BLOCKCHAIN TECHNOLOGY IN HEALTH

By

Manpreet Kaur

(2195166)

Supervisor:

Professor Trish Williams

Thesis submitted to the **College of Science and Engineering**
In partial fulfilment of the requirements for the degree of
Master of Science (Computer Science)
at Flinders University, Adelaide, Australia

8th November 2019

Declaration

I certify that this thesis does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any university. To the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text.

Manpreet Kaur

8-11-2019

Acknowledgement

The completion of this thesis could not have been possible without the assistance and participation of so many people. The contributions of these people are appreciated sincerely. I would like to express my sincere gratitude to my supervisor Professor Trish Williams for providing their invaluable guidance, comments and suggestions throughout the completion of this thesis.

Also, I would like to thank Gihan Gunasekara for his assistance during the preparation of thesis. In addition, I would like to thank Mr. David Langdon (Editor and Tutor in Flinders International Student Services AAS Program) for proofreading of this thesis.

I would like to special thanks to my beloved husband, Mr. Malkeet Singh for encouraging and supporting me throughout this experience. Finally, I thank my God for letting me through all the difficulties.

Table of Contents

Abstract

In the healthcare sector, handling the medical data of patients is critical. There is potential for threat to patient health if a patient’s data is mismatched with another patient’s information or information is delivered to the wrong hands. Nowadays, the idea of having a patient-centric approach is increasing. Healthcare service providers are beginning to give over control of patients’ data so that medical data can be managed by the patients themselves. However, health data is scattered across different service providers and sometimes different service providers make that data unavailable due to their privacy policies.

Blockchain technology is related to security of medical patient records which helps to maintain the scattered data in different areas by storing the information in a common platform. Blockchain in healthcare will improve the accessibility of the data in healthcare so that there will not be any risk in collecting the information about any patient. This will result in securing the patient’s health records. Blockchain technology is resistant to cyber-attacks and failures, and suitable for providing different modes of access control. Blockchain based healthcare systems can help to exchange the medical data across different providers. The security of identifying the patients will be increased and risk of information blocking will be reduced if blockchain technology is implemented within the healthcare system.

As Blockchain is a relatively new technology, it is not yet widely used in healthcare. However, the use of this technology in healthcare has increased since 2015. So, this research identifies the benefits of blockchain in healthcare and advocates for greater use of the technology.

A systematised literature review is used as a research methodology for evaluating the security and privacy concerns in healthcare and explaining how blockchain technology is useful for handling such concerns in healthcare. The review was accomplished firstly by finding the papers in four different databases with broad keywords and then applying filters for removing the duplicates. After that, a brief description is given of the problems in healthcare and their solutions with the help of blockchain. Lastly, the problems are categorised into main issues and descriptions of which type of blockchain technology is useful for overcoming those issues.

After conducting the systematised review, the study investigated some of the common problems in healthcare. Then, the study described how these specific issues in healthcare can be overcome by using a specific type of blockchain technology, such as which type of blockchain platform is useful for handling which type of issue in healthcare. For example, security and privacy issues in healthcare can be overcome by a specific type of blockchain platform, while other issues can be resolved by using another type of blockchain.

It is very useful to have a specific solution for a specific problem. After completing this research, it was found that there is a need for this blockchain technology in healthcare. It will have great advantage for healthcare having specific types of blockchain technology for specific types of issues in the health field. Therefore, medical practitioners, healthcare workers, or patients with problems in healthcare can use this research for overcoming that issue using the specific type of blockchain technology.

Keywords: Blockchain, blockchain technology, blockchain in health, blockchain in healthcare, applications of blockchain, working of blockchain, issues in healthcare.

Abbreviations

ABS: Attribute Based Signature

DDBMS: Distributed Database Management System

EHRs: Electronic health Records

EMRs: Electronic Medical Records

ERM: External Record Management

EOA: Externally Owned Accounts

IOT: Internet of Things

NoSQL: Not only SQL

ONC: Office of the National Coordinator for Health Information Technology

PHI: Personal Health Information

SQL: Structured Query Language

List of Figures

List of Tables

Introduction

The interest of researchers and developers towards blockchain technology has increased since 2008 (Meng et al., 2018). In blockchain, data is stored in the form of blocks and these blocks are interconnected with each other with the help of hash. Each block has a unique hash, which makes the blockchain more secure. The main benefit of this technology is that there is no central authority for handling the data, because the data is handled by all participating nodes in the network. The nodes in the network are known as miners and the process of verifying the transactions in that network is known as mining.

