VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belagavi – 590018

A TECHNICAL SEMINAR REPORT

ON

"Blockchain Technology in Healthcare"

A Dissertation Submitted in partial fulfillment of the requirement for the degree of

BACHELOR OF ENGINEERING

In

COMPUTER SCIENCE & ENGINEERING

Submitted by

MOHAMMED WAQAR (1RG17CS032)

Under The Guidance of

Mrs. Deepti

Asst Professor, Dept of CSE

RGIT, Bengaluru city – 32

Department of Computer Science & Engineering

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

Cholanagar, R.T. Nagar Post, Bengaluru-560032

2021 – 2022

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

(Affiliated to Visvesvaraya Technological University)
Cholanagar, R.T. Nagar Post, Bengaluru-560032

Department of Computer Science & Engineering

CERTIFICATE

This is to certify that the Seminar Report titled **"Blockchain Technology in Healthcare"** is a bona fide work carried out by **Mr. Mohammed Waqar (1RG17CS032)** in partial fulfillment for the award of **Bachelor of Engineering** in **Computer Science and Engineering** under **Visvesvaraya Technological University, Belagavi**, during the year **2021-2022.** It is certified that all corrections/suggestions given for Internal Assessment have been incorporated in the report. This technical seminar report has been approved as it satisfies the academic requirements in respect of technical seminar (17CSS86) work prescribed for the said degree.

Signature of Guide
Mrs. Deepti
Asst. Professor
Dept. of CSE,
RGIT, Bengaluru

Signature of HOD
Mrs. Arudra A
Asst. Professor
Dept. of CSE,
RGIT, Bengaluru

External Evaluation

Name of the Examiners **Signature with date**

1.

2.

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belagavi – 590018

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DECLARATION

I hereby declare that the technical seminar report entitled **"Blockchain Technology in Healthcare"** submitted to the **Visvesvaraya Technological University, Belagavi** during the academic year **2021- 2022**, is record of an original work done by me under the guidance of **Mrs. Deepti,** Asst Professor, Department of Computer Science and Engineering, RGIT, Bengaluru in the partial fulfillment of requirements for the award of the degree of **Bachelor of Engineering** in **Computer Science & Engineering.** The results embodied in this technical seminar report have not been submitted to any other University or Institute for award of any degree or diploma.

MOHAMMED WAQAR (1RG17CS032)

ACKNOWLEDGEMENT

I take this opportunity to thank my college **Rajiv Gandhi Institute of Technology, Bengaluru** for providing me with an opportunity to carry out this seminar work.

I extend my sincere regards and thanks to **Dr. Nagaraj A M**, Principal, RGIT, Bengaluru and to **Mrs. Arudra A**, Associate Professor and Head, Department of Computer Science and Engineering, RGIT, Bengaluru, for being a pillar of support and encouraging me in the face of all adversities.

I would like to acknowledge the thorough guidance and support extended towards us by **Mrs. Deepti**, Assistant Professor, Dept of CSE, RGIT, Bengaluru. Their incessant encouragement and valuable technical support have been of immense help. Their guidance gave me the environment to enhance my knowledge and skills and to reach the pinnacle with sheer determination, dedication and hard work.

I also want to extend my thanks to the entire faculty and support staff of the Department of Computer Science and Engineering, RGIT, Bengaluru, who have encouraged me throughout the course of the Bachelor's Degree.

I want to thank my family for always being there with full support and for providing me with a safe haven to conduct and complete my technical seminar. I will ever grateful to them for helping me in these stressful times.

Lastly, I want to acknowledge all the helpful insights given to me by all my friends during the course of this technical seminar.

MOHAMMED WAQAR (1RG17CS032)

ABSTRACT

Since blockchain was introduced through Bitcoin, research has been ongoing to extend its applications to non-financial use cases. Healthcare is one industry in which blockchain is expected to have significant impacts. Research in this area is relatively new but growing rapidly; so, health informatics researchers and practitioners are always struggling to keep pace with research progress in this area. This paper reports on a systematic review of the ongoing research in the application of blockchain technology in healthcare. The research methodology is based on the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines and a systematic mapping study process, in which a well-designed search protocol is used to search four scientific databases, to identify, extract and analyze all relevant publications. The review shows that a number of studies have proposed different use cases for the application of blockchain in healthcare; however, there is a lack of adequate prototype implementations and studies to characterize the effectiveness of these proposed use cases. The review further highlights the state-of-the-art in the development of blockchain applications for healthcare, their limitations and the areas for future research. To this end, therefore, there is still the need for more research to better understand, characterize and evaluate the utility of blockchain in healthcare.

CONTENTS

INTRODUCTION

CHAPTER 1 INTRODUCTION

Blockchain gained popularity as a distributed ledger technology following the Bitcoin white paper published in October, 2008 . As the underlying technology for Bitcoin, the main utility of blockchain is that it makes possible the exchange of electronic coins among participants in a distributed network without the need for a centralized, trusted third party. Transactions involving the exchange of electronic currencies between persons or companies have traditionally relied on a trusted third party (TTP), such as a bank, as a mediator. The reliance on a TTP is not desirable for a number of reasons. A trusted third party may malfunction, fail or be compromised maliciously to render the financial system unavailable or insecure; thus, a TTP undermines a system potentially as a single point of failure. A TTP also charges transaction fees and adds some transaction delays. The motivation behind Bitcoins is, therefore, to overcome these limitations associated with the reliance on TTP in electronic transactions.

A year after the publication of the famous white paper on Bitcoin, the Bitcoin cryptocurrency was implemented, with the code released as open-source, which made it possible for others to modify the code and improve on it to create different generations of blockchain-based technologies. The first implementations of blockchain-based cryptocurrencies, such as the Bitcoin, constitute the first generation of blockchain technology, which is also referred to as blockchain 1.0 .

Other blockchain 1.0 technologies include Monero , Dash and Litecoin, to name a few. The second generation of blockchain technology (blockchain 2.0) is associated with the introduction of smart properties and smart contracts. The smart properties are those digital properties or assets whose ownership can be controlled by a blockchain-based platform, while the smart contracts are the software programs that encode the rules of how the smart properties are controlled and managed. Examples of blockchain 2.0 cryptocurrencies include Ethereum, Ethereum Classic, NEO and QTUM .

Building on the above, the third generation of blockchain technology (blockchain 3.0) is now concerned with the non-financial applications of blockchain. To this end, efforts have been made to adapt the technology to other application areas, outside finance, so that other industries and use cases can benefit from the interesting features of blockchain. Consequently, blockchain is now considered as a general purpose technology that has found applications in different industries and use cases, such as identity management, dispute resolution, contract management, supply chain management, insurance and healthcare, to name a few.

With the growing fascination for blockchain and its adoption in different organizations and industries, healthcare has come to represent a significant area where a number of use cases have been identified for the application of blockchain. However, blockchain being a relatively new technology and with a lot of hype in the press as well as in grey publications in the form of opinion pieces, commentaries, blog posts, interviews, etc, there is a lot of inaccurate information, speculations and uncertainties about the potential utility of blockchain in the healthcare industry. Members of the research community and practitioners would want to understand the specific areas of application or use cases of blockchain in the healthcare industry; and of these identified use cases, what blockchain-based healthcare applications have been developed, What are the challenges and limitations of the blockchain-based healthcare applications, how are these challenges currently being addressed and what are the areas for improvement.

