Communications and Mobile Computing
22	2019	Dilawar, N. et al.	International Journal of Advanced Computer Science and Applications
23	2020	Celesti, A. et al.	Sensors (Switzerland)
24	2018	Rahman, M. A. et al.	IEEE Access
25	2020	Liu, X. et al.	IEEE Journal of Biomedical and Health Informatics
26	2018	Uddin, M. A. et al.	IEEE Access
27	2020	Yanez, W. et al.	IEEE Internet of Things Journal
28	2019	Ren, Y. et al.	SENSORS
29	2019	Bublitz, F. M. et al.	International Journal of Environmental Research and Public Health
30	2020	Abou-Nassar, E. M. et al.	IEEE Access
31	2019	Iqbal, J. et al.	International Journal of Distributed Sensor Networks
32	2019	Fernández-Caramés, T. M. et al.	Sensors (Switzerland)
33	2018	Griggs, K. N. K. N. et al.	Journal of Medical Systems
34	2019	Xu, J. et al.	IEEE Internet of Things Journal
35	2020	Girardi, F. et al.	Electronics (Switzerland)
36	2020	Maitra, S. et al.	Transactions on Emerging Telecommunications Technologies
37	2020	Singh, R. et al.	Sensors (Switzerland)
38	2020	Biswas, S. et al.	IEEE Transactions on Engineering Management
39	2019	Divya Preetha, A. & Pradeep Kumar, T. S.	International Journal of Recent Technology and Engineering

40	2020	Yuan, X. et al.	TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES
41	2020	Chen, X. et al.	Journal of Healthcare Engineering
42	2020	Tuli, S. et al.	INTERNET Technology Letters
43	2019	Lin, D. et al.	IEEE Access
44	2020	Satamraju, K. P. & Malarkodi, B.	Sensors (Switzerland)
45	2020	Shan, Y. & Mai, Y.	Eurasip Journal on Wireless Communications and Networking
46	2020	Tripathi, G. et al.	Healthcare
47	2020	Tripathi, G. et al.	Electronics (Switzerland)
48	2020	Sousa, P. R. et al.	Journal of Enterprise Information Management
49	2020	Qadri, Y. A. et al.	IEEE Communications Surveys and Tutorials
50	2020	Qadri, Y. A. et al.	Cluster Computing
51	2020	Jamil, F. et al.	Sensors (Switzerland)
52	2020	Shahbazi, Z. & Byun, Y.-C. Y. C.	Sensors (Switzerland)
53	2018	Liang, X. et al.	EAI Endorsed Transactions on Pervasive Health and Technology
54	2019	Mohanta, B. K. et al.	International Journal of Scientific and Technology Research
55	2021	Islam, A et. al.	IEEE Wireless Communications
56	2021	Lee, T.-F. et. al.	International Journal of Information Security
57	2021	Chen, Z	Future Generation Computer Systems
58	2021	Taralunga, D & Florea, B	Sensors
59	2021	Rahman, Z et. al.	IEEE Sensors Journal
60	2021	Aujla, G & Jindal, A,	IEEE Journal on Selected Areas in Communications
61	2021	Muhammad, G & Hossain, M	IEEE Network
62	2021	Fang, L et. al.	IEEE Internet of Things Journal
63	2021	Mohan, D et. al.	Journal of Reliable Intelligent Environments
64	2020	Bigini, G et. al.	Future Internet
65	2021	Jeong, S et. al.	Wireless Communications and Mobile Computing
66	2021	Sadawi, A et. al.	IEEE Access
67	2021	Ratta, P et. al.	Journal of Food Quality
68	2021	Hossein M et. al.	Computer Communications
69	2021	Ray, P et. al.	IEEE Internet of Things Journal
70	2020	Indumathi, J. et. al.	IEEE Access
71	2021	Mehbodniya, A et. al.	Computational and Mathematical Methods in Medicine
72	2021	Wang, W et. al.	IEEE Internet of Things Journal
73	2021	Gao, Y et. al.	IEEE Internet of Things Journal
74	2021	Wang, S et. al.	IEEE Internet of Things Journal
75	2021	Ray, P et. al.	IEEE Systems Journal
76	2021	Akkaoui, R	IEEE Transactions on Engineering Management
77	2020	Uddin, Md et. al.	Internet of Things (Netherlands)
78	2021	ElRahman, S A & Alluhaidan, A S	Soft Computing
79	2021	Srinivasu, P et. al.	Electronics (Switzerland)
80	2021	Almagrabi, A et. al.	Computers, Materials and Continua

81	2021	Wang, W et. al.	Journal of Systems Architecture
82	2021	Abbas, A et. al.	Personal and Ubiquitous Computing
83	2021	Chen, F et. al.	Security and Communication Networks
84	2021	Wu, J et. al.	IEEE Internet of Things Journal
85	2021	Shynu, P et. al.	IEEE Access
86	2021	Ngabo, D et. al.	Electronics (Switzerland)
87	2021	Lydia L et. al.	Soft Computing
88	2021	Lakhan, A et. al.	Mathematical Biosciences and Engineering
89	2021	Elsayeh, M et. al.	Biomedical Engineering - Applications, Basis and Communications
90	2020	Son, S et. al.	IEEE Access
91	2021	Sharmila, A H & Jaisankar, N	Computer Networks
92	2021	Christo, M et. al.	Security and Communication Networks
93	2021	Mayer, A et. al.	IEEE Access
94	2021	Egala, B S et. al.	IEEE Internet of Things Journal
95	2020	Al-Jaroodi, J et. al.	IEEE Access
96	2021	Shukla, S et. al.	Internet of Things (Netherlands)
97	2021	Hameed, K et. al.	Journal of Healthcare Engineering
98	2021	Xie, Yi et. al.	Current Medical Science
99	2020	Nguyen, D et. al.	IEEE Communications Surveys and Tutorials
100	2021	Elhoseny, M et. al.	Energies
101	2021	Arul, R et. al.	Personal and Ubiquitous Computing
102	2021	Abdellatif, A et. al.	IEEE Internet of Things Journal
103	2021	Arul, R et. al.	Personal and Ubiquitous Computing
104	2020	Tomaz, Aet. al.	IEEE Access
105	2021	Otoum, S et. al.	IEEE Network
106	2021	Alsahli, M et. al.	IEEE Access
107	2021	Lin, H et. al.	IEEE Internet of Things Journal
108	2021	Bera, B et. al.	IEEE Consumer Electronics Magazine
109	2021	Krishnamoorthy, S et. al.	Journal of Ambient Intelligence and Humanized Computing
110	2021	Rini, P. L.	Advances in Parallel Computing
111	2020	Rahman, M A et. al.	IEEE Access
112	2021	Nguyen, G et. al.	Journal of Parallel and Distributed Computing
113	2021	Wang, Y et. al.	IEEE Internet of Things Journal
114	2021	Aggarwal, S et. al.	Sensors
115	2021	Barka, E et. al.	Electronics (Switzerland)
116	2021	Al-Khazaali, A et. al.	Applied Nanoscience (Switzerland)
117	2021	Kumar, R & Tripathi, R	Journal of Supercomputing
118	2021	Santos, J A et. al.	Journal of Medical Systems

Table 4. All related papers used to final SLR results (by author).

Even though the search has no initial time period, those publications were very new, starting in 2018 and are increasing year by year. The published papers are increasing, showing in

Figure 11 as 320% (16 papers) in 2019, increased 256,25% (41 papers) from 2020 and 136,59% (56 papers) in 2021. The figure below represents the research of blockchain into healthcare area using sensor are new and it is growing rapidly as the number of publications from 2018 to 2021 in 1120%

.

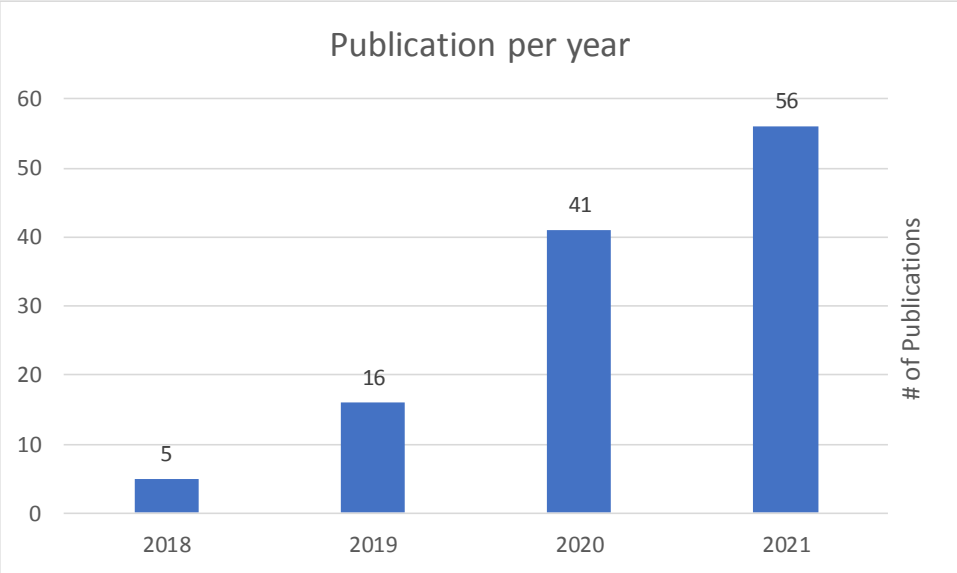


Figure 11. Research selection by year of publication (By Author)

4.3 Results and research gaps

The below section shows all numerical results found in the bibliometric analysis. The first graph shown by Figure 12 shows all publishing countries for this research literature, as the darkness color represents more articles published. China is the country leader with 35 papers published, representing 25,00% of total published countries, followed by India and South Korea with 18 and 15 papers respectively, representing 12,86% and 10,71% of published countries.

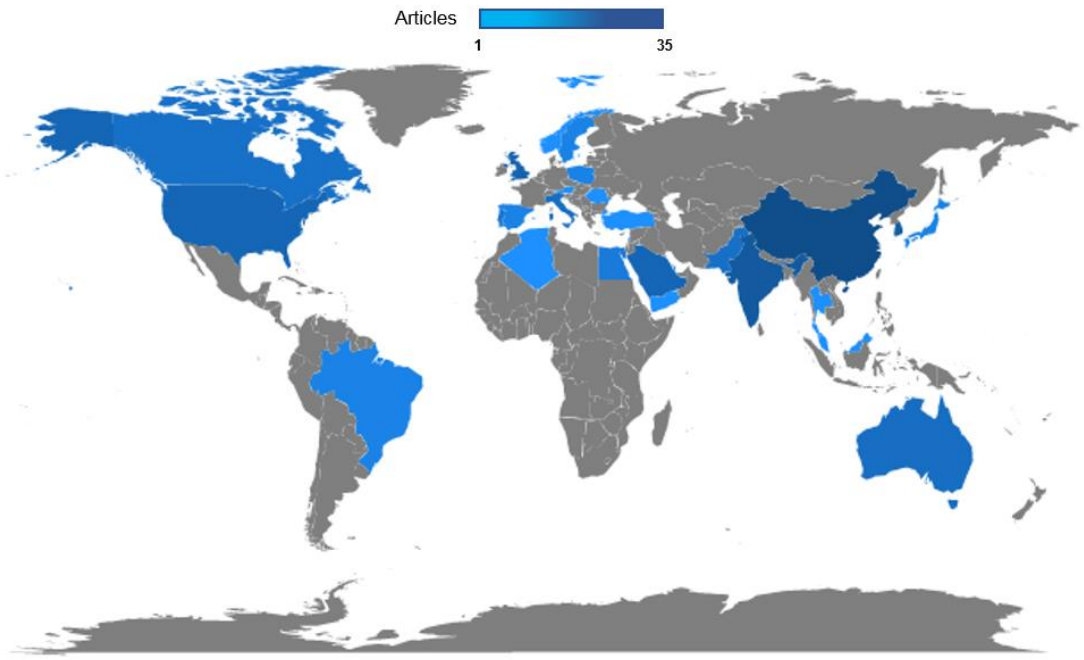


Figure 12. All publishing countries. (by author)

The table below shows the absolute total numerical results found in the bibliometric analysis segmented by country of publication.

Region	Frequency
CHINA	35
INDIA	18
SOUTH KOREA	15
UK	11
SAUDI ARABIA	9
USA	9
AUSTRALIA	6
ITALY	6
CANADA	5
PAKISTAN	5
PORTUGAL	4
EGYPT	3
BRAZIL	2

JAPAN	2
POLAND	2
QATAR	2
SPAIN	2
SWEDEN	2
ALGERIA	1

Table 5. List of total publishing by countries.

Although China is the country leader in publishing, it has 56 articles cited in bibliometric analysis stain in fourth place of citations countries. India and Korea, which were the top 3 publishing countries, are represented and have several articles cited, according to Table 5 and the outcome country is Thailand which is shown at Figure 12.

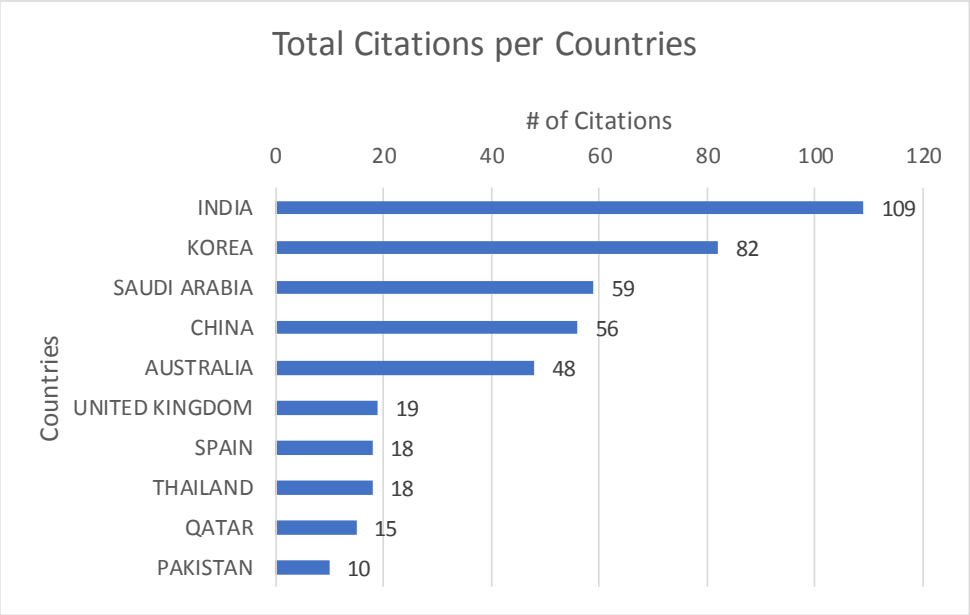


Figure 13. Total Citations per country.