In the healthcare sector, the main problem is with exchanging information while still maintaining the privacy and security of health data. All important information of the patients is scattered across different departments and healthcare providers which makes it difficult to access quickly, efficiently, and securely in time of need. Health data is critical, so there is a need for technology which can handle the data in a secure way. Blockchain provides a common database for health information that may help the doctors, patients, and pharmacists to access the information easily within a given time-period. Blockchain technology has the efficiency to handle such types of data more securely.

The patient's data is very critical and should not be delivered to the wrong hands or mismatched with other patient's information resulting in a threat to their health. Blockchain technology helps to store the data in immutable form which makes the data more secure. Therefore, the aim of this research is to understand the potential applicability of blockchain to healthcare. The main benefit of this study is to provide a specific type of blockchain solution for specific issue in the health field. With the help of having a specific type of solution for a specific issue, the healthcare providers can overcome that problem easily.

This thesis starts with the literature review which will cover simple introduction to the blockchain technology and shows the working of blockchain. Moreover, some applications of blockchain technology in different fields is provided in literature review. Then, the thesis discusses the need of blockchain technology in healthcare and some benefits of blockchain in healthcare. In addition to this, the literature review provides some examples of blockchain technology used in the healthcare industry followed by one case study of blockchain in healthcare. After that the overview of the methodology used for the case study is given and the chosen methodology is described. Then, the results are given and the whole research is discussed, followed by the conclusion.

Literature Review

This section discusses the background of blockchain and also gives the simple overview of working of blockchain technology. Moreover, some applications of blockchain technology in different areas are also discussed. In addition to this, the need of blockchain technology in healthcare and the benefits are given with some examples. One case study related to blockchain technology in healthcare is also given in this section.

Blockchain

In 2008, Satoshi Nakamoto wrote a paper entitled "Bitcoin: A peer-to-peer electronic cash system" where the author described how online payments can be sent securely from one party to another party without going through any financial institution (Nakamoto, 2008). There have been suggestions that this paper was actually written by unknown persons under the pseudonym 'Satoshi Nakamoto'; however, the idea formed the beginning of the invention of cryptocurrency and blockchain technology. Today, all networks and medium of exchanges that use cryptography to secure transactions without the interference of any centralised trusted entity are known as cryptocurrencies (Crosby, Pattanayak, Verma, & Kalyanaraman, 2016).

Blockchain technology holds distributed ledgers which secure data by encryption, and it ensures that no changes have occurred in the transactions (Linn & Koo, 2016). Third parties such as banks are not required as intermediators for verifying and securing the transactions (Singhal, 2018). Blockchain consists of a set of blocks that are linked through cryptographic hashes. Each block is attached to its previous block with the help of hash and no one can alter the data in that block because each hash has its own unique value. The blockchain data is connected by backwards and forwards linking of each block in the chain (Singhal, 2018). "The first block in the blockchain is known as genesis block" (Nofer, Gomber, Hinz, & Schiereck, 2017). The hash of each block is unique and if any changes are made to that block then its hash will also change which can help prevent fraud. Most popular examples of this technology are Bitcoin and other cryptocurrencies.

Three main components of blockchain

- **Distributed network:** Blockchain is a decentralised peer-to-peer network which is a type of independent management system without the involvement of any higher or central authority (Linn & Koo, 2016) . In each network, members have a copy of the blockchain, and the verification and validation of all transactions are done by all the members of that network.

- **Shared ledger:** In blockchain, all digital transactions are stored in the form of a ledger (Linn & Koo, 2016). Whenever, a new transaction has to be added, some algorithms need to be run to verify the transaction. "If the majority of the members of the network agree that the transaction is valid than that new transaction is added to the ledger" (Linn & Koo, 2016). Changes in the shared ledger become visible to all in the blockchain and no alterations can be done in that transaction once it is added (Linn & Koo, 2016). A single member of blockchain cannot change the data because the copy of the blockchain is available to all the members of that network.
- **Digital transactions:** Any type of information can be stored in a blockchain and the type of information contained in the transaction is determined by the network of blockchain (Linn & Koo, 2016). New transactions are added to the blockchain after being signed and verified to ensure the authenticity and accuracy. Transactions are stored in the form of blocks and each block is connected to each other in linear form and chronological order (Linn & Koo, 2016).