This Seminar reports on the systematic review that is conducted to address the above questions. While there exist some interesting reviews in the literature that are related to this topic.ours is different in terms of the methodology and the objectives. In the review conducted, they identify some examples of the application of blockchain technology in healthcare. These include the Guardtime, a firm which operates a blockchain-based healthcare platform for the validation of patients' identities for the citizens of Estonia; and the MedRec project, which was created to facilitate the management of permissions, authorization and data sharing between healthcare entities. Similarly, Engelhardt outlines a collection of 'noteworthy' examples of blockchain technology companies in the healthcare sector. These companies are grouped under different healthcare use cases, namely; prescription drug fraud detection, patient-centered medical records and the dental industry. This review is equally similar to the one conducted by Mettler where he reports some examples of blockchain-based applications and companies in the areas of public health management, medical research and drug counterfeiting in the pharmaceutical industry. On their part, Ku et al, publishes the key benefits of blockchain when compared to traditional databases for healthcare applications. They go further to explain how these benefits can be harnessed to improve medical record management, enhance insurance claim processes, improve clinical research and advance healthcare data ledgers. Lastly, Roman-Belmonte et al, in their review cover the existing and potential applications of blockchain in different fields of medicine, which include the fields of legal medicine, health data analytics, biomedical research, electronic medical records, meaningful use, payment for medical services and so on.

Our approach departs from the ones adopted in the aforementioned reviews in that we follow the guidelines for systematic literature review and systematic mapping study process and the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) statement in conducting and reporting our review. Our systematic review is based on a well-designed research protocol that ensures a holistic and unbiased sampling of all the published peer-reviewed articles that are relevant to the subject matter.

Based on this protocol, we retrieve from reputable scientific databases the relevant articles which we classify and map into different categories to unravel the truestate of the ongoing research in the application of blockchain technology in healthcare. The resulting map from our research will be very valuable to practitioners and researchers in understanding the domain state-of-the-art and the areas for future research. To the best of our knowledge, this is the first literature review on the application of blockchain in healthcare that follows the systematic mapping study process. The systematic review conducted by Yli-Huumo et al. inspired our choice of this methodology; however, their review on the technical challenges of blockchain technology is unrelated to our topic, which is the application of blockchain in healthcare. The systematic review by Holbl et al.,is also similar, but ours differs markedly in scope.

It is also worth noting that the objective of this review is not just to identify the use cases or the examples of blockchain-based applications in healthcare, but also to understand the limitations and challenges for the blockchain-based healthcare applications as well as the current trends in terms of the technical approaches, methodologies and concepts employed in developing these applications (and in overcoming the limitations) in a view to unravel the areas for future research. Moreover, this review covers many new materials which had not been published at the time of the previous reviews. As noted earlier, the application of blockchain in healthcare is a relatively new paradigm which is growing rapidly, and as such, there are many new publications on the topic. To illustrate this point, 32 of the 65 selected papers for this study were published in 2018 whereas most of the existing reviews were published in 2017 or earlier.

Overview of Blockchain

The detailed technical underpinnings of the blockchain technology is outside the scope of this report. However, for the purpose of our discussion going forward, it is important to shed light on some blockchain concepts, features and terminologies that will foster the understanding of how blockchain is applied to solve healthcare problems.

Perhaps, the most obvious and outstanding benefit of blockchain is the fact that it removes the need for a centralized trusted third party in distributed applications. By making it possible for two or more parties to carry out transactions in a distributed environment without a centralized authority, blockchain overcomes the problem of single point of failure which a central authority would otherwise introduce. It also improves transaction speed, by removing the delay introduced by the central authority, and at the same time, it makes transactions cheaper since the transaction fees charged by the central authority is removed. In place of a central authority, blockchain uses a consensus mechanism to reconcile discrepancies between nodes in a distributed application. The difference between centralized and decentralized systems is illustrated in Figure1.

In Figure1a, there are multiple ledgers but all the records are held in one central place, in this case, the Regional Health Information Organization (RHIO). In essence, the RHIO maintains the state of the ledger. When there is a disagreement between two nodes about the "true state" of the ledger, the RHIO is consulted as the final arbiter to determine the "true state" of the ledger. On the contrary, in Figure1b, there is only one ledger, but all the nodes have a copy of the ledger and some level of access to its contents. To maintain the integrity of the ledger, the nodes must have a means to agree on the "true state" of the ledger, in the absence of a central authority. When the nodes agree on a particular "true state" of the ledger, it is referred to as consensus. The different ways in which consensus is achieved in blockchain will be explained in the remaining part of this Section.

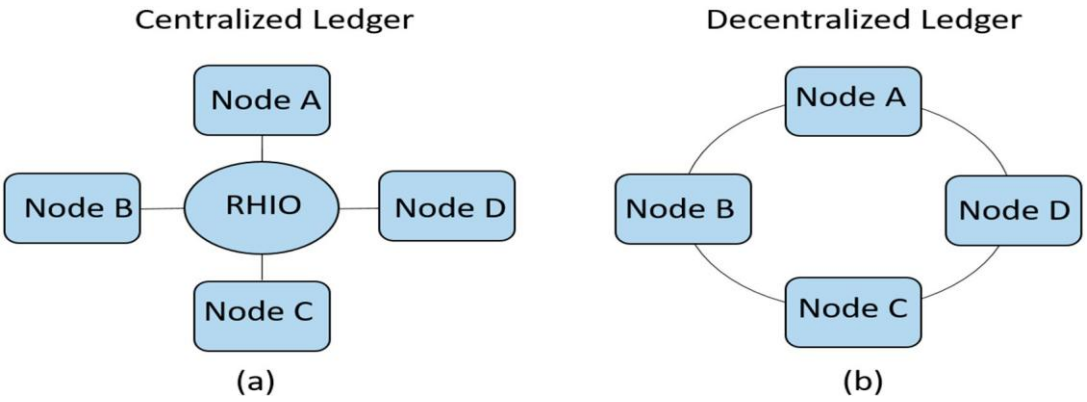

Figure 1. Centralized vs. decentralized system. In (**a**), there are multiple ledgers but all records are held in RHIO, whereas in (**b**), there is only one ledger but every node has some level of access to that ledger. The decentralized architecture removes the need for trusted third party, makes transactions faster, and removes the transaction fees charged by the trusted third party (RHIO).

At its very core, blockchain uses cryptographic primitives to derive most of its capabilities. Participants in a blockchain network are represented as nodes and each node uses public key infrastructure (PKI) to create and propose transactions. Each participant possesses a pair of public and private keys. The public key serves as the public address of the user while the private key is used to authenticate the user. When a transaction is created, it has to include the public key of the user who created the transaction, the public key of the receiver of the transaction and the transaction message. All of these are bundled together and cryptographically signed using the user's private key and subsequently broadcast to the other nodes in the blockchain network. When this is done, the user is said to have proposed a transaction.

A block is a collection of valid transaction proposals that are received within a period of time, say 10 min.A valid transaction proposal is one which satisfies the validation requirements. The process of validation ensures that the proposed transaction is legitimate, for example, that it originates from an authorized user (node). The consensus algorithm determines the order in which the validated blocks are appended to the ledger. There are special nodes in a blockchain network that are responsible for running the consensus algorithms (i.e., for validating transactions and determining the order in which transaction blocks are added to the blockchain). These special nodes are called miners and the process of validating transactions and ordering them in the blockchain is referred to as mining. Once a transaction proposal is received by a miner, the miner proceeds to check if the transaction is valid. Validated transactions are included into a block. After a period (or block) of time, the new block of validated transactions is linked (or chained) to the previous blocks, creating a chain of blocks, known as blockchain. The blockchain is replicated among all the nodes in the network, such that every node has an identical database or ledger of all the transactions in the network.