During the 2018 year five articles were published according to the SLR and there are 4 of them in the top 10 most cited papers. Figure 14 lists the most cited documents during the SLR referring that the most cited article is HEALTHCARE BLOCKCHAIN SYSTEM USING SMART CONTRACTS FOR SECURE AUTOMATED REMOTE PATIENT MONITORING follow by A DECENTRALIZED PRIVACY PRESERVING HEALTHCARE BLOCKCHAIN

FOR IOT all of them with outstanding more than 100 citations. Those papers were at the initial top 10 most cited paper research listed at Table 1

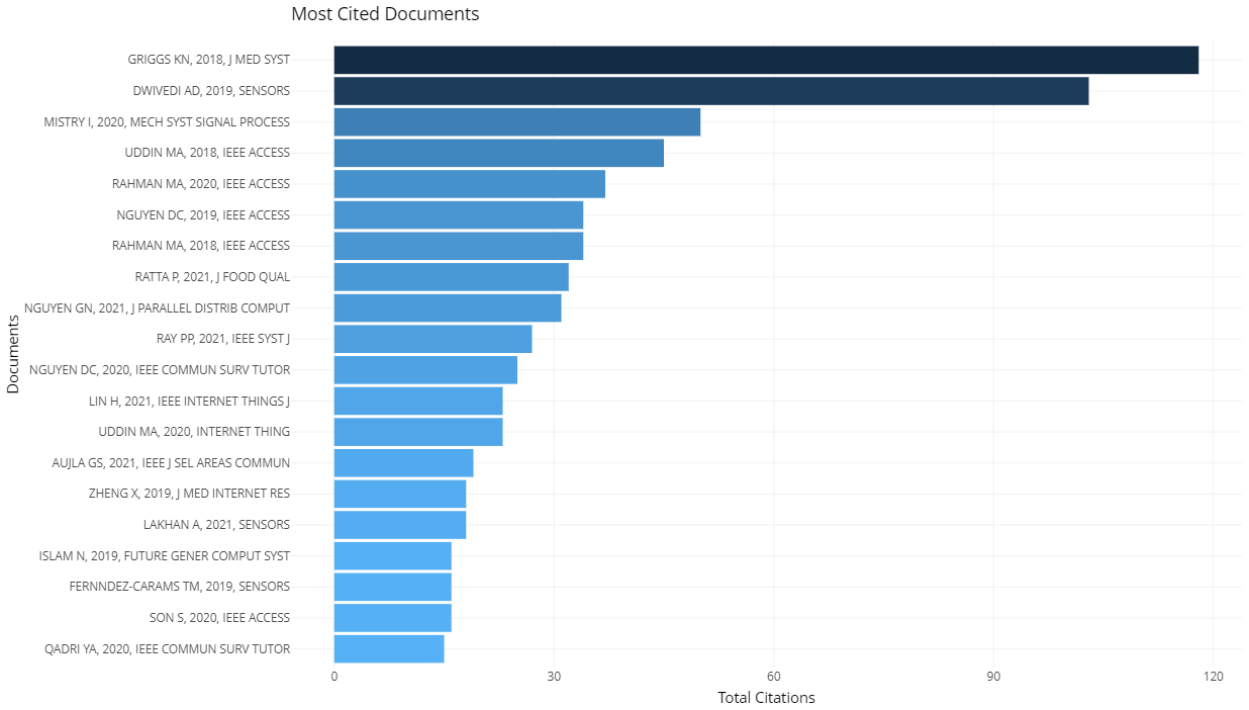


Figure 14. Most Cited Documents

The following figure, called word cloud, represents a quantity of words among the Title, the Abstract and the Author's key word of all SLR bibliometric results. Each size of the word represents the number of words found in the final paper list.

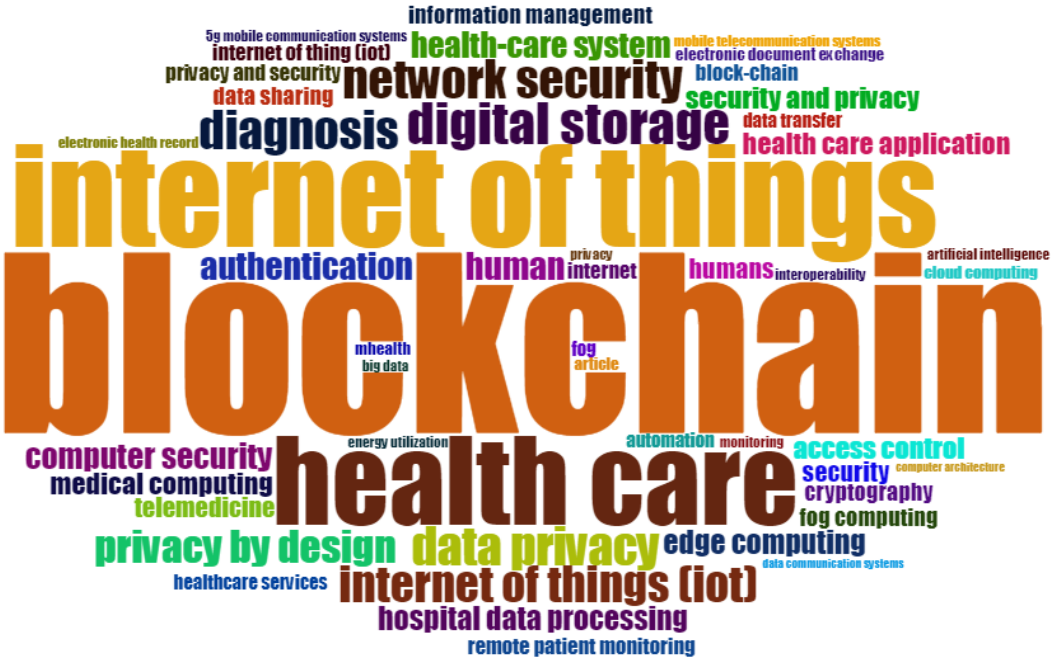


Figure 15. Most relevant word for Word Cloud (by author)

During the search and construction of word cloud, there were several words with the same meaning (Ex: health-care and healthcare) that were distinguished as different and the tool recognizes them as different words. To correct this information, some similar words were replaced by a unique word and the result was described into the Figure 16.

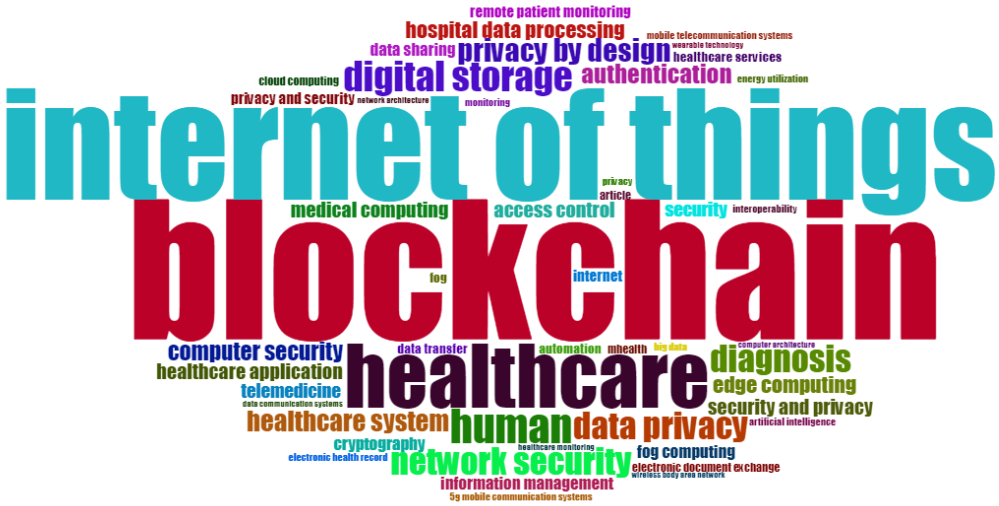


Figure 16. Most relevant word for Word Cloud replaced by unique word (by author)

The most frequent and relevant words represented in word cloud are: Blockchain with 107 appearances, Internet of Things with 85 appearances and Healthcare with 49, following this order of appearance. The Figure 17 is representing the top 10 most relevant words and those words were outstanding and most relevant.

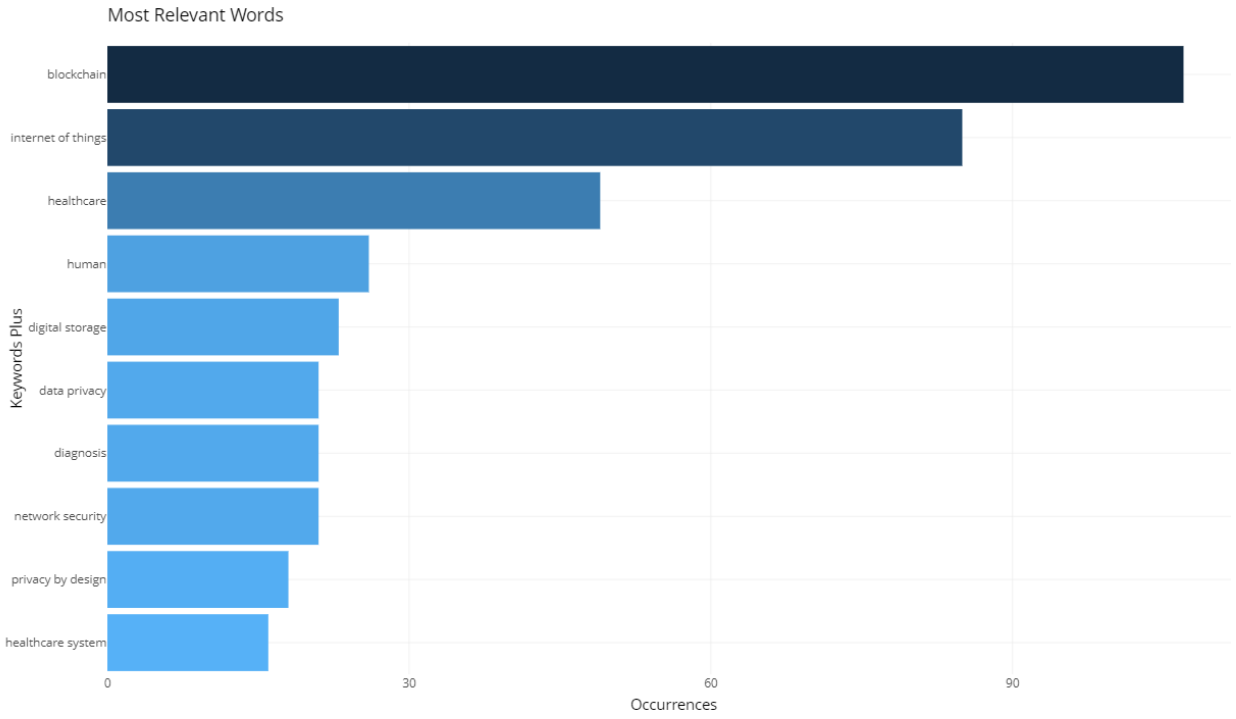


Figure 17. List of most cited word replaced by a unique word (By Author)

Another characteristic of theses 3 words was that the frequency of appearing has been increasing since 2018 as shown in Figure 18, on the other hand the word Data-Privacy frequency reduced along the 2021 year.

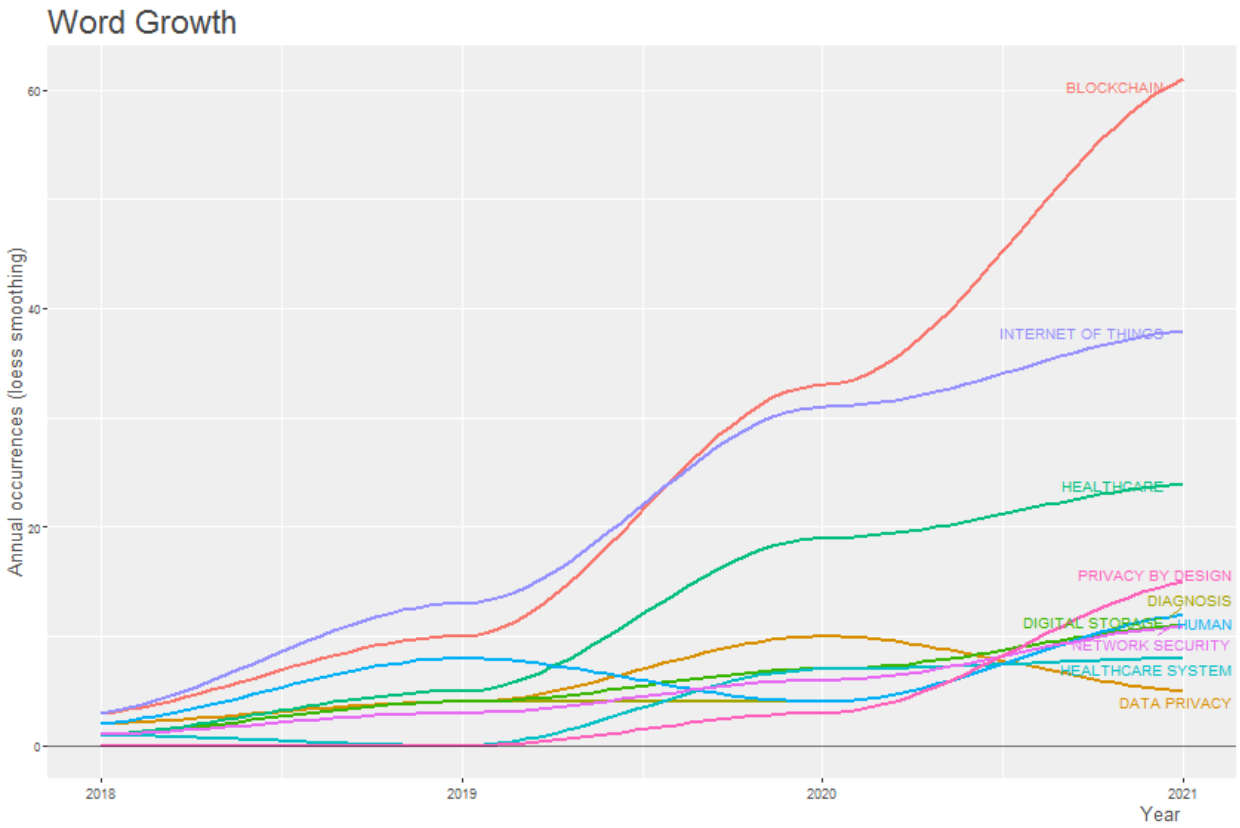


Figure 18. Word growth over year

Working with co-word analysis draws clusters of keywords, they are considered as themes, whose density and centrality can be used in classifying themes and mapping in a two-dimensional diagram. The thematic map is an intuitive plot information and it is possible to analyze those themes according to the quadrant in which they are placed: The upper-right quadrant: motor-themes; The lower-right quadrant: basic themes; The lower-left quadrant: emerging or disappearing themes; The upper-left quadrant: very specialized/niche themes. (Cobo M. et all, 2011), Below are the thematic map and relationship represented into two formats.