How does blockchain technology work?

To understand the concept of blockchain technology, it is necessary to understand how bitcoin works because the concept of blockchain comes from bitcoin. Bitcoin uses cryptographic proof for each transaction instead of trusting third parties for executing transactions online over the internet (Crosby et al., 2016). A digital signature is used for the protection of each transaction. In this regard, "the digital signature, "public key" of the receiver is sent and the "private key" of the sender is used to digitally sign the transaction" (Crosby et al., 2016). Whenever the sender wants to send money, ownership of the "private key" needs to be proved by the owner of cryptocurrency. Then, the receiver verifies the digital signature by proving ownership of the corresponding "private key" using the "public key" of the sender on the respective transaction (Crosby et al., 2016).

In the bitcoin network, each transaction is broadcast to each node and afterward the verification transaction is recorded in the public ledger (Crosby et al., 2016). However, a problem arises for maintaining the order of transactions that are broadcast on the bitcoin network. When transactions are broadcast over the bitcoin network, transactions are passed through each node of the network; however, there is no guarantee that the order of transactions received by each node is same as the order of transactions when generated. Due to this problem, the chances of double-spending of the cryptocurrency may increase (Crosby et al., 2016). To overcome that problem, a system is needed to maintain the order of transactions. The blockchain solved this problem by a mechanism that is known as blockchain technology (Crosby et al., 2016). In this technology, the bitcoin system orders the transactions in the form of blocks and these blocks are linked with each other, which is otherwise known as blockchain. These blocks are linked to each other in a linear, chronological order, and each block contains the hash of the previous block (Crosby et al., 2016). Figure 1 shows the working of the blockchain and how one party can transfer data or money to another party in blockchain.

Figure 1- Working of Blockchain (Crosby et al., 2016) has been removed due to Copyright restrictions.

Terminologies related to blockchain

- **Private blockchain:** There is a specific owner of the blockchain which handles the whole blockchain network (Aung & Tantidham, 2017). In this type of blockchain, permission is required by the nodes to enter in the blockchain network (Rouhani & Deters, 2017). The private blockchain is faster, more efficient, and safer.
- **Public blockchain:** The public blockchain network consists of multiple nodes and anyone can join to the network (Rouhani & Deters, 2017). In this type of blockchain, only synchronised nodes should be used. The network of such blockchain is decentralised, but it is less trustworthy (Rouhani & Deters, 2017).
- **Consortium blockchain:** Consortium is also known as a hybrid blockchain (Rouhani & Deters, 2017). Only specific organisations can access this type of blockchain (Wang, Feng, & Chai, 2018). The network of this blockchain is partially decentralised.
- **Ethereum blockchain:** Ethereum is the most popular platform on which distributed applications can be run (Macrinici, Cartofeanu, & Gao, 2018). The main benefit of using Ethereum platform is that applications can be available anywhere and anytime. There are two types of accounts in Ethereum blockchain: External Owned Accounts

(EOA) and contract accounts to specify unauthorised individuals (Aung & Tantidham, 2017) .

- **Smart contracts:** A smart contract is a computer program having a number of rules that run on the blockchain (Mohanta, Panda, & Jena, 2018). It executes the code without the involvement of third parties. For implementing smart contracts in blockchain platforms, solidity programming language is used (Aung & Tantidham, 2017). The integration of smart contracts and blockchain technology provides peer-to-peer transactions and can securely maintain the database.

Applications of blockchain technology

Blockchain technology has many applications in different areas such as proving digital identity, to reduce electoral fraud in government, handling data of Internet of Things, in supply chain management, and data security.