It is important to understand how blocks are chained to form the blockchain, but let us first explain the different types of blockchain. In some implementations of blockchain, e.g., Bitcoin, any node is free to join the network and to participate in the mining process (that is, take part in validating new blocks and chaining them to the existing ones). This sort of blockchain implementation in which any node is free to join the network and to participate as a miner without requiring any authorization or access permission is referred to as public or permissionless blockchain. In contrast, permissioned blockchain is one in which participants must be authorized and have the right access permissions before they can join and participate in the network. In permissioned blockchain, only certain nodes may be permitted to participate in the mining process. By virtue of their characteristics, permissioned blockchain networks are more likely to be smaller, faster and more secure than the public blockchain networks.

A permissioned blockchain may further be classified as a private or a consortium blockchain. The distinction between private and consortium blockchains is based on the number of nodes permitted to be miners. If only one node is permitted to be a miner, it is more aptly referred to as private blockchain. Note, however, that when only one node is the miner, then that node serves more or less as a central authority, in which case some of the advantages of decentralization is lost. Consortium blockchain is one in which two or more nodes are permitted to take part in the mining process, yet the blockchain network remains permissioned, in the sense that only authorized users can be part of the network. The consortium blockchain, therefore, has the advantages of decentralization as well as the improved security and privacy inherent in the private blockchain. More information about the different types of blockchain (public, permissioned: private and consortium) can be found in.

Let us get back to how blocks are chained to form a blockchain. The chaining of blocks is achieved through another cryptographic primitive which involves the use of hash functions. A hash function takes a message of arbitrary length and crunches it into a hash output of a fixed length, referred to as a message digest or a digital fingerprint. An interesting property of hash function is that it is collision-resistant, i.e., no two different messages will produce the same hash output. This property is the basis of block chaining. To chain a new block to the blockchain, the hash of the previous block header is included in the new block header. Thus, the last block in the blockchain contains the fingerprint of the transactions in the previous block, which in turn contains the fingerprint of the transactions in the preceding block and so on (Figure2).

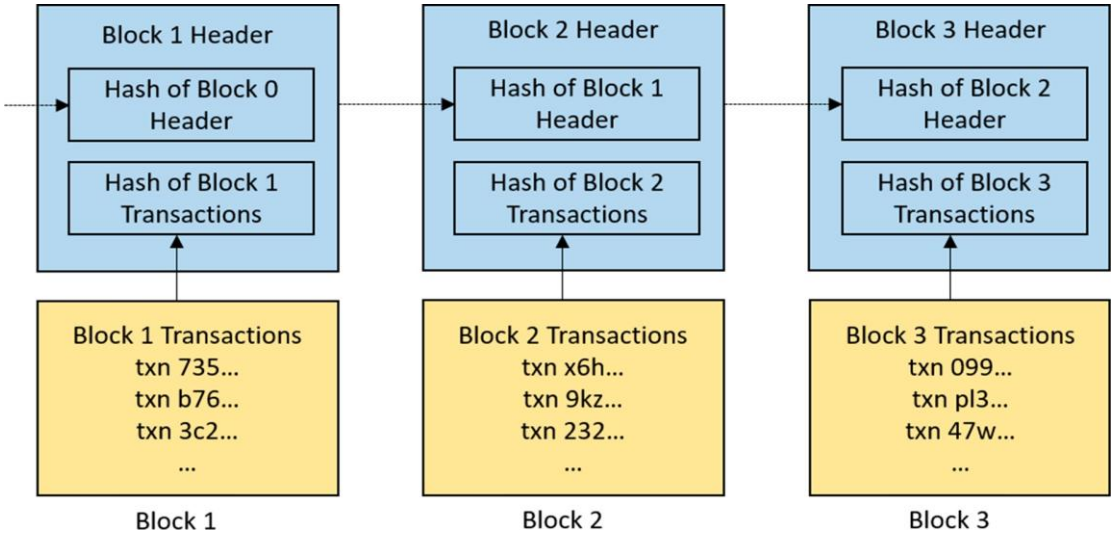

Figure 2. A simplified example of how blocks are chained to form a blockchain. Notice that each block contains a header and a number of transactions. The transactions in a block are hashed to generate a fixed-length hash output which is added to the block header. After the creation of the first block, every subsequent valid block must contain the hash output of the previous block header. The hash of the previous block header which is contained in every block serves as the chain that links every valid block to the ones before it. Thus, by linking every block to the previous blocks, a chain of blocks (blockchain) is established.

As depicted in the diagram in Figure2, if any of the transactions in a block is changed, even if slightly, the corresponding hash output will change drastically, which will break the chain to the subsequent blocks in the blockchain. Therefore, any alteration to the contents of a block in the blockchain is easily detected in the network. For this reason, once a transaction is added to a block and chained to the blockchain, that transaction cannot be altered or undone. Thus, information on the blockchain are said to be immutable. Immutability is an important property of blockchain which ensures that records, once created, cannot be retrieved or modified. To update a record on the blockchain, a new record must be created, hence, blockchain is also said to be an append-only ledger. The process of chaining blocks to the blockchain also ensures that the transactions are time-stamped,

As explained previously, the approaches to mining and reaching consensus differ across the different types of blockchain. In public blockchain, such as Bitcoin, there are usually more than one miner in the blockchain network, with the miners potentially receiving the transaction proposals in varying order, so it is possible that different miners will produce different valid blocks in which the ordering of transactions are different. In order for every node to have an identical copy of the blockchain, miners in the network must agree on the order in which the validated blocks are appended to the blockchain. In other words, only one of the miners is allowed to append a valid block per cycle. This can be done in different ways according to the consensus protocol in use. A popular example of a consensus protocol is the Proof of Work (PoW) used in Bitcoin.

Proof of Work (PoW) is a protocol based also on cryptographic hash function, in which the miners are required to solve a computationally difficult problem to determine the miner whose block is accepted to be added to the blockchain. In PoW protocol, a predetermined pattern of digital fingerprint is given, and the miners are required to find a random number which can be added to the transaction messages and hashed together to produce an identical pattern to the one given. In each cycle, the first miner to finish solving the mathematical problem is allowed to add a block to the blockchain. There are other examples of consensus protocols in the wild but their main purpose is the same, which is to ensure a consistent "true state" of the ledgers in the distributed nodes, without relying on a centralized trusted third party.

From the foregoing, blockchain can be defined as an immutable ledger or database, shared by peers in a network, in which records of events or transactions are appended in a chronological order. Evidently, blockchain embodies some interesting features that are beneficial to healthcare applications. One important feature of blockchain that is clearly beneficial to healthcare applications is decentralization which makes it possible to implement distributed healthcare applications that do not rely on a centralized authority. Additionally, the fact that the information in the blockchain is replicated among all the nodes in the network creates an atmosphere of transparency and openess, allowing healthcare stakeholders, and in particular the patients, to know how their data is used, by whom, when and how. More importantly, compromising any one node in the blockchain network does not affect the state of the ledger since the information in the ledger is replicated among multiple nodes in the network. Therefore, by its nature, blockchain can protect healthcare data from potential data loss, corruption or security attacks, such as the ransomware attack.

In addition, the immutability property of blockchain which makes it impossible to alter or modify any record that has been appended to the blockchain aligns very well with the requirements for storing healthcare records—it is very important to ensure the integrity and validity of patients' health records. What is more, the use of cryptographic algorithms to encrypt the data stored on the blockchain ensures that only the users who have legitimate permissions to access the data can decrypt them, thereby improving the data security and privacy. Furthermore, since the identities of the patients in a blockchain are pseudonymized through the use of cryptographic keys, the health data of patients may be shared among healthcare stakeholders without revealing the identities of the patients. Blockchain also supports smart contracts that can be used to program the rules that allow the patients to be in control of how their health records are shared or used. This is particularly relevant to the European General Data Protection Regulation (GDPR) which prohibits the processing of sensitive personal data of patients unless explicit consent is given, or specific conditions are met.Therefore, blockchain can facilitate the development of a GPDR-compliant EMR management system, by encoding in the smart contract a set of rules that ensure that patients' sensitive data cannot be shared or used without appropriate authorizations. The potential benefits of blockchain to healthcare applications are summed up in Table1.