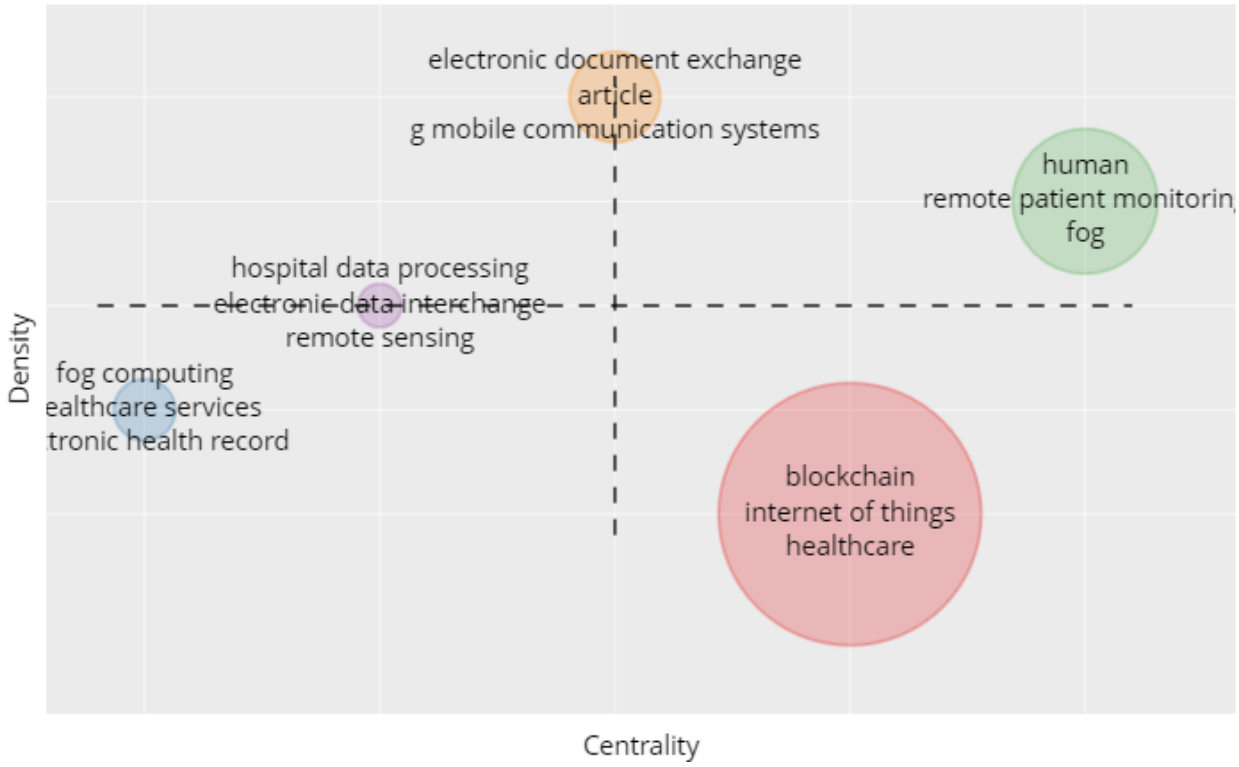


Figure 19. Thematic Word Map graph with five groups and three words (By Author)

The network thematic map and relationship are showing 5 groups where the blockchain, healthcare and IoT are the biggest ones and are considered basic themes. But other relational groups are to be considered such as fog (Motor and Emerging theme), Remote Patience Monitoring (motor theme) and Remote Sensing (niche theme). These words are related to Cloud of Sensor technology. In Figure 20 there are the representation of each group described above with the correlation and interconnection among those themes.

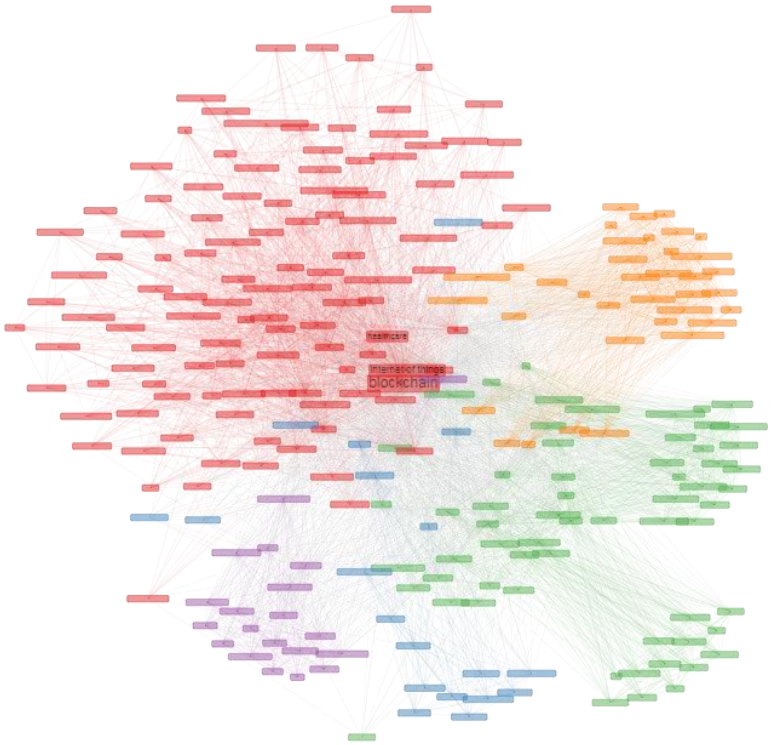


Figure 20. Thematic Word Map correlation groups (by author)

After the full text reading process, all of 118 articles were classified in Technology and focus area and usability scenario. They were also classified by type of technology among the characteristics of SLR, if they have references of Fog usability, what type of sensor are described into article, if it describe the usage of any CoS layers, what type of blockchains is described into the paper analyzed and; as IoT is the most cited type of sensor indicated into all research, there is an classification domain of usability into IoT and those articles were classified among those domains. The following table below are the summary of 118 articles.

Technology Area	Focus Area	Usability Scenarios	Fog Usage	Type of Sensor	CoS Layer Usability	Type of BC	Class Type	Year	Author
Wireless Body Area Network	Patient Monitoring	Body Sensor	No	BLE	L1 and L2	Private	RPM	2020	Wang, J. et al.
Remote Health Monitoring	Patient Monitoring	Body Sensor	Yes	IoT	L1, L2 and L3	Consortium	RPM	2019	Islam, N. et al.
Wireless Body Area Network	Patient Monitoring	Usage of Blockchain with UAV	No	Body Sensor Networks	L1 and L2	Private	RPM	2020	Islam, A. & Young Shin, S.
Blockchain IoT	Blockchain	Types of Blockchain	No	IoT	N/A	All	PHS	2019	Syed, T. A. et al.
Remote Health Monitoring	Patient Monitoring	Torrent	No	IoT	L1 and L2	Public	RPM	2020	Ali, M. S. M. S.et al.
Weareble Devices	Patient Monitoring	Body Sensor	No	IoT	L1	Public	RPM	2019	Dwivedi, A. D. A. D., et al.
Survey	Blockchain	Blockchain Comparation	No	IoT	L1, L2 and L3	Consortium	RPM	2020	Aujla, G. S. & Jindal, A.
Eletronic Medical Record	Medical Record Manag	Data Sharing	Yes	IoT	L1, L2 and L3	Private	PHS	2019	Silva, C.-C. A. et al.
Eletronic Medical Record	Patient Tractability	Data Processsing	No	IoT	L1, L2	Public	RPM	2020	Rathee, G. et al.
Eletronic Medical Record	Patient Monitoring	Security	Yes	IoT	L1, L2 and L3	Public	RPM	2020	Tahir, M. et al.
Wireless Body Area Network	Patient Monitoring	Security	Yes	IoT	L1, L2 and L3	Private	RPM	2020	Guo, R. et al.
Eletronic Medical Record	Healthcare	Healthcare 4.0	Yes	IoT	L1, L2 and L3	Public	PHS	2020	Kumar, A. et al.
Wireless Body Area Network	Blockchain	Healthcare 4.0	No	Wearable	N/A	All	AAL	2019	Padmavathi, U. & Rajagopalan, N.
Eletronic Medical Record	Blockchain	SWOT Analisys	No	Wearable	N/A	All	Survey	2020	De Aguiar, E. et al.
Eletronic Medical Record	Patient Tractability	Data Sharing	No	IoT	L1, L2 and L3	Public	RPM	2019	Zheng, X. et al.
Survey	Patient Tractability	Healthcare 4.0	No	IoT	L1, L2 and L3	All	RPM	2020	Hathaliya, J. J. & Tanwar, S.
Eletronic Medical Record	Smart Contract	Healthcare 4.0	No	IoT	L1	Consortium	AAL	2020	Sharma, A. et al.
5G IoT	Blockchain	Industrial Automation	No	IoT	L1	All	PHS	2020	Mistry, I. et al.
Eletronic Medical Record	Healthcare	Healthcare 4.0	No	IoT	L1, L2 and L3	All	AAL	2019	Nguyen, D. C. et al.
Blockchain Industrial IoT	Healthcare	Internet of Health Things	No	IoT	L1, L2 and L3	All	EM	2020	Farouk, A. et al.
Eletronic Medical Record	Patient Monitoring	Data Sharing	No	Wearable	L1 and L2	Consortium	RPM	2018	Rifi, N. et al.
Eletronic Medical Record	Blockchain	Security	No	IoT	L1	Private	RPM	2019	Dilawar, N. et al.
Eletronic Medical Record	Healthcare	Tele-Medical	No	IoT	L1, L2 and L3	All	AAL	2020	Celesti, A. et al.
Remote Health Monitoring	Patient Monitoring	Torrent	No	IoT	L1, L2 and L3	All	RPM	2018	Rahman, M. A. et al.
Remote Health Monitoring	Patient Monitoring	Coronary heart disease diagnosis (CHD)	No	IoT	L1 and L2	Private	RPM	2020	Liu, X. et al.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	No	IoT	L1, L2 and L3	All	RPM	2018	Uddin, M. A. et al.
Remote Health Monitoring	Patient Monitoring	Fuzzy-Logic	Yes	IoT	L1, L2 and L3	All	RPM	2020	Yanez, W. et al.

Wireless Body Area Network	Patient Monitoring	Security	No	IoT	L1 and L2	Private	RPM	2019	Ren, Y. et al.
Eletronic Medical Record	Patient Monitoring	Artificial Inteligence	Yes	IoT	L1, L2 and L3	All	EM	2019	Bublitz, F. M. et al.
Smart City	Healthcare	Internet of Health Things	No	Semantic Sensor Network	L1 and L2	Private	EM	2020	Abou-Nassar, E. M. et al.
Eletronic Medical Record	Patient Monitoring	Security	No	Body Sensor Networks	L1, L2 and L3	All	RPM	2019	Iqbal, J. et al.
Eletronic Medical Record	Patient Monitoring	Internet of Medical Things	Yes	Continuous Glucose Monitors (CGMs) sensor	L1, L2 and L3	Consortium	RPM	2019	Fernández-Caramés, T. M. et al.
Eletronic Medical Record	Patient Monitoring	Body Sensor	No	Body Sensor Networks	L1	Consortium	RPM	2018	Griggs, K. N. K. N. et al.
Eletronic Medical Record	Patient Monitoring	Data Sharing	No	IoT	L1	Consortium	RPM	2019	Xu, J. et al.
Eletronic Medical Record	Patient Monitoring	Internet of Medical Things	No	IoT	L1 and L2	All	RPM	2020	Girardi, F. et al.
Supply Chain	Medical Transportation	Healthcare 4.0	No	Low Energy	L1 and L2	Private	PHS	2020	Maitra, S. et al.
Supply Chain	Medical Transportation	Temperature Monitoring	No	Temperature Sensor	L1, L2 and L3	Public	PHS	2020	Singh, R. et al.
Eletronic Medical Record	Patient Tractability	Data Sharing	No	IoT	L1	Consortium	PHS	2020	Biswas, S. et al.
Remote Health Monitoring	Healthcare	Security	Yes	Beacons	L1 and L2	Consortium	RPM	2019	Divya Preetha, A. & Pradeep Kumar, T. S.
Wireless Body Area Network	Patient Monitoring	Automation	No	IoT	L1, L2 and L3	Private	RPM	2020	Yuan, X. et al.
Implantable medical devices (IMD)	Patient Monitoring	Data Sharing	Yes	RFID	L1, L2 and L3	Public	RPM	2020	Chen, X. et al.
Wireless Body Sensor Nodes (WBSNs)	Patient Monitoring	Healthcare 4.0	Yes	IoT	L1, L2 and L3	Private	RPM	2020	Tuli, S. et al.
5G	Patient Monitoring	Security	No	Mobile edge computing	L1, L2 and L3	Public	RPM	2019	Lin, D. et al.
Eletronic Medical Record	Patient Monitoring	Healthcare 4.0	No	IoT	L1	Consortium	RPM	2020	Satamraju, K. P. & Malarkodi, B.
Sport Fitness Management	Fitness Monitoring	Body Sensor	No	IoT	L1, L2 and L3	Private	RPM	2020	Shan, Y. & Mai, Y.
Eletronic Medical Record	Healthcare	Security	No	IoT	L1, L2 and L3	All	AAL	2020	Tripathi, G. et al.
Eletronic Medical Record	Smart Cities	Healthcare 4.0	No	IoT	L1, L2 and L3	Consortium	AAL	2020	Tripathi, G. et al.
Eletronic Medical Record	Blockchain	Identity Management	No	IoT	L1	Private	RPM	2020	Sousa, P. R. et al.
Healthcare IoT	Survey	Healthcare 4.0	Yes	IoT	L1, L2 and L3	All	Survey	2020	Qadri, Y. A. et al.
Healthcare IoT	Blockchain	Security	No	IoT	L1, L2 and L3	Consortium	AAL	2020	Qadri, Y. A. et al.
Eletronic Medical Record	Patient Monitoring	Data Sharing	No	IoT	L1	Consortium	RPM	2020	Jamil, F. et al.