- **Digital identity:** Providing personal identity to individuals has always been a great challenge (Baucherel, 2018). When an individual crosses national borders, they are required to give proof of identity using an identity card or passport. Since the invention of the Internet and the interactions that take place online, the problem of identity has become an even more critical issue for many reasons. Blockchain technology may be useful to securely store and access the identity and comprehensive individual data of each person to be maintained (Baucherel, 2018). An app is being developing by United Nations ID2020 Project which will provide identity (legal identity) to all(Baucherel, 2018).
- **Government:** Blockchain technology provides opportunities for government to reduce fraud, minimise errors in payments, and provide transparency between government agencies and citizens (Alketbi, Nasir, & Talib, 2018) . Blockchain is also useful in voting systems as it provides transparency in the voting process. The votes can be recorded in immutable form. With the help of blockchain technology, government can efficiently maintain the health data of the population, so that health data can be shared among other service providers (Alketbi et al., 2018).
- **Internet of Things:** Internet of Things (IoT) is defined as the collection of data through connected devices and sensors from their surroundings (Al-Megren et al., 2018). The data generated from the smart devices is stored in diverse forms, which

may result in privacy and security issues. “Blockchain technology is a suitable solution for providing a secure and immutable method for handling data generated from IoT techniques” (Al-Megren et al., 2018).

- **Supply chain:** Supply chain is the perfect example of blockchain approach. Steps starting from raw material to finished product can be reflected through blockchain (Lu & Xu, 2017). Blockchain provides data transparency in the supply chain management. Blockchain technology is used by the Everledger Limited company where blockchain is used for tracking the features of diamonds, such as cutting, their quality and also helps to reduce the risk of fraud (Lu & Xu, 2017). Blockchain technology is suitable for traceability in the supply chain.
- **Data security:** Nowadays, data theft problem is growing as the volume of data is also growing (Baucherel, 2018). It has become possible for hackers to crack the security layers around data. So, there is need of new ways of securing data. Third parties can also audit the blockchain to ensure that everything is genuine, but they cannot tamper with the data (Baucherel, 2018). Only some part of the information can be visible unless the algorithms behind the blockchain are known (Baucherel, 2018).

Need of blockchain in healthcare

In the healthcare sector, secure storage and access to the medical data of patients is very important. The patient’s data is very critical and should not be delivered to the wrong hands or mismatched with other patient’s information resulting in a threat to their health (Marko, Marko, Aida, & Lili Nemec, 2018). Blockchain technology is resistant against cyberattacks and failures in other systems, such as computer files, and is suitable for providing different modes of access control. Also, data should be ideally managed by the patients. Now, healthcare services are enabling the patient-centric approach so that patients can manage and their own data. Blockchain based healthcare systems can help to exchange the medical data across different providers. So, blockchain technology is an effective framework for handling healthcare data.

Blockchain in healthcare

To understand the benefits of blockchain technology in biomedical and health care applications, it is necessary to compare the benefits of blockchain technology over traditional Distributed Databases (DDBMS). Examples of DDBMS are SQL and NoSQL based systems.

The key benefits are:

- The very first key benefit is that blockchain is a peer-to-peer, **decentralised database management system** whereas DDBMS is a centralised management system (Kuo, Kim, & Ohno-Machado, 2017). Therefore, blockchain technology is suitable for the applications where health care and biomedical stakeholders (hospitals, patients, payers, and providers) want to collaborate with one another without any central authority.
- Second benefit is **immutable audit trail**. DDBMS supports insert, delete, update, and read functions, but blockchain provides only create and read function (Kuo et al., 2017). This functionality of blockchain helps to maintain the critical data because no one can alter or delete the information in blockchain.
- The third key benefit is **data provenance**. In DDBMS, “the ownership of the digital assets can be changed or altered by the system administrator, but in blockchain technology, the ownership of the digital assets can be modified by the owner only by using cryptocurrency protocols” (Kuo et al., 2017). Also, the sources of data and records can be confirmed in blockchain (Kuo et al., 2017). Therefore, it is suitable for managing critical digital assets.
- The final key benefit of blockchain is **security and privacy**. “Blockchain technology has an improved security and privacy using cryptographic algorithms” (Kuo et al., 2017). Bitcoin blockchain uses 256-bit Secure Hash Algorithm (SHA-256), which is defined in the US Federal Information Processing Standards (Kuo et al., 2017). Bitcoin blockchain exploits the 256-bit Elliptic Curve Digital Signature Algorithm which helps to generate and verify the high-security-level public and private keys as digital signature (Kuo et al., 2017).