Table 1. Benefits of blockchain to healthcare applications.

Decentralization	The very nature of healthcare, in which there are distributed stakeholders, requires a decentralized management system. Blockchain can become that decentralized health data management backbone from where all the stakeholders can have controlled access to the same health records, without any one playing the role of a central authority over the global health data.
Improved data security and privacy	The immutability property of blockchain greatly improves the security of the health data stored on it, since the data, once saved to the blockchain cannot be corrupted, altered or retrieved. All the health data on blockchain are encrypted, time-stamped and appended in a chronological order. Additionally, health data are saved on blockchain using cryptographic keys which help to protect the identity or the privacy of the patients.
Health data ownership	Patients need to own their data and be in control of how their data is used. Patients need the assurance that their health data are not misused by other stakeholders and should have a means to detect when such misuse occurs. Blockchain helps to meet these requirements through strong cryptographic protocols and well-defined smart contracts.
Availability/robustness	Since the records on blockchain are replicated in multiple nodes, the availability of the health data stored on blockchain is guaranteed as the system is robust and resilient against data losses, data corruption and some security attacks on data availability.
Transparency and trust	Blockchain, through its open and transparent nature, creates an atmosphere of trust around distributed healthcare applications. This facilitates the acceptance of such applications by the healthcare stakeholders.
Data verifiability	Even without accessing the plaintext of the records stored on blockchain, the integrity and validity of those records can be verified. This feature is very useful in areas of healthcare where verification of records is a requirement, such as pharmaceutical supply chain management and insurance claim processing.

Research Methodology

In conducting and reporting this seminar,I adopted the guidelines for systematic literature review and the process for systematic mapping study ,as well as the guidelines described in the PRISMA statement. As explained in, the goal of a systematic mapping study is to get an overview of the research area, and to complement this by investigating the state of evidence in specific topics. In this case, the results of the mapping study would help us to identify and map the blockchain use cases in healthcare, and to understand the extent to which blockchain-based applications have been developed in relation to the identified use cases. They would also help us to identify areas of possible research gaps. The systematic review would again enable us to investigate the current trends in terms of the technical approaches, methodologies and concepts employed in developing blockchain-based healthcare applications. In what follows, we go through the systematic mapping process as shown in Figure3.

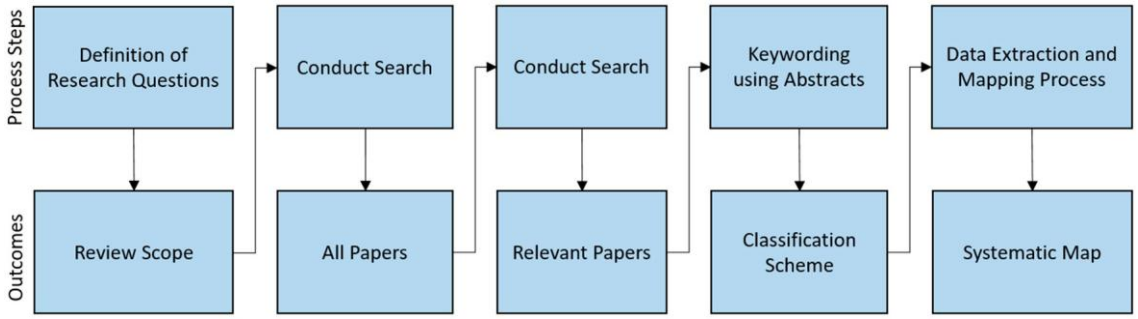

Figure 3. The systematic mapping process steps.

1.1. Definition of Research Questions

As the first process step in the systematic mapping study, we defined the following four research questions in line with our objective which is to unravel the state-of-the-art in research on the application of blockchain technology in healthcare.

1.1.1. What Are the Use Cases of Blockchain in Healthcare?

The primary question in this research is to understand the different areas of healthcare that blockchain has been shown to find application. By reviewing the relevant articles from scientific databases, we are be able to identify what healthcare problems that blockchain can solve, and by so doing, isolate those problems which are better solved using other techniques. Given the frenzy in the media in which a lot of problems are deemed solvable by blockchain, a map of problem domains in healthcare in which blockchains are applicable will help researchers and practitioners to focus their interest on those promising areas of blockchain application in the industry.

1.1.2. Of the Identified Use Cases, What Blockchain-Based Applications Have Been Developed?

Many areas of application of blockchain have been proposed in scientific literature. However, not all of these proposals have been translated into working prototypes. It is therefore important to understand the extent of real-world implementations of blockchain-based healthcare applications in relation to the identified use cases. This will help to highlight areas where there are research gaps and the need to shift research focus to these areas.

1.1.3. What Are the Challenges and Limitations of the Blockchain-Based Applications?

This question seeks to understand the challenges facing the implementations of blockchain-based healthcare applications. Based on the prototype applications that have been developed, what are the limitations of this new technology in meeting the expected goals of solving healthcare-related problems?

1.1.4. How Are These Challenges and Limitations Currently Being Addressed?

This research question seeks to understand the approaches taken to develop blockchain-based healthcare applications with a view to guiding future projects, so that there will be no need to reinvent the wheels. Since the first blockchain implementation in Bitcoin cryptocurrency, several modifications and improvements have been made to the technology to make it adaptable to non-financial use cases. This research question looks at the current trends in terms of the technical approaches and methodologies that are employed in developing blockchain-based applications for healthcare.

1.1.5. What Are the Open Research Issues and the Areas for Future Research?

The last question addresses the issues for future research. Identifying research gaps and the challenges in the field will help researchers to streamline their future research to focus on addressing these research gaps and challenges.

Electronic Medical Record (EMR)

One of the popular use cases of blockchain in healthcare is the management of electronic medical records (EMRs). EMRs, which are sometimes used interchangeably with electronic health records (EHRs) or personal health records (PHRs), have to do with the electronic creation, storage and management of patients' personal, medical or health-related data. Indeed, EMR use case of blockchain is a major research topic in the literature, with 48% (32) of the 65 selected papers addressing the topic. Blockchain's property of decentralization, immutability, data provenance, reliability, robustness, the smart contracts, security and privacy are being canvassed as the features that make it very suitable for storage and management of patients' electronic medical records (EMR). Some of the papers are focused on how to facilitate patient-centric data sharing among different healthcare stakeholders, such as providers, researchers and insurers. Consistent with the European General Data Protection Regulation (GDPR) which prohibits the processing of sensitive personal data of patients unless explicit consent is given by the patients, blockchain is widely proposed as a viable technology to build the healthcare platform that can empower patients to be in control of how their data are shared, processed or used.

Guardtime, a company that uses a blockchain-based platform to secure over 1 million patients records in Estonia is cited in other reviews as a popular example of the use of blockchain for the management of EMR, another such example is the MedRec project, a project of MIT Media Lab and Beth Israel Deaconess Medical Center, which aims at giving patients agency over their own data, to determine who can access them, through some fine-grained access permissions built on blockchain. The Gem Health Network (GHN) is yet another example, which is developed by the US startup, Gem, using the Ethereum blockchain platform. GHN allows different healthcare practitioners to have shared access to the same data, Healthbank, a Swiss digital health company, is similarly working on empowering patients to be in full control of their data using blockchain platform, the author discusses the Medicalchain project, whose blockchain-based platform will facilitate the sharing of patients' medical records across international healthcare institutions, and the Healthcoin initiative, which aims at constructing a global EMR system. Other players working on different initiatives and projects based on blockchain-enabled patient-centric EMR include Factom, HealthCombix, Patientory, SimplyVital, IBM's Watson, BurstIQ, Bowhead, QBRICS and Nuco .