Wireless Body Area Network	Patient Monitoring	Thermal Energy	No	Body Sensor Networks	L1	Private	RPM	2020	Shahbazi, Z. & Byun, Y.-C. Y. C.
Eletronic Medical Record	Blockchain	Data Sharing	No	Body Sensor Networks	L1 and L2	Consortium	AAL	2018	Liang, X. et al.
Eletronic Medical Record	Patient Monitoring	Security	No	IoT	L1	Private	RPM	2019	Mohanta, B. K. et al.
Artificial Intelligence	Patient Monitoring	Temperature Monitoring	Yes	IoDT (Drone)	L1, L2 and L3	Public	PHS	2021	Islam, A., Rahim, T., Masuduzzaman & Shin, S. Y.
Wireless Body Area Network	Patient Monitoring	Tele-Medical	No	IoT	L1	Private	RPM	2021	Lee, T.-F., Li, H.-Z. & Hsieh, Y.-P.
Eletronic Medical Record	Patient Monitoring	Data Sharing	Yes	IoT	L1, L2 and L3	Consortium	RPM	2021	Chen, Z., Xu, W., Wang, B. & Yu, H.
Wireless Body Area Network	Patient Monitoring	Healthcare 4.0	No	Wearable	L1, L2 and L3	Private	RPM	2021	Taralunga, D. D. & Florea, B. C.
Wireless Body Area Network	Patient Monitoring	Data Sharing	No	Medical Sensor	L1, L2 and L3	Private	RPM	2021	Rahman, Z. U. et al.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	Yes	IoT	L1, L2 and L3	Private	RPM	2021	Aujla, G. S. & Jindal, A.
Remote Health Monitoring	Patient Monitoring	Data Sharing	Yes	Medical Sensor	L1, L2 and L3	Public	RPM	2021	Muhammad, G. & Hossain, M. S.
Remote Health Monitoring	Patient Monitoring	Home Monitoring	No	IoT	L1	Consortium	RPM	2021	Fang, L., Wu, Y., Wu, C. & Yu, Y.
Remote Health Monitoring	Patient Monitoring	Data Sharing	No	Raspberry Pi	L1	Private	RPM	2021	Mohan, D., Alwin, L., Neeraja, P., Lawrence, K. D. & Pathari, V.
Remote Health Monitoring	Blockchain	Data Sharing	No	Medical Sensor	N/A	All	RPM	2020	Bigini, G., Freschi, V. & Lattanzi, E.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	No	IoT	L1	Private	RPM	2021	Jeong, S., Shen, J.-H. J. & Ahn, B.
Survey	Blockchain	Security	Yes	IoT	L1, L2 and L3	Public	EM	2021	Sadawi, A. A., Hassan, M. S. & Ndiaye, M.
Wireless Body Area Network	Blockchain	Data Sharing	No	IoT	L1	Private	EM	2021	Ratta, P., Kaur, A., Sharma, S., Shabaz, M. & Dhiman, G.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	No	Medical Sensor	L1	Consortium	RPM	2021	Mohammad Hossein, K., Esmaeili, M. E., Dargahi, T., Khonsari, A. & Conti, M.
Eletronic Medical Record	Patient Monitoring	Data Sharing	No	IoT	L1	Private	RPM	2021	Ray, P. P., Chowhan, B., Kumar, N. & Almogren, A.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	No	Medical Sensor	L1, L2 and L3	Private	AAL	2020	Indumathi, J. et al. Block Chain Based
Remote Health Monitoring	Patient Monitoring	Security	Yes	Medical Sensor	L1, L2 and L3	Private	RPM	2021	Mehbodniya, A. et al.

Wireless Medical Sensor Network (WMSN)	Security Authentication	Security	No	Medical Sensor	L1	Private	RPM	2021	Wang, W. et al.
Eletronic Medical Record	Blockchain	Security	Yes	Medical Sensor	L1, L2 and L3	Consortium	RPM	2021	Gao, Y., Lin, H., Chen, Y. & Liu, Y.
Eletronic Medical Record	Patient Monitoring	Security	Yes	Medical Sensor	L1, L2 and L3	Public	RPM	2021	Wang, S., Wu, G., Ning, Z. & Li, J.
Survey	Blockchain	Consensus Algorithm	No	IoT	L1, L2 and L3	Public	Survey	2021	Ray, P. P., Dash, D., Salah, K. & Kumar, N.
Remote Health Monitoring	Patient Monitoring	Security	No	IoT	L1	Consortium	RPM	2021	Akkaoui, R.
Remote Health Monitoring	Patient Monitoring	Data Sharing	Yes	IoT	L1, L2 and L3	Public	RPM	2020	Uddin, M. A., et al.
Survey	Blockchain	Data Sharing	Yes	IoT	L1, L2 and L3	All	RPM	2021	ElRahman, S. A. & Alluhaidan, A. S.
Eletronic Medical Record	Patient Monitoring	Data Sharing	No	IoT	L1, L2 and L3	Public	AAL	2021	Srinivasu, P. Net al.
Wireless Body Area Network	Blockchain	Security	Yes	Body Sensor Networks		All	RPM	2021	Almagrabi, A. O et al.
Wireless Body Area Network	Blockchain	Security	Yes	Medical Sensor	L1	Private	RPM	2021	Wang, W. et al.
Eletronic Medical Record	Patient Monitoring	Data Sharing	Yes	Medical Sensor	L1, L2 and L3	Private	RPM	2021	Abbas, A. et al.
Wireless Body Area Network	Patient Monitoring	Security	Yes	IoT	L1, L2 and L3	Consortium	RPM	2021	Chen, F. et al.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	Yes	IoT	L1, L2 and L3	Private	AAL	2021	Wu, J. et al.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	Yes	Medical Sensor	L1, L2 and L3	Consortium	RPM	2021	Shynu, P. G., et al.
Wireless Body Area Network	Patient Monitoring	Healthcare 4.0	Yes	IoT	L1, L2 and L3	Public	AAL	2021	Ngabo, D. et al.
Cognitive Compute	Patient Monitoring	Healthcare 4.0	Yes	IoT	L1, L2 and L3	Consortium	RPM	2021	Laxmi Lydia, E. et al.
Wireless Body Area Network	Patient Monitoring	Cost Reduction	Yes	Medical Sensor	L1, L2 and L3	Consortium	RPM	2021	Lakhan, A. et al.
Wireless Body Area Network	Patient Monitoring	Security	No	Medical Sensor	L1	Private	RPM	2021	Elsayeh, M., Ezzat, K. A., El-Nashar, H. & Omran, L. N.
Wireless Body Area Network	Patient Monitoring	Tele-Medical	No	Medical Sensor	L1	Consortium	RPM	2020	Son, S. et al.
Wireless Body Area Network	Patient Monitoring	Security	Yes	IoT	L1	Private	RPM	2021	Sharmila, A. H. & Jaisankar, N.
Eletronic Medical Record	Medical record Manag	Security	No	Smart Device	L1	Private	RPM	2021	Christo, M. S. et al.
Eletronic Medical Record	Medical record Manag	Security	Yes	IoT	L1, L2 and L3	Private	RPM	2021	Mayer, A. H. et al.
Eletronic Medical Record	Medical record Manag	Data Sharing	Yes	IoT	L1	Private	RPM	2021	Egala, B. S., Pradhan, A. K., Badarla, V. & Mohanty, S. P.
Survey	Healthcare	Healthcare 4.0	Yes	IoT	L1, L2 and L3	All	RPM	2020	Al-Jaroodi, J., Mohamed, N. & Abukhousa, E.

Eletronic Medical Record	Medical record Manag	Security	Yes	Medical Sensor	L1	Consortium	RPM	2021	Shukla, S., et al.
Eletronic Medical Record	Patient Monitoring	Tele-Medical	No	Medical Sensor	L1	Private	AAL	2021	Hameed, K. et al.
Wireless Body Area Network	Patient Monitoring	Artificial Inteligence	No	Wearable	L1	Consortium	AAL	2021	Xie, Y. et al.
Survey	Blockchain	Cloud of Things	No	IoT	L1	Consortium	RPM	2020	Nguyen, D. C., Pathirana, P. N., Ding, M. & Seneviratne, A.
Eletronic Medical Record	Patient Monitoring	Security	No	Medical Sensor	L1	Private	RPM	2021	Elhoseny, M. et al.
Wireless Body Area Network	Patient Monitoring	Healthcare 4.0	Yes	Medical Sensor	L1	Private	RPM	2021	Arul, R. et al.
Eletronic Medical Record	Medical record Manag	Data Sharing	No	Medical Sensor	L1	Public	AAL	2021	Abdellatif, A. A. et al.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	No	Medical Sensor	L1	Consortium	RPM	2021	Arul, R. et al.
Wireless Body Area Network	Patient Monitoring	Security	No	Medical Sensor	L1	Public	RPM	2020	Tomaz, A. E. B., et al.
Remote Health Monitoring	Patient Monitoring	Artificial Inteligence	Yes	Medical Sensor	L1, L2 and L3	Public	RPM	2021	Otoum, S., Al Ridhawi, I. & Mouftah, H. T.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	Yes	Medical Sensor	L1	Private	RPM	2021	Alsahli, M. A., Alsanad, A., Hassan, M. M. & Gumaei, A.
Remote Health Monitoring	Patient Monitoring	Security	Yes	IoT	L1, L2 and L3	Public	RPM	2021	Lin, H. et al.
Remote Health Monitoring	Patient Monitoring	Artificial Inteligence	Yes	Medical Sensor	L1, L2 and L3	Private	RPM	2021	Bera, B., Mitra, A., Das, A. K., Puthal, D. & Park, Y.
Eletronic Medical Record	Patient Monitoring	Healthcare 4.0	Yes	Medical Sensor	L1	Private	AAL	2021	Krishnamoorthy, S., Dua, A. & Gupta, S.
Remote Health Monitoring	Patient Monitoring	Healthcare 4.0	Yes	Medical Sensor	L1, L2 and L3	Private	AAL	2021	Rini, P. L.
Remote Health Monitoring	Patient Monitoring	Security	Yes	Medical Sensor	L1, L2 and L3	Private	RPM	2020	Rahman, M. A., Shamim Hossain, M., Islam, M. S., Alrajeh, N. A. & Muhammad, G.
Eletronic Medical Record	Medical record Manag	Security	Yes	Medical Sensor	L1, L2 and L3	Private	AAL	2021	Nguyen, G. N. et al.
Eletronic Medical Record	Medical record Manag	Security	No	Medical Sensor	L1	Consortium	EM	2021	Wang, Y., Zhang, A., Zhang, P., Qu, Y. & Yu, S.
Eletronic Medical Record	Medical record Manag	Data Sharing	Yes	Medical Sensor	L1, L2 and L3	Consortium	EM	2021	Aggarwal, S. et al.

Remote Health Monitoring	Patient Monitoring	Data Sharing	No	IoT	L1	Private	AAL	2021	Barka, E., Dahmane, S., Kerrache, C. A., Khayat, M. & Sallabi, F.
Remote Health Monitoring	Patient Monitoring	Security	Yes	IoT	L1, L2 and L3	Consortium	AAL	2021	Al-Khazaali, A. A. T. & Kurnaz, S.
Remote Health Monitoring	Patient Monitoring	Security	Yes	IoT	L1, L2 and L3	Public	AAL	2021	Kumar, R. & Tripathi, R.
Eletronic Medical Record	Patient Monitoring	Healthcare 4.0	No	IoT	L1	Consortium	RPM	2021	Santos, J. A., Inácio, P. R. M. & Silva, B. M. C.

Table 6. Classification of Articles (by Author)

The paper classification was divided into technology area, focus area and usability scenarios. The technology area was to differentiate the main technology described into the articles, they did not follow any publication but just to separate and classify the papers. The focus area was classified by what is the main objective of the paper, and the usability scenarios was to separate the sub area of actuation.

Technology Area	Number of Articles
Eletronic Medical Record	43
Remote Health Monitoring	30
Wireless Body Area Network	22
Survey	7
Supply Chain	2
Healthcare IoT	2
Blockchain IoT	1
Weareble Devices	1
5G IoT	1
Blockchain Industrial IoT	1
Smart City	1
Implantable medical devices (IMD)	1
Wireless Body Sensor Nodes (WBSNs)	1
5G	1
Sport Fitness Management	1
Artificial Intelligence	1
Wireless Medical Sensor Network (WMSN)	1
Cognitive Compute	1

Table 7. Articles by Technology Area (by Author)

Although EMR is not a technology, it has a technology behind it, to manage, to control, to store. The objective of this classification is to indicate the major technology involved in managing the EMRs.

Focus Area	Number of Articles
Patient Monitoring	72
Blockchain	18
Medical Record Management	9
Healthcare	5
Patient Tractability	4
Healthcare	3
Medical Transportation	2
Smart Contract	1

Fitness Monitoring	1
Smart Cities	1
Survey	1
Security Authentication	1

Table 8. Articles by Focus usability area. (By Author)

Following the same classification parameter, the characteristics of the article is to focus into any acting area. There are 72 articles who has the main focus into Patient Monitoring, and some of them has the characteristics to track the patient.