Examples of blockchain in healthcare industry

As blockchain has a decentralised database, it has many advantages in the healthcare industry. In addition, this decentralised database is very useful when different parties need to access the same information. In the US, an initiative has been taken by developing Gem, a blockchain product for health claims management and sharing of patient data (Mettler, 2016). The Gem Health Network is based on the Ethereum blockchain technology which is a shared network enabling different health specialists to access the same health information (Mettler, 2016). This approach provides clear access to the latest treatment information to all medical stakeholders. Sometimes medical stakeholders can have outdated information related to any treatment. By this system, the issue of outdated information can be removed and can prevent health issues by providing updated information. Also, medical experts can have access to all the previous health information related to any patient. So, the entire treatment of patient will be transparent (Mettler, 2016). In 2011,

A further example of blockchain in the health industry is Estonia’s recent cooperation with the Guardtime company, which operates healthcare systems based on the blockchain technology (Mettler, 2016). By using the Guardtime platform, citizens of Estonia, healthcare providers, and health insurance can have access and retrieve all information of medical treatment performed in Estonia. This example in Estonia demonstrates that complete public healthcare infrastructure can be operated by using blockchain technology (Mettler, 2016).

Healthbank is a global Swiss digital health startup, which handles the personal health data. In this Healthbank, “users can store and manage their health information in a secure environment” (Mettler, 2016). Nowadays, in Healthbank, users not only store their health data but also make their health data available for the medical research. By this sharing of information, in return, they receive financial compensation for approving use of their data. Now, “Healthbank plans to apply blockchain technology for underlying business model” (Mettler, 2016). In future, health apps, wearable devices, or physician visits can be used to retrieve personal patient-generated health data and can securely store the information in Healthbank blockchain (Mettler, 2016). Users who are contributing in medical health research can be awarded at a higher level than average by identifying uniquely with the help of blockchain (Mettler, 2016).

According to the World Health Organization (WHO), worldwide the percentage of drugs on the market that are counterfeit is estimated to be10%. Furthermore, in developing countries, the rate is up to 30% (Mettler, 2016). The ingredients of these medications may be inactive, incorrect, or even harmful. Not only are lifestyle and supplement products being affected by counterfeit drugs, drugs for cancer treatment, antibiotics, analgesics, and other prescription drugs are affected (Mettler, 2016). Recently, the Counterfeit Medicine Project was launched by Hyperledger which is focused on the issue of counterfeit drugs (Mettler, 2016).

Accenture, Cisco, Intel, IBM, Block Stream, and Bloomberg are all involved in this research project. The labelling of each drug is marked with a timestamp which helps to determine when and where the drug is produced in a given time period (Mettler, 2016). The origin of the product and its components can be detected by using blockchain, which will helps to track poor quality or forged goods, and this technology has many other applications across the manufacturing and commercial industries (Mettler, 2016).

Case study for blockchain in healthcare

A MedRec prototype based on blockchain technology is proposed which is used to handle electronic health records (EHRs) using a decentralised record management system (Ekblaw, Azaria, Halamka, & Lippman, 2016). This system provides an easy access to the health information for patients and providers. MedRec stores the health information in an immutable log. The system is design in such a way that it can integrate with existing databases. This prototype will help to address four main problems in healthcare systems: Interoperability, fragmented data, patient agency, and data for medical research (Ekblaw et al., 2016). These problems are further explained as follows:

- Interoperability is the most important factor that is considered in the healthcare centre (Ekblaw et al., 2016). It has become a challenge for different providers and hospital systems to exchange information, which leads to ineffective data sharing.
- In the healthcare sector, all important information of the patients is scattered in different departments, which makes it difficult to access in times of need (Qiu, Liang, Shetty, & Bowden, 2018). This is an inadequate way of handling the information. This results in difficulty in gathering the important data about the patient and that leads to health information blocking.
- Sometimes patients have doubt about the confidentiality of their data (Qiu et al., 2018). With trending of social media and online media, patients are increasingly willing to manage their own health data online.

- For health researchers, medical data is very crucial. Research on previous health issues may help to find another new treatment for those problems (Qiu et al., 2018). This prototype helps to improve the quality and quantity of data for medical research.