Some of the barriers to blockchain-enabled patient-centric electronic medical records include interoperability among disparate blockchain-based EMR solutions (because of lack of standards), scalability (high volume of clinical data), patient engagement (not all patients are willing and able to manage their own data), data security and privacy, and lack of incentives.

Some workarounds have been proposed to tackle some of these challenges. For example, as a countermeasure to the challenge of scalability, given the large volume of clinical data involved, the trend is to store the actual healthcare data on the cloud and store only the pointers to the data on blockchain, along with their fingerprints. A good number of the technical papers report on the implementation of blockchain-based EMR applications in which different approaches are adopted to address these challenges. Yet, some publications propose different solutions to improve the security and privacy of the EMR data on blockchain.

HealthChain is an EMR application developed as a permissioned, private blockchain network using the IBM Blockchain's Hyperledger Fabric and deployed on Bluemix. The modular architecture of Hyperledger Fabric enables HealthChain to achieve health data confidentiality, scalability and security. HealthChain also incorporates chaincodes (smart contracts) that control authorizations and access privileges on the blockchain network. There is also another blockchain-based framework, Ancile , which similarly utilizes smart contracts, but is built on Etherum blockchain platform to achieve access control, data security, privacy and interoperability of electronic medical records. MedRec earlier discussed) and the medical data preservation system (DPS) developed by Li et al. are two other examples of blockchain implementations of EMR that utilize the Ethereum blockchain platform. Other blockchain-based EMR applications include MedBlock [64], BlockHIE , FHIRChain and MeDShare.

In the area of security and privacy of the sensitive data stored on blockchain-based EMR, some cryptographic schemes are proposed to strengthen the security and validity of the EMRs stored on the blockchain. Hussein et al. propose a blockchain-based access control method to EMR that employs Discrete Wavelength Transform and Genetic Algorithm to enhance the security and optimize the performance of the system. An attribute-based signature scheme with multiple authorities is also proposed, in which the patient is able to endorse a message to be added to the blockchain based on attributes of the message, without disclosing any sensitive information. This protocol is shown to resist collusion attack and is demonstrated to be computationally secure. In a similar way, an attribute-based encryption (ABE), identity-based encryption (IBE) and identity-based signature (IBS) are proposed to be used with blockchain in , Other security-related proposals for blockchain-based EMR include the key management schemes by Zhao et al. Zhang and Poslad propose an architecture called GAA-FQ (Granular Access Authorization supporting Flexible Queries) which provides secure authorization at different levels of granularity without requiring public key infrastructure (PKI).

Shifting emphasis to privacy, Zhang and Lin propose a blockchain-based secure and privacy-preserving EMR scheme which uses private and consortium blockchains to store the actual EMR and the pointers to the EMR respectively. This scheme also relies on asymmetric encryption but also implements mechanisms for conformance testing to ensure the system's availability. In the authors propose a privacy-preserving platform, MediBchain that employs cryptographic functions to deidentify patients' data in blockchain-based EMR systems. Yeu et al. in also propose an architecture called Healthcare Data Gateway (HDG) for blockchain-based EMR application which allows patients to own, control and choose how to share their data in a privacy-preserving manner.

1.1.6. Drug/Pharmaceutical Supply Chain

One other identified use case of blockchain is in health supply chain management, particularly in the drug/pharmaceutical industry. The delivery of counterfeit or substandard medications can have dire consequences for the patients, yet this is a common problem faced in the pharmaceutical industry. Blockchain technology has been identified as having the capability to address this problem .

Engelhardt, in his survey, mentions some companies that are working on how blockchain can be used to detect prescription drug fraud. The companies mentioned include Nuco, HealthChainRx and Scalamed ,The general idea is to record every transaction relating to the prescription of drugs on the blokchain network to which all the stakeholders (manufacturers, distributors, doctors, patients and pharmacists) are connected. This way, any alteration or malicious modification of the prescription by any of the parties can be detected. Mettler also mentions the Counterfeit Medicines Project that is launched by Hyperledger (the developers of Hyperledger Fabric)to combat drug counterfeiting. Only one paper in this review presents an implementation of an example blockchain-based application for pharmaceutical supply chain management. Modum.io AG is a startup that uses blockchain to achieve data immutability while creating public accessibility of the temperature records of pharmaceutical products during their transportation so that their compliance to quality control temperature requirements can be verified ,Mackey and Nayyar, however, report that they found from grey literature many examples of prototypes and research initiatives related to the application of blockchain in the area of pharmaceutical supply chain management ,This indicates that industrial players may have released many commercialblockchain-based products to combat the fake medicine
trade even when there are still limited academic publications on the subject.

1.1.7. Biomedical Research and Education

Blockchain has an interesting use case in biomedical research and education. In clinical trials, blockchain can help to eliminate falsification of data and the under-reporting or exclusion of undesirable results of clinical research, makes it easier for patients to grant permission for their data to be used for clinical trials because of the anonymization that is inherently encoded in the data ,Additionally, the immutability property of blockchain certifies the integrity of data collected through blockchain for clinical study. The transparent and public nature of blockchain also make it easier to replicate research from blockchain-based data. All these are some of the reasons blockchain is expected to revolutionize biomedical research ,Blockchain has also been noted to have the potential to revolutionize the peer-review process for clinical research publications based on its decentralized, immutable and transparent properties ,Another potential application of blockchain to health professions education (HPE) is presented ,where Funk et al. make a case for using blockchain to build an HPE system that will be value-based, competency-based and offer credentialing services without relying on a third-party.

A proof of concept implementation of consent traceability in clinical trial using blockchain protocol is presented in ,Similarly, Nugent et al. present their research in which they demonstrate how smart contracts on Ethereum blockchain platform can be used to improve data transparency in clinical trials. The Ethereum platform is also used to implement another blockchain-based solution that is proposed to notarize documents retrieved from biomedical databases.

1.1.8. Remote Patient Monitoring (RPM)

In this Section, we look at how blockchain technology facilitates remote patient monitoring (RPM). Remote patient monitoring involves the collection of biomedical data through body area sensors (or IoT devices) and mobile devices to be able to remotely monitor the status of the patient outside.traditional healthcare environments such as the hospital. Blockchain has been proposed as a means for storing, sharing and retrieving the remotely-collected biomedical data .

In Griggs et al. demonstrate how smart contracts on the Ethereum blockchain platform can support real-time patient monitoring application with capability to provide automated interventions in a secure environment. Liang et al. present a Hyperledger-based implementation of blockchain-enabled data collection and sharing among healthcare stakeholders in a mobile healthcare environment. Similarly, blockchain is employed to develop SMEAD, mobile-enabled assisting device for monitoring diabetes patients Another example application is presented in where mobile devices (smartphones) were successfully used to transmit data to a blockchain-based application on Hyperledger Fabric. Ashraf Uddin et al. also developed a blockchain-based patient centric agent (PCA) to achieve end-to-end data security and privacy in a continuous remote patient monitoring application In the authors proposed to use practical swarm optimization (PSO) for root exploit detection and feature optimization in blockchain-based mobile device medical data management. Lastly, Ji et al. proposed a scheme known as BMPLS (Blockchain-based Multi-level Privacy-preserving Location Sharing) for realizing privacy-preserving location sharing for remote monitoring applications.