Type of Sensor	Number of Articles
IoT	65
Medical Sensor	31
Body Sensor Networks	6
Wearable	5
BLE	1
Semantic Sensor Network	1
Continuous Glucose Monitors (CGMs) sensor	1
Low Energy	1
Temperature Sensor	1
Beacons	1
RFID	1
Mobile edge computing	1
IoDT (Drone)	1
Raspberry Pi	1
Smart Device	1

Table 9. Types of sensor used (By Author)

A great number of articles described IoT as the sensor used in the research, and it was not described exactly what type of sensor was used. For those articles they were classified into the IoT group of sensors.

Year	Number of fog articles	% of total articles in year
2021	33	58,93%
2020	10	24,39%
2019	5	31,25%
2018	0	0,00%

Table 10. Articles that consider Fog technology per year (By Author)

Some articles have related to usability of Fog, or CoS. The column described what Layer type of Sensor is described in the paper. Considered L1, as sensor Tier, L2 Edge Tier and L3 FoG or CoS Tier.

Class Type	Number of articles
Remote Patient Monitoring (RPM)	79
Public Health Surveillance (PHS)	8
Ambient Assisted Living (AAL)	21
Survey	3
Environmental Monitoring (EM)	7

Table 11. Internet of things technology surveillance domain (by Author)

According to Bublitz, F. M. et.al (2019), internet of things plays a growing role in varying domains, as described by Ziegler (2015), including environmental monitoring and health. This tables describes current uses of IoT technology within these domains among collected articles and providing context for some of the potential data sources (Ambient Assisted Living—AAL, Remote Patient Monitoring—RPM, Environmental monitoring, and Public Health Surveillance) that could be considered in scoping and developing the hospital surveillance system.

4.4 Research Result

Blockchain can be applied within healthcare management applications in public or private areas, monitoring and automatizing health claims adjudication and online patient information, achievement of healthcare records, sharing patients' medical data information, pharmaceutical and drug medicine counterfeiting, medical clinical trial, and precision medicine. (Casino et al., 2019; Boulos et al., 2018; Badr et al., 2018; Benchoufi & Ravaud, 2017; Gordon & Catalini, 2018; Vazirani et al., 2019). Combining blockchain technology and the Cloud of Sensor allows solving problems of scientific credibility of losing information (data missing or dredging, endpoint switching and selective publication) in clinical trials as well as issues of patients' informed consent (Benchoufi & Ravaud, 2017).

The adoption of blockchain technology into healthcare operations tends to increase the efficiency, reflecting on costs reduction, because virtually all transactions with blockchain are safer, more transparent, traceable and efficient (Kshetri, 2018). Furthermore, the blockchain adoption can enhance customers' trust, which will allow them to check the entire journey of goods across the service healthcare operation with full confidence. In this regard, the traceability mechanisms of the blockchain will support products fraud prevention and fake across the medical operations (Chen et al., 2018). As a result, hospital service operations will gain efficiency and cost reduction.

The healthcare system has become complex years after years for over the last three decades (Plsek & Greenhalgh, 2001; Reibling et al., 2019) due to differences regarding how countries fund, provide, and organize their health system. The new digital technologies, part of industry 4.0, such as blockchain, along with Radio frequency identification (RFID), Internet of Things (IoT), and Cloud of Sensors (CoS) are helping to control, to define, to monitor healthcare applications (Dhanvijay & Patil, 2019; Santos et al., 2018).

Blockchain is considered a disruptive technology, the potential uses of blockchains transcended the initial idea of the financial industry (Nofer et al., 2017). Because blockchains allow the secure exchange of data in a distributed manner, the technology could affect the structure and governance of healthcare operations as well as relationship configurations and information sharing between agent actors. If integrated with field-sensing technologies such as the Internet of Things (IoTs), blockchains could create permanent, shareable, and actionable records of products' digital footprints throughout the entire healthcare organization. Such improved visibility would provide product traceability, authenticity, and legitimacy – all of which are crucial to the medical, pharmaceutical, and healthcare industry (Nofer et al., 2017).

Based on the 118 papers screened, IoT technologies, blockchain and healthcare seem to be a representative new scenario within the application of blockchain in healthcare environment. Among those papers we can reference some papers discussing about topics related to sensors, medical sensors, RFID, Body Sensor Network and a great representative number of IoT. In this scenario, there is a possible solution to implement a sensor network system to control and to grant data security and trackability of medical information.

Therefore, a first challenge that emerges on the application of blockchain in the healthcare industry is how to use blockchain, IoT and CoS, to track medicine/drugs/medical equipment into

the healthcare environment to avoid loss of information and medical control, as well as counterfeited drugs. It is necessary to understand the internal logistic process among diverse internal areas of a hospital/clinic and elaborate a process to use electronic devices (sensors and IoT technologies) to collect data on medicine transactions among those areas. This allows controlling and managing medicine stock to avoid dispensation. It is necessary to identify the logistic technology process behind the healthcare areas, map the medicine or drug flow into the hospital and analyze the usage of electronical equipment, such as scanners, to collect the information to be processed. Some articles are referring the challenge applications.

Focus Area	Usability Scenarios	Fog Usage	Type of Sensor	Class Type	Year	Author
Patient Tractability	Data Processsing	No	IoT	RPM	2020	Rathee, G. et al.
Healthcare	Healthcare 4.0	Yes	IoT	PHS	2020	Kumar, A. et al.
Patient Tractability	Data Sharing	No	IoT	RPM	2019	Zheng, X. et al.
Patient Tractability	Healthcare 4.0	No	IoT	RPM	2020	Hathaliya, J. J. & Tanwar, S.
Smart Contract	Healthcare 4.0	No	IoT	AAL	2020	Sharma, A. et al.
Healthcare	Healthcare 4.0	No	IoT	AAL	2019	Nguyen, D. C. et al.
Medical Transportation	Healthcare 4.0	No	Low Energy	PHS	2020	Maitra, S. et al.
Medical Transportation	Temperature Monitoring	No	Temperature Sensor	PHS	2020	Singh, R. et al.
Patient Tractability	Data Sharing	No	IoT	PHS	2020	Biswas, S. et al.
Smart Cities	Healthcare 4.0	No	IoT	AAL	2020	Tripathi, G. et al.
Survey	Healthcare 4.0	Yes	IoT	Survey	2020	Qadri, Y. A. et al.
Blockchain	Data Sharing	No	Medical Sensor	RPM	2020	Bigini, G. et al
Blockchain	Data Sharing	Yes	IoT	RPM	2021	ElRahman, S. A. & Alluhaidan, A. S.
Healthcare	Healthcare 4.0	Yes	IoT	RPM	2020	Al-Jaroodi, J. et al

Table 12. Articles regarding controlling and tracking medicine information (by Author)

A second challenge that emerges on the application of blockchain in the healthcare environment is regards the EMRs. It refers to how to build a framework based on blockchain to meet accuracy and integrity requirements of EMRs. It is also possible to use sensors and the IoT technology to help improve the accuracy of data collected, to maintain the integrity of EMR information. Thus, the IoT can be part of such a framework. There is a broad area to be explored in challenge, regarding the specification of topology models and information technology architectures to attend the EMR requirements. Table 13 has articles referring the usage of blockchain into a sensor networking to control the integrity of EMR.

Focus Area	Usability Scenarios	Fog Usage	Type of Sensor	Class Type	Year	Author
Medical Record Managemanet	Data Sharing	Yes	IoT	PHS	2019	Silva, C.-C. A. et al.
Patient Tractability	Data Processsing	No	IoT	RPM	2020	Rathee, G. et al.
Patient Monitoring	Security	Yes	IoT	RPM	2020	Tahir, M. et al.
Healthcare	Healthcare 4.0	Yes	IoT	PHS	2020	Kumar, A. et al.
Blockchain	SWOT Analisys	No	Wearable	Survey	2020	De Aguiar, E. et al.
Patient Tractability	Data Sharing	No	IoT	RPM	2019	Zheng, X. et al.
Smart Contract	Healthcare 4.0	No	IoT	AAL	2020	Sharma, A. et al.
Healthcare	Healthcare 4.0	No	IoT	AAL	2019	Nguyen, D. C. et al.
Patient Monitoring	Data Sharing	No	Wearable	RPM	2018	Rifi, N. et al.
Blockchain	Security	No	IoT	RPM	2019	Dilawar, N. et al.
Healthcare	Tele-Medical	No	IoT	AAL	2020	Celesti, A. et al.
Patient Monitoring	Artificial Inteligence	Yes	IoT	EM	2019	Bublitz, F. M. et al.
Patient Monitoring	Security	No	Body Sensor Networks	RPM	2019	Iqbal, J. et al.
Patient Monitoring	Internet of Medical Things	Yes	(CGMs) sensor	RPM	2019	Fernández-Caramés, T. M. et al.
Patient Monitoring	Body Sensor	No	Body Sensor Networks	RPM	2018	Griggs, K. N. K. N. et al.
Patient Monitoring	Data Sharing	No	IoT	RPM	2019	Xu, J. et al.
Patient Monitoring	Internet of Medical Things	No	IoT	RPM	2020	Girardi, F. et al.
Patient Tractability	Data Sharing	No	IoT	PHS	2020	Biswas, S. et al.
Patient Monitoring	Healthcare 4.0	No	IoT	RPM	2020	Satamraju, K. P. & Malarkodi, B.
Healthcare	Security	No	IoT	AAL	2020	Tripathi, G. et al.
Smart Cities	Healthcare 4.0	No	IoT	AAL	2020	Tripathi, G. et al.
Blockchain	Identity Management	No	IoT	RPM	2020	Sousa, P. R. et al.
Patient Monitoring	Data Sharing	No	IoT	RPM	2020	Jamil, F. et al.
Blockchain	Data Sharing	No	Body Sensor Networks	AAL	2018	Liang, X. et al.
Patient Monitoring	Security	No	IoT	RPM	2019	Mohanta, B. K. et al.
Patient Monitoring	Data Sharing	Yes	IoT	RPM	2021	Chen, Z., Xu, W., Wang, B. & Yu, H.
Patient Monitoring	Data Sharing	No	IoT	RPM	2021	Ray, P. P. et al.
Blockchain	Security	Yes	Medical Sensor	RPM	2021	Gao, Y., Lin, H., Chen, Y. & Liu, Y.
Patient Monitoring	Security	Yes	Medical Sensor	RPM	2021	Wang, S., Wu, G., Ning, Z. & Li, J.
Patient Monitoring	Data Sharing	No	IoT	AAL	2021	Srinivasu, P. N. et al.
Patient Monitoring	Data Sharing	Yes	Medical Sensor	RPM	2021	Abbas, A. et al.
Medical Record Managemanet	Security	No	Smart Device	RPM	2021	Christo, M. S. et al.
Medical Record Managemanet	Security	Yes	IoT	RPM	2021	Mayer, A. H. et al.
Medical Record Managemanet	Data Sharing	Yes	IoT	RPM	2021	Egala, B. S., et al.
Medical Record Managemanet	Security	Yes	Medical Sensor	RPM	2021	Shukla, S., et al.

Patient Monitoring	Tele-Medical	No	Medical Sensor	AAL	2021	Hameed, K. et al.
Patient Monitoring	Security	No	Medical Sensor	RPM	2021	Elhoseny, M. et al.
Medical Record Managemanet	Data Sharing	No	Medical Sensor	AAL	2021	Abdellatif, A. A. et al.
Patient Monitoring	Healthcare 4.0	Yes	Medical Sensor	AAL	2021	Krishnamoorthy, S., Dua, A. & Gupta, S.
Medical Record Managemanet	Security	Yes	Medical Sensor	AAL	2021	Nguyen, G. N. et al.
Medical Record Managemanet	Security	No	Medical Sensor	EM	2021	Wang, Y., Zhang, A., Zhang, P., Qu, Y. & Yu, S.
Medical Record Managemanet	Data Sharing	Yes	Medical Sensor	EM	2021	Aggarwal, S. et al.
Patient Monitoring	Healthcare 4.0	No	IoT	RPM	2021	Santos, J. A., Inácio, P. R. M. & Silva, B. M. C.

Table 13. Articles regarding EMR information (by Author)

A third challenge that emerges on the application of blockchain in the healthcare regards the development of new devices and protocols to use for collecting data in healthcare operation applications. The benefits of using technologies such as sensor networks and clouds of sensors (CoS) with blockchain and healthcare may comprise, besides ensuring the accuracy of data collected and maintaining the integrity of exchanged information, the processing of large amounts of data, along with the reduction in the response time of applications. Those characteristics are to guarantee the accuracy data for monitoring patient, inside and outside of a hospital. The necessity to collect health data from a patient and treat the collected information with accuracy and integrity, was responsible for are a great number of articles referring the patient monitoring specially into the COVID-19 pandemic period as show in figure 21. Using Islam, A. et al, 2021, as reference, the article provide specification to use a sensor, into a drone device, to collect temperature information and to present at a special screen. Use the temperature information, a fever suspicious can indicate a possible COVID patient.

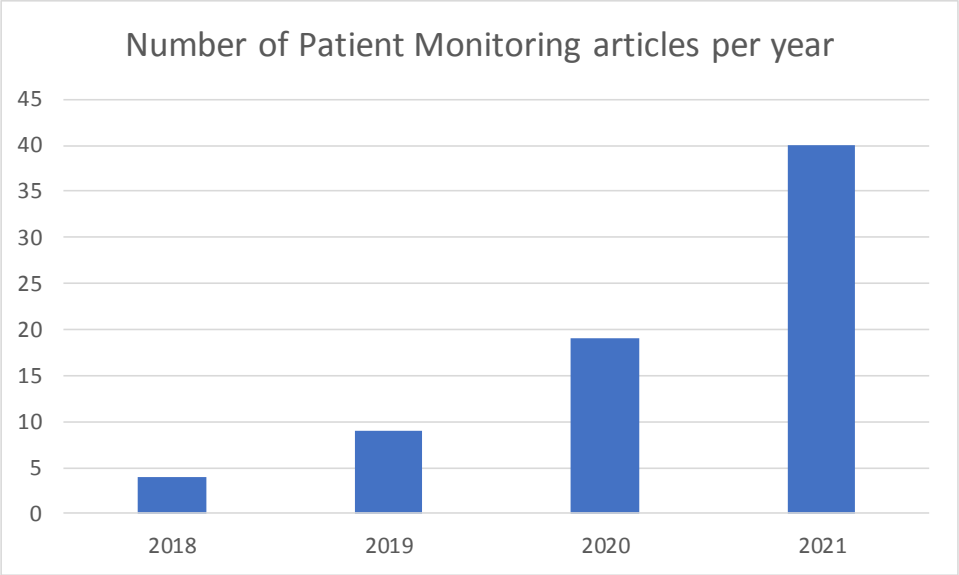


Figure 21. Number of patient monitoring articles per year (by author).