After doing the literature review, it is clear that there are some issues or problems in healthcare domain related to data security, data privacy and many more.

Authors (Ekblaw et al., 2016) highlights the issues of interoperability and confidentiality in healthcare, while author (Mettler, 2016) suggest that access to health data is also a major problem. Confidentiality problem and data access problem in healthcare is also highlighted by authors (Qiu et al., 2018). Some countries such as in US and Estonia has started the use of blockchain technology to overcome the problem of access to health data. Counterfeit drug problem in healthcare is also discussed by the author (Mettler, 2016). For this issue, some companies are trying to use blockchain technology. Authors (Marko et al., 2018) proposed the mismatched data problem in health field which may lead to a threat to patient’s health.

There is a need of an investigation to evaluate different issues in healthcare domain and how they can be solved by using a technology which is more secure. In different papers, different issues related to healthcare domain has been identified. There is need of an investigation which helps to identify issues in healthcare domain on single paper with their solutions.

Research question

In the healthcare sector, a huge amount of data is generated on a regular basis (Asad Ali et al., 2019). Storing and handling such a large amount of data is very crucial. Moreover, maintaining the security and privacy of such sensitive data is very challenging. Consequently, there is a need for a secure technology which can manage the sensitive data in healthcare. Therefore, blockchain technology provides a secure way to handle the healthcare data. Nowadays, interest of researchers towards blockchain technology has been increased (Asad Ali et al., 2019). This research will address how blockchain is being used in healthcare to address security and privacy issues. This can be followed by identifying issues in healthcare and then determining how blockchain is useful for overcoming problems in the system.

The research question is: How is blockchain being used in healthcare to address security and privacy issues?

Methodology

General overview of methodology

This study used a review methodology in the process of conducting the case study on 'Blockchain in healthcare'. There are 14 different types of review methods that enable researchers to examine a question, for example, a systematic review, a systematised review, or a state-of-the-art review (Grant & Booth, 2009). Different types of reviews have their own methods or steps to complete that review. For this research, a systematised review was chosen as most appropriate for the case study to investigate how blockchain works and how it is applied in healthcare currently. This systematised review enabled a logical approach to find the answers to the research question by firstly identifying the existing problems in the healthcare sector, then determining the reasons behind those problems, and finally explaining how blockchain technology can help to minimise those problems. This review method and process helped to explore the qualitative research about the use of blockchain technology in health.

Designing of methodology to answer the research question

Steps for the systematised review are as follows:

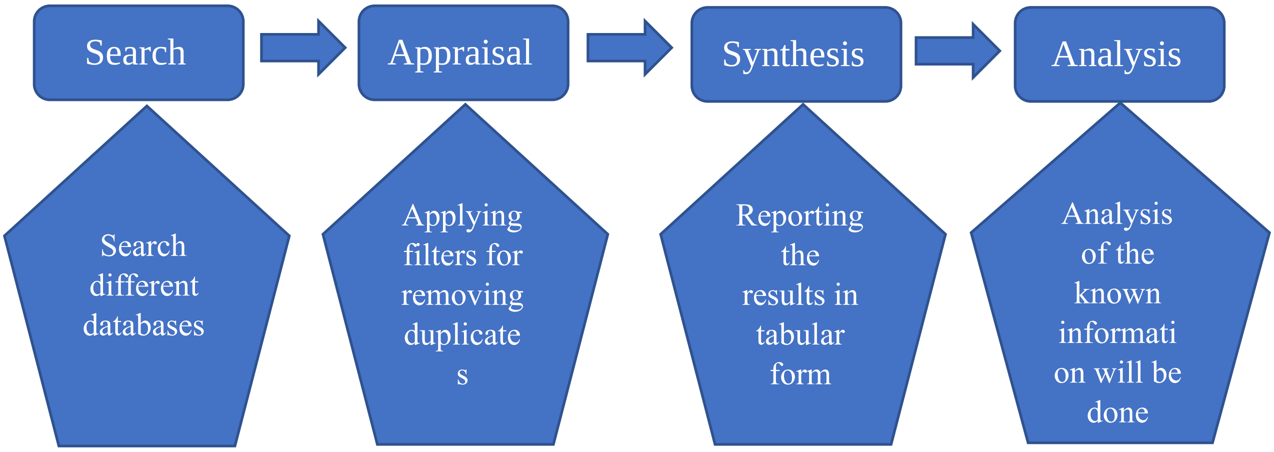
Search
Appraisal
Synthesis
Analysis
Search different databases
Applying filters for removing duplicates
Reporting the results in tabular form
Analysis of the known information will be done