1.1.9. Health Insurance Claims

Insurance claims processing in healthcare can benefit from blockchain's transparency, decentralization, immutability and auditability of records stored on it A number of papers identify insurance claim processing as a very promising area for the application of blockchain in healthcareHowever, examples of prototype implementations of such systems are very limited. One good example we can find is the MIStore (a blockchain-based medical insurance storage system) which is deployed on the Ethereum blockchain platform Additionally, talks about an initiative by a company named Pokitdok that aims to partner with Intel to build a blockchain-based system that will facilitate insurance claim resolution in healthcare.

1.1.10. Others

There are other potential areas of application of blockchain in healthcare, including areas such as the dental industry, legal medicine and meaningful use but there are no papers in our review that address such use cases. On the contrary, there are two papers that cannot be classified under any of the identified use cases of blockchain, but they present relevant research perspectives. One sets out to identify the metrics for evaluating blockchain-based healthcare while the other studies the socio-technical implications of using blockchain technology in healthcare.

Discussion

1.2. What Are the Use Cases of Blockchain in Healthcare?

From the mapping study, the blockchain use cases in healthcare include the managements of electronic medical records (EMRs), pharmaceutical supply chain, biomedical research and education, remote patient monitoring (RPM), health insurance claims, health data analytics and other potential areas of healthcare applications.

Based on the selected papers, a substantial portion of the research (48%) concentrates on the application of blockchain in the management of electronic medical records. Traditionally, patients' records are stored separately in different databases across different service providers, with little or no interoperability. This leaves the control of the health data mostly in the hands of the service providers and also limits the collaborative sharing of such data among healthcare stakeholders. By applying blockchain to the management of EMRs, patients will be in control of their own health data and be able to decide how they are used. Data sharing between healthcare stakeholders will be easier, better controlled, transparent and trustworthy. However, using blockchain to store EMRs brings up concerns about the security and privacy of patients' sensitive information, an issue that a good portion of the research is also dedicated.

Some companies and research projects, such as Guardtime and MedRec have developed blockchain-based EMR applications. In addition, a number of the reviewed materials discuss the prototype implementations of different blockchain-based EMR applications

Similarly, blockchain use cases in pharmaceutical supply chain management, biomedical research/education and remote patient monitoring have received considerable research attention with example prototype implementations (see Table5). There is also one example implementation of prototype application relating to health insurance claim processing ,However, other use cases are still mostly at the conceptual level.

To identify the research trends as it concerns the identified use cases of blockchain in healthcare, the diagram of Figure11was extended as shown in Figure13to further highlight the number of papers published for the respective use cases from 2016 to 2018.

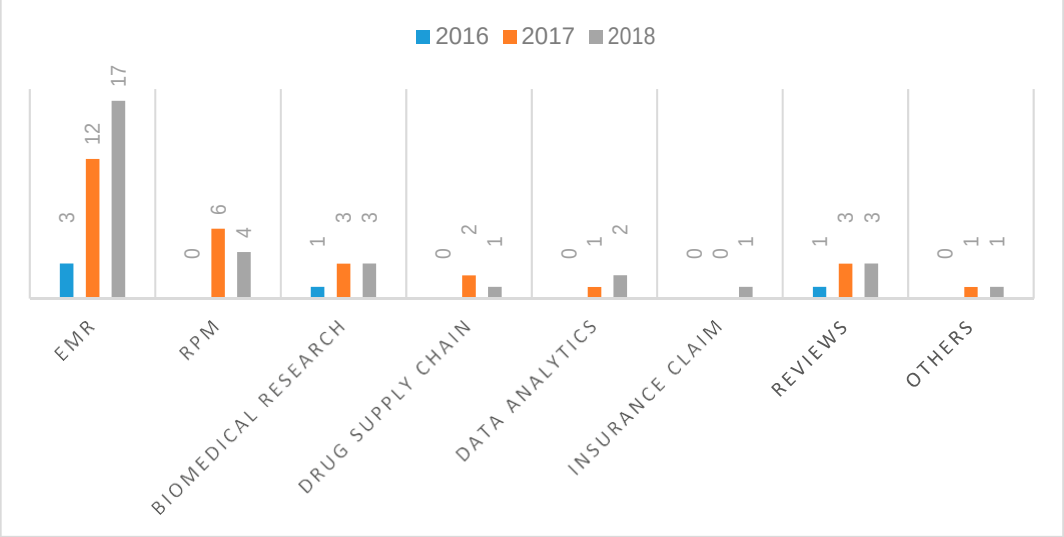

Figure 13. Classification of the selected papers showing publication trend from 2016 to 2018.

1.3. Of the Identified Use Cases, What Blockchain-Based Applications Have Been Developed?

In general, the technology is still maturing and even when prototype applications are developed, in some cases, they are just for experimental purposes with very basic functionalities. That said, there are papers that present implementation details of applications that have been developed for the various use cases.

For the EMR use case, example applications include the Healthchain which is developed on Hyperledger Fabric, Acile and MedRec both of which are developed on the Ethereum platform. Other examples include MedBlock BlockHIE FHIRChain and MeDShare ,Similarly, other blockchain use cases, such as the management of the drug/pharmaceutical supply chain, biomedical research and education, health insurance claim processing and remote patient monitoring have example use cases as discussed in Section4.2. There are, however, some potential use cases of blockchain that are still at the conceptual levels where prototypes have not yet been developed, such as the application of blockchain in legal medicine , Table5gives a summary of the blockchain use cases in healthcare and the corresponding examples of prototype applications that have been developed for the respective use cases.

It is also interesting to observe that most of these applications are developed on popular blockchain frameworks, such as Ethereum and Hyperledger Fabric as shown in Table6.

Table 6. Blockchain frameworks used in developing healthcare applications.

Frameworks	Example Applications
Ethereum	MedRec Ancile [34], DPS [46], GHN [15], FHIRChain [54], MedShare [68], SMEAD [79], Medium.io AG [47], MIStore [57,60,70,71]
Hyperledger Fabric	HealthChain [42], MedicalChain [40,61,62,81]
Bitcoin	[38]
Proprietary	Guardtime [13], MedBlock [64], BlockHIE [48,50]

1.4. What Are the Challenges and Limitations of the Blockchain-Based Applications?

Some identified challenges to the development of blockchain-based applications include interoperability, security and privacy, scalability, speed and patient engagement.

The interoperability challenge stems from the fact that there is not yet an existing standard for developing blockchain-based healthcare applications; therefore, applications developed by different vendors or on different platforms may not be able to interoperate. Consider, for example, the two remote patient monitoring applications, in which one is developed on the Ethereum platform while the other is developed on the Hyperledger Fabric platform (see Table6), it would be difficult to exchange information from one platform to the other.

With regards to the security and privacy of blockchain-based healthcare applications, there is a concern that despite the encryption techniques employed, it could still be possible to reveal the identity of a patient in a public blockchain by linking together sufficient data that are associated to that patient , In addition, there is also the potential risk of security breaches that could arise from intentional malicious attacks to the healthcare blockchain by criminal organizations or even government agencies that could compromise the privacy of the patients. There have been several cases of reported attacks on the blockchain networks that power different cryptocurrencies , The private keys that are used for data encryption and decryption in blockchain are also prone to potential compromise which could result in unauthorized access to the stored health data.

Furthermore, there is the concern that the immutability property of blockchain does not augur well with the GDPR's "right to be forgotten," which is part of the European Union General Data Protection Regulation which stipulates that the user has the right to request for the complete erasure of the user's data , Since the immutability of blockchain ensures that data once saved to the blockchain cannot be deleted or altered, it could prove counterproductive when it is desirable to completely wipe out the medical history of a patient.