However, further implementations and evaluations in real scenarios are still more necessary. Moreover, the usage of new sensors combined with IoT technology to control healthcare applications is becoming a standard nowadays and have more competitive prices than more recent technologies. In this sense, a challenge that emerges in this paper is how to apply the blockchain technology along with clouds of sensors to enable healthcare applications, given that these technologies could play a pivotal role in the healthcare industry, and could bring all the aforementioned benefits to healthcare

5. Conclusion

This paper presented a systematic literature review on the application of blockchain in the healthcare using sensors. The systematic literature review followed a protocol based on PRISMA. The first research question referred to investigating the bibliometric evolution of publications regarding the usage of blockchain in the healthcare environments and possible usage of Wireless Sensor Network. The results show that research in this field is growing rapidly as the number of publications has increased in the most recent years, and there is much interest from specialists from the areas of healthcare and computer science. In addition, the potential benefits of using sensor and blockchain to several applications in the healthcare system were raised.

The Internet of Things network is growing tremendously in terms of number of devices and application types and most of this growing process is to use IoT technology to represent network sensor. Some of listed articles describes as IoMT (Internet of medical Things) a medical sensor that communicate among other devices using the IP (Internet Protocol), other articles define the type of sensor like Continuous Glucose Monitors (CGMs) sensor or Coronary Diagnostic sensor, and some of the reference a sensor as a physical device like Raspberry, RFID or Beacon. In this paper, there are a lot of articles referring IoT technology thru a sensor network, due this, there are a great number of IoT devices listed in this study. This has created many challenges that need urgent solutions to enable the full potential of IoT (or sensor) to be exploited in the future. On the other hand, blockchain technology has emerged as a decentralized and secure, immutable, transparent and distributed technology that has a promising role in many sectors, include healthcare. The characteristics and structure of blockchain system make it a strong candidate to solve IoT system problems through integration among other types of sensor. The integration process caught the attention of many researchers who created different architectures and cited many integrate IoT, running locally or into Edge / Fog architecture thru Blockchain projects.

Blockchains have the potential to revolutionize the way healthcare data is efficiently stored, manipulated, and exchanged between healthcare entities while maintaining those entities' incentives. As an example, after a patient receives a lab result, the data instead of being stored centrally on the lab's servers, it can be stored encrypted on the blockchain network. The data itself can be mark with the creator of the data (i.e., the lab) and all parties accessing the data in the future can see who generated it. This process allows the preservation of commercial incentives for the

hospital or clinic, as they will still be able to bill insurers and receive funding based on their work. This mechanism transfer to the patient the control of the data who can actively decide to share it with a new family doctor or send it to a university for research purposes. This reduces concerns about lost or corrupted data, slow data exchange, and unknown resale of data.

In the healthcare field, IoT is brought into use for applications such as regular monitoring of patient health, drug traceability, electronic medical records control. However, there are several security issues in IoT, which can be solved by integrating IoT with Blockchain. In this paper an attempt was made to enumerate different possible ways in which IoT technology, along with Blockchain, can be integrated into the healthcare sector to improve overall performance and strengthen the current healthcare industry. Across several areas, three of them has a major application. (a) Medical records management, (b) Remote monitoring of patient health and (c) Drug traceability, where Blockchain and IoT technologies have their applicability were explored in detail. Furthermore, various challenges and potential issues in deploying these two revolutionary technologies, namely IoT and Blockchain in the healthcare sector, were explored and discussed. Based on this study, it can be clearly stated that these two technologies have enormous potential in the healthcare environment and, once integrated, will revolutionize the entire healthcare sector.

6. References

Abujamra, R. & Randall, D., 2019. Blockchain applications in healthcare and the opportunities and the advancements due to the new information technology framework. Em: *Advances in Computers.* s.l.:Elsevier.

Adjekum, A., Ienca, M. & Vayena, E., 2017. What Is Trust? Ethics and Risk Governance in Precision Medicine and Predictive Analytics. *OMICS: A Journal of Integrative Biology,* 12, 21(12), pp. 704-710.

Agbo, C., Mahmoud, Q. & Eklund, J., 2019. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare,* 4 4, 7(2), p. 56.

Almanasreh, E., Moles, R. & Chen, T. F., 2016. The medication reconciliation process and classification of discrepancies: a systematic review.. *British Journal of Clinical Pharmacology,* 9, 82(3), pp. 645-658.

Anandhi, S., Anitha, R. & Sureshkumar, V., 2018. An automatic RFID reader-to-reader delegation protocol for SCM in cloud computing environments. *Journal of Supercomputing,* 7, 74(7), pp. 3148-3167.

ANTONELLI, D.; BRUNO, G. Application of Process Mining and Semantic Structuring Towards a Lean Healthcare Network. **Advances in Information and Communication Technology**, v. 463, p. 497-508, 2015.

Avram, R. et al., 2018. Understanding the patient perspective on research access to national health records databases for conduct of randomized registry trials. *International Journal of Cardiology,* Volume 262, pp. 110-116.

Bäck, M. A. & Calltorp, J., 2015. The Norrtaelje model: a unique model for integrated health and social care in Sweden.. *International Journal of Integrated Care,* Volume 15.

Badr, S., Gomaa, I. & Abd-Elrahman, E., 2018. *Multi-tier blockchain framework for IoT-EHRs systems.* s.l., Elsevier B.V., pp. 159-166.

Balsari, S. et al., 2018. Reimagining health data exchange: An application programming interface-enabled roadmap for India. *Journal of Medical Internet Research,* 7.20(7).

Banerjee, M., Lee, J. & Choo, K. K. R., 2018. A blockchain future for internet of things security: a position paper. *Digital Communications and Networks,* 1 8, 4(3), pp. 149-160.

Benchoufi, M. & Ravaud, P., 2017. Blockchain technology for improving clinical research quality. *Trials,* 18(1).

Benniche, S., 2019. Using blockchain technology to recycle cancer drugs. *The Lancet Oncology,* 20(6), p. e300.

Bloomrosen, M. & Berner, E. S., 2018. Findings from 2017 on Health Information Managemen. *Yearbook of medical informatics,* 8, 27(1), pp. 67-73.

Boulos, M. N. K., Wilson, J. T. & Clauson, K. A., 2018. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. *INTERNATIONAL JOURNAL OF HEALTH GEOGRAPHICS,* 7.Volume 17.

Brogan, J., Baskaran, I. & Ramachandran, N., 2018. Authenticating Health Activity Data Using Distributed Ledger Technologies. *Computational and Structural Biotechnology Journal,* 1 1, Volume 16, pp. 257-266.

Casino, F., Dasaklis, T. K. & Patsakis, C., 2019. *A systematic literature review of blockchain-based applications: Current status, classification and open issues.* s.l.:Elsevier Ltd.

Chen, Y. et al., 2018. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *Journal of Medical Systems,* 11.43(1).

Cossy-Gantner, A., Germann, S., Schwalbe, N. R. & Wahl, B., 2018. Artificial intelligence (AI) and global health: How can AI contribute to health in resource-poor settings?. *BMJ Global Health,* 3(4).

Damaševičius, R., Maskeliūnas, R., Kazanavičius, E. & Woźniak, M., 2018. Combining Cryptography with EEG Biometrics.. *Computational Intelligence and Neuroscience,* Volume 2018.

Ding, B., 2018. Pharma Industry 4.0: Literature review and research opportunities in sustainable pharmaceutical supply chains. *Process Safety and Environmental Protection,* Volume 119, pp. 115-130.

Drosatos, G. & Kaldoudi, E., 2019. Blockchain Applications in the Biomedical Domain: A Scoping Review. *Computational and Structural Biotechnology Journal,* Volume 17, pp. 229-240.

Dubovitskaya, A. et al., 2017. Secure and Trustable Electronic Medical Records Sharing using Blockchain.

Dubovitskaya, A. et al., 2017. Secure and Trustable Electronic Medical Records Sharing using Blockchain.. *AMIA ... Annual Symposium proceedings. AMIA Symposium,* Volume 2017, pp. 650-659.

Durham, J., Pavignani, E., Beesley, M. & Hill, P. S., 2015. Human resources for health in six healthcare arenas under stress: A qualitative study. *Human Resources for Health,* 13(1).

Dwivedi, A. D., Srivastava, G., Dhar, S. & Singh, R., 2019. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors (Switzerland),* 1.19(2).

El-Hajj, M., Fadlallah, A., Chamoun, M. & Serhrouchni, A., 2019. A survey of internet of things (IoT) authentication schemes. *Sensors (Switzerland),* 3.19(5).

Fan, K. et al., 2018. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems,* 1 8.42(8).

Firdaus, A. et al., 2018. Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management. *Journal of Medical Systems,* 6.42(6).

Galvez, J. F., Mejuto, J. C. & Simal-Gandara, J., 2018. *Future challenges on the use of blockchain for food traceability analysis.* s.l.:Elsevier B.V..

GOMES, A.; SENNA, P.; MONTEIRO, A.; PINHA, D. Study on techniques and tools used in lean healthcare implementation: a literature review. **Brazilian Journal of Operations & Production Management**, v. 13, n. 4, p.406-420, 2016.

Gordon, W. J. & Catalini, C., 2018. *Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability.* s.l.:Elsevier B.V..

Greenes, R. A., 2015. Health information systems 2025. *Healthcare Information Management Systems: Cases, Strategies, and Solutions: Fourth Edition,* 8(2), pp. 579-600.

Hackl, W. O. & Hoerbst, A., 2018. On the Way to Close the Loop in Information Logistics: Data from the Patient - Value for the Patient. *Yearbook of medical informatics,* 8, 27(1), pp. 91-97.

Hofman, D., Lemieux, V. L., Joo, A. & Batista, D. A., 2019. "The margin between the edge of the world and infinite possibility": Blockchain, GDPR and information governance. *Records Management Journal,* 29(1/2), pp. 240-257.

Hölbl, M., Kompara, M., Kamišalić, A. & Zlatolas, L. N., 2018. A systematic review of the use of blockchain in healthcare. *Symmetry,* 10(10).

Hovenga, E. J. & Grain, H., 2013. Health information systems. *Health Information Governance in a Digital Environment,* 36(1), pp. 120-140.

Hussein, A. F. et al., 2018. A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. *Cognitive Systems Research,* 1 12, Volume 52, pp. 1-11.

I., R. & Likic R. AO - Likic, R. O. h.-0.-1.-4., 2018. Opportunities for Use of Blockchain Technology in Medicine. *Applied Health Economics and Health Policy,* 16(5), pp. 583-590.

IEEE-SA, 2017. State of Blockchain Adoption on the Pharmaceutical Supply Chain Industry Study. *The State of Blockchain Adoption on the Pharmaceutical Supply Chain,* Issue October, pp. 1-5.

Irving, G. & Holden, J., 2017. How blockchain-timestamped protocols could improve the trustworthiness of medical science. *F1000Research,* 30 3, Volume 5, p. 222.

Janvier, S., De Spiegeleer, B., Vanhee, C. & Deconinck, E., 2018. Falsification of biotechnology drugs: current dangers and/or future disasters?. *Journal of Pharmaceutical and Biomedical Analysis,* Volume 161, pp. 175-191.

Jiang, Y., Wang, C., Wang, Y. & Gao, L., 2019. A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management. *Sensors (Basel, Switzerland),* 5.19(9).

Jo, B. W., Khan, R. M. A. & Lee, Y. S., 2018. Hybrid blockchain and internet-of-things network for underground structure health monitoring. *Sensors (Switzerland),* 12.18(12).

Kamel Boulos, M. N., Wilson, J. T. & Clauson, K. A., 2018. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare.. *International journal of health geographics,* 17(1), p. 25.

Kitchenham, B. et al., 2009. *Systematic literature reviews in software engineering - A systematic literature review.* s.l.:s.n.

Kitchenham, B. et al., 2010. *Systematic literature reviews in software engineering-A tertiary study.* s.l.:Elsevier B.V..

Kivoto, P. M. et al., 2018. Clinical and Financial Implications of Medicine Consumption Patterns at a Leading Referral Hospital in Kenya to Guide Future Planning of Care. *Frontiers in Pharmacology,* Volume 9.

Kolff, C. A., Scott, V. P. & Stockwell, M. S., 2018. *The use of technology to promote vaccination: A social ecological model based framework.* s.l.:Taylor and Francis Inc..

Koshechkin, K. A., Klimenko, G. S., Ryabkov, I. V. & Kozhin, P. B., 2018. Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation. *Procedia Computer Science,* Volume 126, pp. 1323-1328.

Kumar, A. et al., 2016. Improving medical stores management through automation and effective communication. *Medical Journal Armed Forces India,* 72(1), pp. 61-66.

Kumar, R. & Tripathi, R., 2019. *Traceability of counterfeit medicine supply chain through Blockchain.* s.l., s.n., pp. 568-570.

Kuo, T. T., Kim, H. E. & Ohno-Machado, L., 2017. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association,* 11, 24(6), pp. 1211-1220.

Kuupiel, D. et al., 2019. Poor supply chain management and stock-outs of point-of-care diagnostic tests in Upper East Region's primary healthcare clinics, Ghana. *PLoS ONE,* 14(2).

Lee, J., 2018. Patch transporter: Incentivized, decentralized software patch system for WSN and IoT environments. *Sensors (Switzerland),* 2.18(2).

Leurent, B. et al., 2016. Monitoring patient care through health facility exit interviews: an assessment of the Hawthorne effect in a trial of adherence to malaria treatment guidelines in Tanzania.. *BMC Infectious Diseases,* Volume 16.