Figure 2- Steps for Systematised Review (Grant & Booth, 2009)

Search: In this, different databases are used to collect the information related to the research problem (Barr-Walker, 2017). Also, this section defines the language of the papers used for the study.

Appraisal: Studies where the data is not related to the research problem are excluded.

Synthesis: The collected information is synthesised by reporting the studies with tabular form. The information which answers the research questions is organised in a systematic way, to enable an understanding the studies in proper manner.
Analysis: Analysis of the known information was done.

Research Design

The following steps are used to conduct the systematised review on blockchain technology in healthcare:

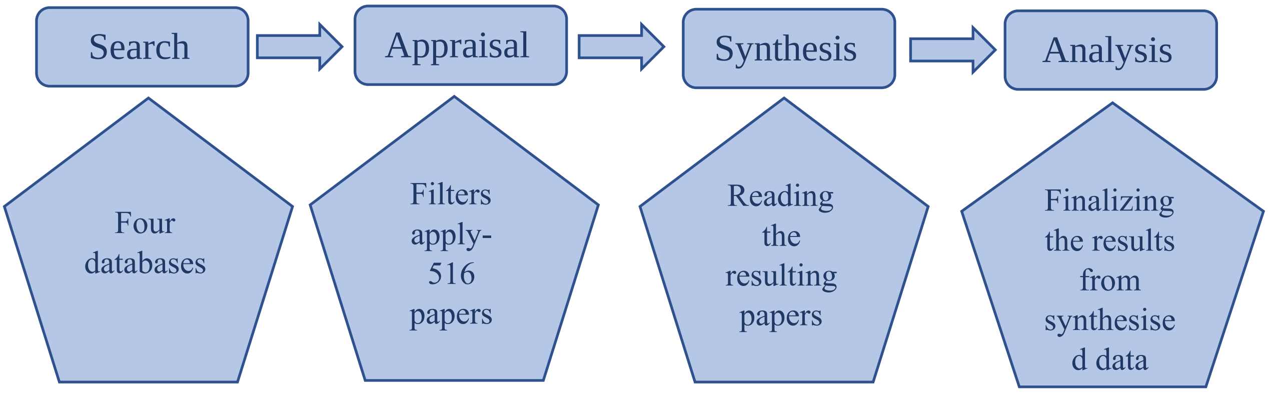
Search
Appraisal
Synthesis
Analysis
Four databases
Filters apply- 516 papers
Reading the resulting papers
Finalizing the results from synthesise d data

Figure 3- Implementation of Systematised Review

1. **Search:** The search is based on the research question: How is blockchain being used in healthcare to address security and privacy issues? The research question is based upon the health and science field, so, for this search method, four different databases were searched: IEEE Xplore, Science Direct, ProQuest, and Wiley Online Library. For this research, reference papers from the past 10 years were used, because the latest technology and research is needed for this study rather than using publications that predate the introduction of blockchain technology. Journals, conference papers, review articles, and research articles are used in this report. The language limitation for all the papers is English. Only the papers with full text available are used for this research. Keywords used for this research are: blockchain; blockchain technology; healthcare; blockchain and healthcare.

   Details of all the databases and total number of papers found in those databases are listed in Table 1.