Scalability of blockchain-based healthcare solutions is a major challenge especially in relation to the volume of data involved. It is not optimal, or even practicable in some cases, to store the high-volume biomedical data on blockchain as this is bound to cause serious performance degradation. There is also the problem of speed as the blockchain-based processing can introduce some significant

latency. For example, the validation mechanism in the current set-up of the Ethereum blockchain platform necessitates all the nodes in a network to participate in the validation process .This incurs considerable processing delay, especially if the data load is significant.

One more challenge is how to engage patients in the management of their data on blockchain. Patients, especially the elderly and the young, may not be interested or able to participate in the management of their health data.

1.5. How Are These Challenges and Limitations Currently Being Addressed?

Some workarounds are being proposed to circumvent some of the challenges and limitations posed by the application of blockchain in health IT (information technology) systems. For example, as a countermeasure to the problem of scalability, it is proposed to store the encrypted health data "off-chain," such that only some condensed information about the data and how they can be accessed are stored on the blockchain. This also takes care of the GDPR's "right to be forgotten" problem, since the actual health data stored off-chain can be permanently deleted, even if the pointer to the data on the blockchain cannot be deleted. However, this countermeasure has some limitations such as the fact that the redundancy that is built into blockchain, which enhances data availability, is partially lost.

To further secure the data and protect patients' privacy, permissioned blockchain such as the private or consortium blockchain is used instead of the permissionless, public blockchain for healthcare applications , In addition, by following rigorous software development process and applying all known security measures during code development, much of the security threats may be contained. In permissioned healthcare blockchains, controls are also put in place to be able to reverse fraudulent or invalid transactions [24]. With the blockchain-based smart contracts , different rules can be defined and programmed to control how the healthcare application behaves and how it handles the patients' data.

Furthermore, to improve the performance of the system and enhance the processing speed, only some nodes are permitted to participate in the consensus and validation processes ,This is in contrast to the protocols in public blockchain, such as Bitcoin, in which any node can take part in the consensus or validation process.

1.6. What Are the Open Research Issues and the Areas for Future Research?

As the blockchain technology application in healthcare is still an emerging field, there is need for researchers to develop more prototypes and proof-of-concepts to deepen the understanding and maturity of the technology in relation to its application in healthcare. Many of the proposed frameworks, concepts, models and architectures, such as , need to be implemented and tested to evaluate their strengths and weaknesses.

To guarantee interoperability between different blockchain products, there is need for open standards. Currently, the focus is on testing the functionality of blockchain prototypes for proof of concepts. However, for blockchain to be fully adopted and deployed in operational healthcare environments, open standards for interoperability need to be defined. It is therefore important that researchers start looking into the interoperability issues and the standardization processes. There is already a standards group (ISO/TC 307) to which researchers can send in their contributions .

The challenges of data security and privacy, interoperability, scalability and speed that characterize blockchain-based healthcare applications are all open research issues that require concerted further research engagements in order to improve stakeholders' confidence in the use of the technology and to foster its adoption in healthcare.

1.7. Limitations of the Study

Systematic mapping studies can be marred by publication or selection bias, errors in data extraction or miscalculations.

Publication bias arises from the tendency for researchers to publish more positive results than negative ones because positive results are more likely to be accepted for publication and also more likely to be cited by others. It is difficult to overcome publication bias from the perspective of the reviewers, however; we made efforts to address this by searching different but reputable scientific databases to retrieve as many relevant publications as possible. We were thus able to find many papers, and our chances of retrieving any publications with negative results were significantly enhanced. However, by searching only peer-reviewed articles and excluding grey literature in our search protocol, we stand a high chance of missing some important grey publications such as white papers from industries. We believe, however, that by using only scientific databases to search for peer-reviewed articles, we have more chances of retrieving high quality scientific publications.

Selection bias, on its part is more controllable by the reviewers since it has to do with the tendency to exclude some relevant publications in the analysis by using a flawed search protocol. In our case, we took the time to design a search protocol and our analysis showed that our search protocol was able to retrieve every relevant paper. In defining our inclusion and exclusion criteria, care was also taken to ensure that the selected papers would represent an unbiased sampling of all the papers that were relevant to our research. However, as earlier stated, the fact that we based our research only on peer-reviewed publications means that we were not able to access, for example, information published on company websites, discussion forums and other such related venues. Interestingly, we realize that most of the important information available in those grey literatures, like the different blockchain-based healthcare applications, has been synthesized and put into some peer-reviewed publications. For example, has a list of a number of important blockchain applications, some of which we are not able to retrieve directly by using our search protocol. Therefore, through such secondary publications, we were able to compensate for the information we may have missed by not searching the grey literature.

Errors in data extraction and miscalculations could stem from the inability of the reviewers to accurately and properly extract information and data from the selected papers. To address this limitation, we made use of a reference management software, Mendeley, to organize and manage all the papers we downloaded in relation to this study. We further employed Excel for recording and organizing the extracted data items, as well as for performing statistical analysis on the extracted data, while also being painstakingly meticulous and rigorous in our analysis to avoid introducing any human errors.

CONCLUSION

CONCLUSION

Blockchain technology has evolved from the time it was introduced to the world through Bitcoin into a general-purpose technology with use cases in many industries including healthcare. To understand the state-of-the-art of the application of blockchain technology in healthcare, we conducted a systematic review in which we created the map of all relevant research using the systematic mapping study process, Specifically, the objectives of the study were to identify the blockchain technology use cases in healthcare, the example applications that have been developed for these use cases, the challenges and limitations of the blockchain-based healthcare applications, the current approaches employed in developing these applications and areas for future research. Our search and paper selection protocol produced 65 papers which we analyzed to address the research questions.

Our study shows that blockchain has many healthcare use cases including the management of electronic medical records, drugs and pharmaceutical supply chain management, biomedical research and education, remote patient monitoring, health data analytics, among others. A number of blockchain-based healthcare applications have been developed as prototypes based on emerging blockchain paradigms, such as smart contracts, permissioned blockchain, off-chain storage, etc. However, more research still needs to be conducted to better understand, characterize and evaluate the utility of blockchain technology in healthcare. Further research is also needed to supplement ongoing efforts to address the challenges of scalability, latency, interoperability, security and privacy in relation to the use of blockchain technology in healthcare.

REFERENCES

REFERENCES

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online:www.bitcoin.org (accessed on 12 March 2019).
2. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015. [CrossRef]
3. The Monero Project. Available online:https://getmonero.org/the-monero-project/(accessed on 12 March 2019).
4. Dash Official Website|Dash Crypto Currency—Dash. Available online:https://www.dash.org/(accessed on 12 March 2019).
5. Litecoin—Open Source P2P Digital Currency. Available online:https://litecoin.org/(accessed on 12 March 2019).
6. Ethereum Project. Available online:https://www.ethereum.org/(accessed on 12 March 2019).
7. Ethereum Classic—A Smarter Blockchain that Takes Digital Assets Further 2018. Available online:https://ethereumclassic.org/(accessed on 12 March 2019).
8. NEO Smart Economy 2018. Available online:https://neo.org/(accessed on 12 March 2019). 9.Qtum. 2018. Available online:https://qtum.org/en(accessed on 12 March 2019).
10. Burniske, C.; Vaughn, E.; Cahana, A.; Shelton, J. *How Blockchain Technology Can Enhance Electronic Health Record Operability*; Ark Invest: New York, NY, USA, 2016.
11. Jovanovic, B.; Rousseau, P.L. General Purpose Technologies. In *Handbook of Economic Growth*; Elsevier: New York, NY, USA, 2005. [CrossRef]
12. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference*; EuroSys '18; Association for Computing Machinery: New York, NY, USA, 2018; pp. 30:1–30:15. [CrossRef]
13. Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain Technology Applications in Health Care.