Li, D. et al., 2018. Information security model of block chain based on intrusion sensing in the IoT environment. *Cluster Computing,* 3.pp. 1-18.

Li, H. et al., 2018. Blockchain-Based Data Preservation System for Medical Data. *Journal of Medical Systems,* 1 8.42(8).

Lin, L.-y., Warren-Gash, C., Smeeth, L. & Chen, P.-C., 2018. Data resource profile: the National Health Insurance Research Database (NHIRD).. *Epidemiology and Health,* Volume 40.

Liu, F., Tang, Y. & Wang, L., 2019. EHAPAC: A privacy-supported access control model for IP-enabled wireless sensor networks. *Sensors (Switzerland),* 4.19(7).

Lopez, D., Brown, A. W. & Plans, D., 2019. Developing opportunities in digital health: The case of BioBeats Ltd. *Journal of Business Venturing Insights,* Volume 11, p. e00110.

Mackey, T. K. et al., 2019. 'Fit-for-purpose?' - Challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Medicine,* 27 3.17(1).

Ma, H. et al., 2019. PPCD: Privacy-preserving clinical decision with cloud support.. *PLoS ONE,* 14(5).

Mamoshina, P. et al., 2018. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget,* 1, 9(5), pp. 5665-5690.

Maslove, D. M., Klein, J., Brohman, K. & Martin, P., 2018. Using Blockchain Technology to Manage Clinical Trials Data: A Proof-of-Concept Study. *JMIR Medical Informatics,* 6(4), p. e11949.

McGhin, T., Choo, K. K. R., Liu, C. Z. & He, D., 2019. *Blockchain in healthcare applications: Research challenges and opportunities.* s.l.:Academic Press.

Memon, R. A., Li, J. P. & Ahmed, J., 2019. Simulation Model for Blockchain Systems Using Queuing Theory. *ELECTRONICS,* 8(2).

Min, H., 2019. Blockchain technology for enhancing supply chain resilience. *Business Horizons,* 1 1, 62(1), pp. 35-45.

MOHER, D.; LIBERATI, A.; TETZLAFF, J.; ALTMAN, D. G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. **PLoS Medicine**, v. 6, n. 7, p. 1-9, 2009.

Namisango, E. et al., 2016. Strengthening pharmaceutical systems for palliative care services in resource limited settings: Piloting a mHealth application across a rural and urban setting in Uganda. *BMC Palliative Care,* 15(1).

Nightingale, A., 2009. *A guide to systematic literature reviews.* s.l.:s.n.

Niranjanamurthy, M., Nithya, B. N. & Jagannatha, S., 2018. *Analysis of Blockchain technology: pros, cons and SWOT.* s.l.:Springer New York LLC.

Nørfeldt, L. et al., 2019. Cryptopharmaceuticals: increasing the safety of medication by a blockchain of pharmaceutical products. *Journal of Pharmaceutical Sciences.*

Onik, M. M. H. et al., 2019. Blockchain in Healthcare: Challenges and Solutions. Em: N. Dey, H. Das, B. Naik & H. S. Behera, eds. *Big Data Analytics for Intelligent Healthcare Management.* s.l.:Academic Press, pp. 197-226.

Ozercan, H. I., Ileri, A. M., Ayday, E. & Alkan, C., 2018. Realizing the potential of blockchain technologies in genomics. *Genome Research,* 9, 28(9), pp. 1255-1263.

Queiroz, M. M. & Fosso Wamba, S., 2019. Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management,* 1 6, Volume 46, pp. 70-82.

Rasheed, H., Höllein, L. & Holzgrabe, U., 2018. Future information technology tools for fighting substandard and falsified medicines in low- and middle-income countries. *Frontiers in Pharmacology,* 9(AUG).

Rathee, G. et al., 2019. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications,* 6.

Reyna, A. et al., 2018. On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems,* 1 11, Volume 88, pp. 173-190.

Rotenberg, D. J. et al., 2018. The CAMH Neuroinformatics Platform: A Hospital-Focused Brain-CODE Implementation.. *Frontiers in Neuroinformatics,* Volume 12.

Santos, M. A. et al., 2019. Online Heart Monitoring Systems on the Internet of Health Things Environments: A Survey, a Reference Model and an Outlook. *Information Fusion.*

Satoshi Nakamato, 2008. *Bitcoin: A Peer-toPeer Electronic Cash System,* s.l.: s.n.

Shanley, A., 2017. *Could blockchain improve pharmaceutical supply chain security?,* s.l.: s.n.

Shen, Y. et al., 2019. KMR: knowledge-oriented medicine representation learning for drug–drug interaction and similarity computation.. *Journal of Cheminformatics,* Volume 11.

Simske, S., 2019. Application II: Medical and health-care informatics, economics, business, and finance. Em: S. Simske, ed. *Meta-Analytics.* s.l.:Morgan Kaufmann, pp. 299-310.

Staffa, M. et al., 2018. An OpenNCP-based Solution for Secure eHealth Data Exchange. *Journal of Network and Computer Applications,* Volume 116, pp. 65-85.

Sylim, P., Liu, F., Marcelo, A. & Fontelo, P., 2018. Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. *Journal of Medical Internet Research,* 9.20(9).

T.K., M. & Nayyar G. AO - Mackey, T. K. O. h.-0.-2.-7., 2017. A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opinion on Drug Safety,* 16(5), pp. 587-602.

Till, B. M., Peters, A. W., Afshar, S. & Meara, J. G., 2017. From blockchain technology to global health equity: Can cryptocurrencies finance universal health coverage. *BMJ Global Health,* 2(4).

Townend, D., 2018. Conclusion: harmonisation in genomic and health data sharing for research: an impossible dream?. *Human Genetics,* 137(8), pp. 657-664.

Trap, B. et al., 2016. Article 1: Supervision, Performance Assessment, and Recognition Strategy (SPARS) - a multipronged intervention strategy for strengthening medicines management in Uganda: Method presentation and facility performance at baseline. *Journal of Pharmaceutical Policy and Practice,* 9(1).

Tseng, J. H., Liao, Y. C., Chong, B. & Liao, S. W., 2018. Governance on the drug supply chain via gcoin blockchain. *International Journal of Environmental Research and Public Health,* 6.15(6).

Van Roessel, I., Reumann, M. & Brand, A., 2018. Potentials and Challenges of the Health Data Cooperative Model. *Public Health Genomics,* 8, 20(6), pp. 321-331.

Vazirani, A. A., O'Donoghue, O., Brindley, D. & Meinert, E., 2019. Implementing Blockchains for Efficient Health Care: Systematic Review. *Journal of medical Internet research,* 2, 21(2), p. e12439.

Vega-Barbas, M., Seoane, F. & Pau, I., 2019. Characterization of User-Centered Security in Telehealth Services. *International Journal of Environmental Research and Public Health,* 3, 16(5), p. 693.

Verde, F. et al., 2019. Could Blockchain Technology Empower Patients, Improve Education, and Boost Research in Radiology Departments? An Open Question for Future Applications. *Journal of Digital Imaging,* 6.

Viriyasitavat, W., Anuphaptrirong, T. & Hoonsopon, D., 2019. When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. *Journal of Industrial Information Integration.*

Wallace, A. S. et al., 2017. Vaccine wastage in Nigeria: An assessment of wastage rates and related vaccinator knowledge, attitudes and practices. *Vaccine,* 12, 35(48), pp. 6751-6758.

Wallgren, U. M., Antonsson, V. E., Castrén, M. K. & Kurland, L., 2016. Longer time to antibiotics and higher mortality among septic patients with non-specific presentations -a cross sectional study of Emergency Department patients indicating that a screening tool may improve identification. *Scandinavian Journal of Trauma, Resuscitation and Emergency Medicine,* 6 1.24(1).

Wang, Y., Singgih, M., Wang, J. & Rit, M., 2019. Making sense of blockchain technology: How will it transform supply chains?. *International Journal of Production Economics,* 1 5, Volume 211, pp. 221-236.

Wong, D. R., Bhattacharya, S. & Butte, A. J., 2019. Prototype of running clinical trials in an untrustworthy environment using blockchain. *Nature Communications,* 10(1).

Yue, X. et al., 2016. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *Journal of Medical Systems,* 40(10).

Zhang, P., Schmidt, D. C., White, J. & Lenz, G., 2018. Blockchain Technology Use Cases in Healthcare. Em: P. Raj & G. C. Deka, eds. *Advances in Computers.* s.l.:Elsevier, pp. 1-41.

Zhou, L., Wang, L. & Sun, Y., 2018. MIStore: a Blockchain-Based Medical Insurance Storage System. *Journal of Medical Systems,* 42(8).

Santos, I. L; 2017; " ON THE VIRTUALIZATION AND RESOURCE ALLOCATION IN THE CLOUD OF SENSORS" UFRJ

Vieira, S, P, 2019 " SUPPLY CHAIN RISK MANAGEMENT IN HEALTHCARE: IDENTIFICATION, ASSESSMENT AND MITIGATION" CEFET.

A. Reyna, C. Martin, J. Chen, E. Soler, M. Diaz, (2018) On blockchain and its integration with IoT. Challenges and opportunities, Future Gener. Comput. Syst.

Azzi, R.; Kilany,; R. Sokhn, M.; (2019) "The power of a blockchain-based supply chain" Computers & Industrial Engineering

Abeyratne, S. A. and R. P. Monfared. (2016). "Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger". In: International Journal of Research in Engineering and Technology 5.9, pp. 1–10.

CAPES: Portal do Periódico CAPES. http://www.periodicos.capes.gov.br/, Accessed: 2018-Dec-01.

Christidis, K. and Devetsikiotis, M. (2016), "Blockchains and smart contracts for the internet of things", IEEE Access, Special Section on the Plethora of Research in IoT, Vol. 4, pp. 2292-2303.

Gale T.; Rajamani D., Sriskandarajah C. (2009). "The Impact of RFID on Supply Chain Performance". Technology, Operations and Management. 2.

J. Lin, Z. Shen, C. Miao, S. Liu, (2017) "Using blockchain to build trusted LoRaWAN sharing server", International Journal of Crowd Science, Vol. 1 Issue: 3, pp.270-280

Kais M., Bajica, E.; Chaxela, F.; Meyerb, F (2017) A comparative study of LPWAN technologies for large-scale IoT deployment. The Korean Institute of Communications Information Sciences.

Kshetri, N. (2018) "Blockchain's roles in meeting key supply chain management objectives", International Journal of Information Management, Vol. 39 (April), pp. 80-89.

Lambert, D. M., Cooper, M. C., (2000)" Issues in Supply Chain Management", Industrial Marketing Management 29, 65–83

M.A. Khan, K. Salah, (2017) Iot security: review, blockchain solutions, and open challenges, Future Gener. Comput. Syst.

Nakamoto S.; (2008) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, Accessed: 2018-Dec-01.

Neuenfeld JR, A. L.; SILUK J. C.; NARA E. O. ;(2015) ESTUDO DE UM FLUXO INTERNO DE MATERIAIS BASEADO NA FILOSOFIA LEAN MANUFACTURING Associação Brasileira de Engenharia de Produção vol.25 no.3 São Paulo.

Romano, D. and Schmid, G., (2017) "Beyond Bitcoin: a critical look at Blockchain-Based systems", Cryptography, Vol. 1 No. 2, available at: www.mdpi.com/2410-387X/1/2/15/htm (accessed:2018-Nov-18)

Sinha, R S.; Wei, Y.; Hwang, S. (2017) A survey on LPWA technology: LoRa and NB-IoT. The Korean Institute of Communications Information Sciences.

Tabbane, S.; (2017) "Developing the ICT ecosystem to harness Internet-of-Things (IoT)" Regional Workshop for Africa,

Tapscott D, Tapscott A. (2016.) Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. New York: Penguin;

Van Gralingen, B. (2016). How blockchain could help to make the food we eat safer around the world. Forbes, 2016. [Online]. Available: https://www.forbes.com/sites/ibm/2016/11/01/how-blockchain-could-help-to-make-the-food-we-eat-safer-around-the-world/#6b998fd5143d [Accessed 01.may 2019].

Xu, L.; He, W.; Li, S.; (2014) "Internet of Things in Industries: A Survey" IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS vol.10, Issue: 4, pp. 2233-2243

Y. Li, M. Hou, H. Liu, and Y. Liu, (2012.)"Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things," Inf. Technol. Manage., vol. 13, no. 4, pp. 205–216,

Krähenbühl-Melcher A, Schlienger R, Lampert M, et al. Drug-related problems in hospitals: a review of the recent literature. Drug Saf. 2007 ;30:379–407.

Westbrook J, Rob M, Woods A, Parry D. Errors in the administration of intravenous medications in hospital and the role of correct procedures and nurse experience. BMJ Qual Saf. 2011 ;20:1027–1034.

Keers RN, Williams SD, Cooke J, Ashcroft DM. Prevalence and nature of medication administration errors in health care settings: a systematic review of direct observational evidence. Ann Pharmacother. 2013 ;47:237–256

Schepel Lotta, Aronpuro Kirsi, Kvarnström Kirsi, Holmström Anna-Riia, Airaksinen Marja (2019) "Strategies for improving medication safety in hospitals: Evolution of clinical pharmacy services" Research in Social and Administrative Pharmacy, In press, corrected proof

P.E. Plsek, T. Greenhalgh, (2001) "The challenge of complexity in health care" BMJ: British Medical Journal, 323 (7313), pp. 625-628

N. Reibling, M. Ariaans, C. Wendt, "Worlds of Healthcare: A Healthcare System Typology of OECD Countries" (2019), Health Policy, Volume 123, Issue 7, Pages 611-620,

Mrinai M. Dhanvijay, Shailaja C. Patil (2019): "Internet of Things: A survey of enabling technologies in healthcare and its applications", Computer Networks, Volume 153.

Ziegler, S.; Nikoletsea, S.; Krco, S.; Rolim, J.; Fernandes, J. Internet of Things and crowd sourcing—A paradigm change for the research on the Internet of Things. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 395–399.

Bublitz, F. M. et al. Disruptive technologies for environment and health research: An overview of artificial intelligence, blockchain, and internet of things. Int. J. Environ. Res. Public Health 16, (2019).