    Circ. Cardiovasc. Qual. Outcomes **2017**, *10*, e003800. [CrossRef]
14. Engelhardt, M.A. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technol. Innov. Manag. Rev.* **2017**, *7*, 22–34. [CrossRef]
15. Mettler, M. Blockchain Technology in Healthcare the Revolution Starts Here. In Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 520–522. [CrossRef]
16. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef]
17. Roman-Belmonte, J.M.; De la Corte-Rodriguez, H.; Rodriguez-Merchan, E.C.C.; la Corte-Rodriguez, H.; Carlos Rodriguez-Merchan, E. How Blockchain Technology Can

Change Medicine. *Postgrad. Med.* **2018**, *130*, 420–427. [CrossRef] [PubMed]

18. Kitchenham, B.; Charters, S. Guidelines for Performing Systematic Literature Reviews in Software Engineering. *Engineering* **2007**, *2*, 1051. [CrossRef]

19. Petersen, K.; Feldt, R.; Mujtaba, S.; Mattsson, M. Systematic Mapping Studies in Software Engineering. In Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering, Bari, Italy, 26–27 June 2008; pp. 68–77. [CrossRef]

20. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; Altman, D.; Antes, G.; Atkins, D.; Barbour, V.; Barrowman, N.; Berlin, J.A.; et al. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Med.* **2009**, *6*. [CrossRef] [PubMed]

21. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology? A Systematic Review. *PLoS ONE* **2016**, *11*, 1–27. [CrossRef] [PubMed]

22. Hölbl, M.; Kompara, M.; Kamišalic´, A.; Zlatolas, L.N. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]

23. Housley, R. Public Key Infrastructure (PKI). In *The Internet Encyclopedia*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2004. [CrossRef]

24. Alhadhrami, Z.; Alghfeli, S.; Alghfeli, M.; Abedlla, J.A.; Shuaib, K. Introducing Blockchains for Healthcare. In Proceedings of the 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, UAE, 19–21 November 2017; pp. 1–4.

25. MccCarthy, J. MedStar Attack Found to Be Ransomware, Hackers Demand Bitcoin. 2016. Available online:https://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware- hackers-demand-bitcoin(accessed on 12 March 2019).

26. Patients and Privacy: GDPR Compliance for Healthcare Organizations—Security News—Trend Micro DK. Available online:https://www.trendmicro.com/vinfo/dk/security/news/online-privacy/patients-and-privacy-gdpr-compliance-for-healthcare-organizations(accessed on 12 March 2019).

27. Patel, V. A Framework for Secure and Decentralized Sharing of Medical Imaging Data via Blockchain Consensus. *Health Inform. J.* **2018**. [CrossRef]

28. Hussein, A.F.; ArunKumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Manuel, J.; Tavares, R.S.; Hugo, V.; De Albuquerque, C.; Tavares, J.M.R.S.; de Albuquerque, V.H.C. A Medical Records Managing and Securing Blockchain Based System Supported by a Genetic Algorithm and Discrete Wavelet Transform. *Cogn. Syst. Res.* **2018**, *52*, 1–11. [CrossRef]

29. Dey, T.; Jaiswal, S.; Sunderkrishnan, S.; Katre, N. A Medical Use Case of Internet of Things and Blockchain. In Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 7–8 December 2017; pp. 486–491. [CrossRef]

30. Kaur, H.; Alam, M.A.; Jameel, R.; Kumar Mourya, A.; Chang, V.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *J. Med. Syst.* **2018**, *42*, 156. [CrossRef] [PubMed]

31. Mackey, T.K.; Nayyar, G. A Review of Existing and Emerging Digital Technologies to Combat the Global Trade in Fake Medicines. *Expert Opin. Drug Saf.* **2017**, *16*, 587–602. [CrossRef] [PubMed]

32. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology? A Systematic Review. *PLoS ONE* **2016**, *11*, 1–27. [CrossRef] [PubMed]

33. Hölbl, M.; Kompara, M.; Kamišalic´, A.; Zlatolas, L.N. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]

34. Housley, R. Public Key Infrastructure (PKI). In *The Internet Encyclopedia*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2004. [CrossRef]

35. Alhadhrami, Z.; Alghfeli, S.; Alghfeli, M.; Abedlla, J.A.; Shuaib, K. Introducing Blockchains for Healthcare. In Proceedings of the 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, UAE, 19–21 November 2017; pp. 1–4.

36. MccCarthy, J. MedStar Attack Found to Be Ransomware, Hackers Demand Bitcoin. 2016. Available online:https://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware- hackers-demand-bitcoin(accessed on 12 March 2019).

37. Patients and Privacy: GDPR Compliance for Healthcare Organizations—Security News—Trend Micro DK. Available online:https://www.trendmicro.com/vinfo/dk/security/news/online-privacy/patients-and-privacy-gdpr-compliance-for-healthcare-organizations(accessed on 12 March 2019).

38. Patel, V. A Framework for Secure and Decentralized Sharing of Medical Imaging Data via Blockchain Consensus. *Health Inform. J.* **2018**. [CrossRef]

39. Hussein, A.F.; ArunKumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Manuel, J.; Tavares, R.S.; Hugo, V.; De Albuquerque, C.; Tavares, J.M.R.S.; de Albuquerque, V.H.C. A Medical Records Managing and Securing Blockchain Based System Supported by a Genetic Algorithm and Discrete Wavelet Transform. *Cogn. Syst. Res.* **2018**, *52*, 1–11. [CrossRef]

40. Dey, T.; Jaiswal, S.; Sunderkrishnan, S.; Katre, N. A Medical Use Case of Internet of Things and Blockchain. In Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 7–8 December 2017; pp. 486–491. [CrossRef]

41. Kaur, H.; Alam, M.A.; Jameel, R.; Kumar Mourya, A.; Chang, V.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *J. Med. Syst.* **2018**, *42*, 156. [CrossRef] [PubMed]

42. Mackey, T.K.; Nayyar, G. A Review of Existing and Emerging Digital Technologies to Combat the Global Trade in Fake Medicines. *Expert Opin. Drug Saf.* **2017**, *16*, 587–602. [CrossRef] [PubMed]

43. Zhang, J.; Xue, N.; Huang, X. A Secure System for Pervasive Social Network-Based Healthcare. *IEEE Access*

2017, *4*, 9239–9250. [CrossRef]

44. Liu, W.; Zhu, S.S.; Mundie, T.; Krieger, U. Advanced Block-Chain Architecture for e-

Health Systems. In Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, 12–15 October 2017; pp. 1–6. [CrossRef]

45. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B.; Marella, B. Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]

46. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information* **2017**, *8*, 44. [CrossRef]

47. Magyar, G. Blockchain: Solving the Privacy and Research Availability Tradeoff for EHR Data: A New Disruptive Technology in Health Data Management. In Proceedings of the 2017 IEEE 30th Neumann Colloquium (NC), Budapest, Hungary, 24–25 November 2017; pp. 135–140. [CrossRef]

48. Weiss, M.; Botha, A.; Herselman, M.; Loots, G. Blockchain as an Enabler for Public MHealth Solutions in South Africa. In Proceedings of the 2017 IST-Africa Week Conference, Windhoek, Namibia, 31 May–2 June 2017; pp. 1–8. [CrossRef]

49. Benchoufi, M.; Porcher, R.; Ravaud, P. Blockchain Protocols in Clinical Trials: Transparency and Traceability of Consent. *F1000 Res.* **2017**. [CrossRef]

50. Zhang, X.; Poslad, S. Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR). In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018.

51. Gordon, W.J.; Catalini, C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 224–230. [CrossRef]