I.C. Lin, T.C. Liao, A survey of blockchain security issues and challenges, IJ Netw. Secur. 19 (5) (2017) 653–659.

C. Cachin, M. Vukolić, Blockchain consensus protocols in the wild, 2017, arXiv preprint arXiv:1707.01873.

Scarlat, Emil & Maracine, Virginia & Maries, Iulia. (2011). Modelling the dynamics of knowledge flow within networked communities of professionals. 10.1016/B978-1-84334-646-3.50002-2.

S. Mubeen, P. Nikolaidis, A. DIdic, H. Pei-Breivold, K. Sandstrom, M. Behnam, Delay mitigation in offloaded cloud controllers in industrial IoT, IEEE Access 5 (2017) 4418–4430.

K. Bilal, S. Ur, R. Malik, S.U. Khan, Trends and Challenges in Cloud Datacenters, 2016.

A.M. Elmisery, S. Rho, M. Aborizka, A new computing environment for collective privacy protection from constrained Healthcare devices to IoT cloud services, Cluster Comput. (2017) 1–28.

W. You, W. Learn, Fog Computing and the Internet of Things : Extend the Cloud to Where the Things Are, 2015, pp. 1–6.

P. Hu, S. Dhelim, H. Ning, T. Qiu, Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues, Vol. 98, Academic Press, 2017,pp. 27–42.

H. Zhang, Y. Xiao, S. Bu, D. Niyato, R. Yu, Z. Han, Fog Computing in Multi-Tier Data Center Networks : A Hierarchical Game Approach, 2016, pp. 1–6.

M. Aazam, E.N. Huh, Fog computing: The Cloud-IoT/IoE middleware paradigm, IEEE Potentials 35 (3) (2016) 40–44.

L. Cerina, S. Notargiacomo, M.G. Paccanit, M.D. Santambrogio, A fogcomputing architecture for preventive healthcare and assisted living in smart ambients, in: RTSI 2017 - IEEE 3rd Int. Forum Res. Technol. Soc. Ind. Conf. Proc., 2017.

J. Li, J. Jin, D. Yuan, M. Palaniswami, K. Moessner, EHOPES: Data-centered Fog platform for smart living, in: 25th Int. Telecommun. Networks Appl. Conf. ITNAC 2015, 2015, pp. 308–313.

K. Bilal, O. Khalid, A. Erbad, S.U. Khan, Potentials, Trends, and Prospects in Edge Technologies: Fog, Cloudlet, Mobile Edge, and Micro Data Centers, Comput. Netw. 130 (2017) 94–120.

Ashkan Y., Caleb F., Tam N., Krishna K., Fatemeh J., Amirreza N., Jian K., Jason P. J., All one needs to know about fog computing and related edge computing paradigms: A complete survey. Journal of Systems Architecture, Volume 98, 2019, Pages 289-330

Brogan J., Baskaran I., Ramachandran N., Authenticating Health Activity Data Using Distributed Ledger Technologies - Computational and Structural Biotechnology Journal - Volume 16, 2018, Pages 257-266

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the fuzzy sets theory field. Journal of Informetrics, 5(1), 146-166.

Islam, A., Rahim, T., Masuduzzaman & Shin, S. Y. A Blockchain-Based Artificial Intelligence-Empowered Contagious Pandemic Situation Supervision Scheme Using Internet of Drone Things. IEEE Wirel. Commun. 28, 166–173 (2021).

Lee, T.-F., Li, H.-Z. & Hsieh, Y.-P. A blockchain-based medical data preservation scheme for telecare medical information systems. Int. J. Inf. Secur. 20, 589–601 (2021).

Chen, Z., Xu, W., Wang, B. & Yu, H. A blockchain-based preserving and sharing system for medical data privacy. Futur. Gener. Comput. Syst. 124, 338–350 (2021).

Taralunga, D. D. & Florea, B. C. A blockchain-enabled framework for mhealth systems. Sensors 21, (2021).

Rahman, Z. U. et al. A Collateral Sensor Data Sharing Framework for Decentralized Healthcare Systems. IEEE Sens. J. 21, 27848–27857 (2021).

Aujla, G. S. & Jindal, A. A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring. IEEE J. Sel. Areas Commun. 39, 491–499 (2021).

Muhammad, G. & Hossain, M. S. A Deep-Learning-Based Edge-Centric COVID-19-Like Pandemic Screening and Diagnosis System within a B5G Framework Using Blockchain. IEEE Netw. 35, 74–81 (2021).

Fang, L., Wu, Y., Wu, C. & Yu, Y. A Nonintrusive Elderly Home Monitoring System. IEEE Internet Things J. 8, 2603–2614 (2021).

Mohan, D., Alwin, L., Neeraja, P., Lawrence, K. D. & Pathari, V. A private Ethereum blockchain implementation for secure data handling in Internet of Medical Things. J. Reliab. Intell. Environ. (2021). doi:10.1007/s40860-021-00153-2

Bigini, G., Freschi, V. & Lattanzi, E. A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision. Futur. Internet 12, 1–16 (2020).

Jeong, S., Shen, J.-H. J. & Ahn, B. A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain. Wirel. Commun. Mob. Comput. 2021, (2021).

Sadawi, A. A., Hassan, M. S. & Ndiaye, M. A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges. IEEE Access 9, 54478–54497 (2021).

Ratta, P., Kaur, A., Sharma, S., Shabaz, M. & Dhiman, G. Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives. J. Food Qual. 2021, (2021).

Mohammad Hossein, K., Esmaeili, M. E., Dargahi, T., Khonsari, A. & Conti, M. BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. Comput. Commun. 180, 31–47 (2021).

Ray, P. P., Chowhan, B., Kumar, N. & Almogren, A. BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem. IEEE Internet Things J. 8, 10857–10872 (2021).

Indumathi, J. et al. Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6HCS). IEEE Access 8, 216856–216872 (2020).

Mehbodniya, A. et al. Blockchain and IPFS Integrated Framework in Bilevel Fog-Cloud Network for Security and Privacy of IoMT Devices. Comput. Math. Methods Med. 2021, (2021).

Wang, W. et al. Blockchain and PUF-based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. IEEE Internet Things J. (2021). doi:10.1109/JIOT.2021.3117762

Gao, Y., Lin, H., Chen, Y. & Liu, Y. Blockchain and SGX-Enabled Edge-Computing-Empowered Secure IoMT Data Analysis. IEEE Internet Things J. 8, 15785–15795 (2021).

Wang, S., Wu, G., Ning, Z. & Li, J. Blockchain Enabled Privacy Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things. IEEE Internet Things J. (2021). doi:10.1109/JIOT.2021.3138104

Ray, P. P., Dash, D., Salah, K. & Kumar, N. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. IEEE Syst. J. 15, 85–94 (2021).

Akkaoui, R. Blockchain for the Management of Internet of Things Devices in the Medical Industry. IEEE Trans. Eng. Manag. (2021). doi:10.1109/TEM.2021.3097117

Uddin, M. A., Stranieri, A., Gondal, I. & Balasubramanian, V. Blockchain leveraged decentralized IoT eHealth framework. Internet of Things (Netherlands) 9, 100159 (2020).

ElRahman, S. A. & Alluhaidan, A. S. Blockchain technology and IoT-edge framework for sharing healthcare services. Soft Comput. 25, 13753–13777 (2021).

Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R. & Woźniak, M. Blockchain technology for secured healthcare data communication among the non-terminal nodes in iot architecture in 5g network. Electron. 10, (2021).

Almagrabi, A. O., Ali, R., Alghazzawi, D., AlBarakati, A. & Khurshaid, T. Blockchain-as-a-Utility for Next-Generation Healthcare Internet of Things. Comput. Mater. Contin. 68, 359–376 (2021).

Wang, W. et al. Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment. J. Syst. Archit. 115, (2021).

Abbas, A. et al. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Pers. Ubiquitous Comput. (2021). doi:10.1007/s00779-021-01583-8

Chen, F. et al. Blockchain-Based Efficient Device Authentication Protocol for Medical Cyber-Physical Systems. Secur. Commun. Networks 2021, (2021).

Wu, J. et al. Blockchain-based Privacy-Aware Contextual Online Learning for Collabrative Edge-Cloud-Enabled Nursing System in Internet of Things. IEEE Internet Things J. (2021). doi:10.1109/JIOT.2021.3133653

Shynu, P. G., Menon, V. G., Kumar, R. L., Kadry, S. & Nam, Y. Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing. IEEE Access 9, 45706–45720 (2021).

Ngabo, D. et al. Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. Electron. 10, (2021).

Laxmi Lydia, E. et al. Cognitive computing-based COVID-19 detection on Internet of things-enabled edge computing environment. Soft Comput. 6, (2021).

Lakhan, A. et al. Cost-efficient service selection and execution and blockchain-enabled serverless network for internet of medical things. Math. Biosci. Eng. 18, 7344–7362 (2021).

Elsayeh, M., Ezzat, K. A., El-Nashar, H. & Omran, L. N. Cybersecurity architecture for the internet of medical things and connected devices using blockchain. Biomed. Eng. - Appl. Basis Commun. 33, (2021).

Son, S. et al. Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain. IEEE Access 8, 192177–192191 (2020).

Sharmila, A. H. & Jaisankar, N. Edge Intelligent Agent Assisted Hybrid Hierarchical Blockchain for continuous healthcare monitoring & recommendation system in 5G WBAN-IoT. Comput. Networks 200, (2021).

Christo, M. S. et al. Ensuring Improved Security in Medical Data Using ECC and Blockchain Technology with Edge Devices. Secur. Commun. Networks 2021, (2021).

Mayer, A. H. et al. FogChain: A Fog Computing Architecture Integrating Blockchain and Internet of Things for Personal Health Records. IEEE Access 9, 122723–122737 (2021).

Egala, B. S., Pradhan, A. K., Badarla, V. & Mohanty, S. P. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control. IEEE Internet Things J. 8, 11717–11731 (2021).

Al-Jaroodi, J., Mohamed, N. & Abukhousa, E. Health 4.0: On the Way to Realizing the Healthcare of the Future. IEEE Access 8, 211189–211210 (2020).

Shukla, S., Thakur, S., Hussain, S., Breslin, J. G. & Jameel, S. M. Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model. Internet of Things (Netherlands) 15, (2021).

Hameed, K. et al. Integration of 5G and block-chain technologies in smart telemedicine using IoT. J. Healthc. Eng. 2021, (2021).

Xie, Y. et al. Integration of Artificial Intelligence, Blockchain, and Wearable Technology for Chronic Disease Management: A New Paradigm in Smart Healthcare. Curr. Med. Sci. 41, 1123–1133 (2021).

Nguyen, D. C., Pathirana, P. N., Ding, M. & Seneviratne, A. Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges. IEEE Commun. Surv. Tutorials 22, 2521–2549 (2020).

Elhoseny, M. et al. Iot solution for ai-enabled privacy-preserving with big data transferring: An application for healthcare using blockchain. Energies 14, (2021).

Arul, R. et al. IoT-enabled healthcare systems using block chain-dependent adaptable services. Pers. Ubiquitous Comput. (2021). doi:10.1007/s00779-021-01584-7

Abdellatif, A. A. et al. MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange. IEEE Internet Things J. 8, 15762–15775 (2021).

Arul, R. et al. Multi-modal secure healthcare data dissemination framework using blockchain in IoMT. Pers. Ubiquitous Comput. (2021). doi:10.1007/s00779-021-01527-2

Tomaz, A. E. B., Nascimento, J. C. Do, Hafid, A. S. & Souza, J. N. De. Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. IEEE Access 8, 204441–204458 (2020).

Otoum, S., Al Ridhawi, I. & Mouftah, H. T. Preventing and Controlling Epidemics through Blockchain-Assisted AI-Enabled Networks. IEEE Netw. 35, 34–41 (2021).

Alsahli, M. A., Alsanad, A., Hassan, M. M. & Gumaei, A. Privacy Preservation of User Identity in Contact Tracing for COVID-19-Like Pandemics Using Edge Computing. IEEE Access 9, 125065–125079 (2021).

Lin, H. et al. Privacy-Enhanced Data Fusion for COVID-19 Applications in Intelligent Internet of Medical Things. IEEE Internet Things J. 8, 15683–15693 (2021).

Bera, B., Mitra, A., Das, A. K., Puthal, D. & Park, Y. Private Blockchain-Based AI-Envisioned Home Monitoring Framework in IoMT-Enabled COVID-19 Environment. IEEE Consum. Electron. Mag. (2021). doi:10.1109/MCE.2021.3137104

Krishnamoorthy, S., Dua, A. & Gupta, S. Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions. J. Ambient Intell. Humaniz. Comput. (2021). doi:10.1007/s12652-021-03302-w

Rini, P. L. Secure and privacy based home patient monitoring internet of things (HPMIoT). Adv. Parallel Comput. 39, 55–62 (2021).

Rahman, M. A., Shamim Hossain, M., Islam, M. S., Alrajeh, N. A. & Muhammad, G. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. IEEE Access 8, 205071–205087 (2020).

Nguyen, G. N. et al. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. J. Parallel Distrib. Comput. 153, 150–160 (2021).

Wang, Y., Zhang, A., Zhang, P., Qu, Y. & Yu, S. Security-Aware and Privacy-Preserving Personal Health Record Sharing using Consortium Blockchain. IEEE Internet Things J. (2021). doi:10.1109/JIOT.2021.3132780

Aggarwal, S. et al. Smart-contract aware ethereum and client-fog-cloud healthcare system. Sensors 21, 483–493 (2021).

Barka, E., Dahmane, S., Kerrache, C. A., Khayat, M. & Sallabi, F. Sthm: A secured and trusted healthcare monitoring architecture using sdn and blockchain. Electron. 10, (2021).

Al-Khazaali, A. A. T. & Kurnaz, S. Study of integration of block chain and Internet of Things (IoT): an opportunity, challenges, and applications as medical sector and healthcare. Appl. Nanosci. (2021). doi:10.1007/s13204-021-02070-5

Kumar, R. & Tripathi, R. Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. J. Supercomput. 77, 7916–7955 (2021).

Santos, J. A., Inácio, P. R. M. & Silva, B. M. C. Towards the Use of Blockchain in Mobile Health Services and Applications. J. Med. Syst. 45, (2021).