Table 1- Searched databases with their results

S.No.	Keywords	Database	Total Number of papers	conference	journals	Review Articles	Research articles
1.	Blockchain	IEEE Xplore	2,833	2,209	328	-	-
		Science Direct	1,699	-	-	127	994
		ProQuest	227,774	1,918	-	3,478	-
		Wiley Online Library	857	-	402	-	-
2.	Blockchain technology	IEEE Xplore	1,911	1,451	273	-	-
		Science Direct	1,582	-	-	127	936
		ProQuest	165,571	1,153	-	3,043	-
		Wiley Online Library	812	-	381	-	-
3.	Healthcare	IEEE Xplore	20,996	17,299	2,587	-	-
		Science Direct	450,820	-	-	29,791	269,719
		ProQuest	8,761,761	9,535	-	936,991	-
		Wiley Online Library	473,783	-	435,455	-	-
4.	Blockchain and healthcare	IEEE Xplore	147	103	25	-	-
		Science Direct	363	-	-	46	193
		ProQuest	20,539	94	--	437	-
		Wiley Online Library	157	-	85	-	-

2. **Appraisal**: After searching the broad keywords, more filters are applied to the resulting papers to obtain the correct papers according to the research question. The following list defines the filters applied to remove unwanted material:
   a) **Language**: Only English language-based papers are used for this research.
   b) **Publication date:** The range of the publication dates is set from 2018 to 2019.
   c) **Availability of text**: The limit of the text is set to full text, so that the papers with full text are available.
   d) **Source type**: Journals, conference papers and proceedings, review articles, and research article source-based papers are used.
   e) **Subject**: The papers having the following areas are used for this research:
      - Blockchain
      - Health
      - Healthcare
      - Privacy
      - Security
      - Information system
      - Interoperability
      - Electronic Health Records (EHRs)
      - Information sharing
      - Medical computing

The above filters are applied only to IEEE Xplore and ProQuest databases, while the other two databases, being Science Direct and Wiley Online Library, do not have all filters. Therefore, only publication date and availability of text filters are applied on these two databases. After applying filters, the total number of papers that remained are listed in Table 2.

Table 2- Number of papers after applying filters

S.No.		Database	Numbers of papers reduced
1.		IEEE Xplore	89
2.		Science Direct	225

Table 2 continued…

S.No.	Database	Numbers of papers reduced
3.	ProQuest	105
4.	Wiley Online Library	97

The number of the papers was further reduced after reading the abstract of each paper. The papers that are related to the research question are included and the rest of the papers are removed. The total number of papers that were found after filtering was 27.

3. **Synthesis:** A brief summary of the resulting 27 papers that were finalised after applying all filters is provided in Table 3. A brief explanation of problems in the healthcare field, their related proposed solutions, and discussion on how proposed solutions are useful is given in the Table 3.

Table 3- Problems in healthcare, their solutions, and how the solution is useful

S.No.	Problems in Healthcare	Proposed Solution	How Proposed Solution is Useful	References
1.	Lack of trust in the data, in conventional health systems. Data leakage by insurance companies of patient data.	The framework is the combination of IoT, blockchain, and mobile learning techniques. The data that is generated by the wearable devices using IoT and blockchain used to in the form of transactions. In this, machine learning is used to detect the inconsistencies in the data.	The proposed ERM blockchain is used to maintain the generated data. This ERM blockchain can be accessed by the insurance companies directly without any need of paperwork.	(Chakraborty, Aich, & Kim, 2019)
2.	Integrity and interoperability problem in personal health records.	**OmniPHR** architecture model is proposed using private blockchain technology and openEHR interoperability standard.	Helps to integrating distributed health records. And private blockchain ensures that the health data blocks are accessed by authorized participants in the network only.	(Roehrs et al., 2019)

Table 3 Continued…

S.No.	Problems in Healthcare	Proposed Solution	How Proposed Solution is Useful	References
3.	Privacy issue during data sharing in EMRs.	**BDPS**: A Blockchain based Privacy-Preserving Data Sharing framework is a three-layered architecture: data acquirement layer, data storage layer, and data sharing layer. The first layer is used to create the EMRs of patients by the doctors using content extraction signature. The second layer stores the original EHR into cloud and its indexes are stored in consortium blockchain network. In the third layer, authorized individuals such as patients, medical institutions can access the patients' EMRs.	As EMRs are stored in cloud and their indexed are recorded in the consortium blockchain which solves the problem of security risks of centralized data. Also, privacy in data sharing can be provided by extraction signature scheme.	(Liu et al., 2018)
4.	Security and privacy issue of the patients increases with IoT devices in Healthcare System	On the basis of blockchain technology a **Remote Healthcare System** is proposed based on Smart Contracts. System consists of three main parts: healthcare providers (hospitals), healthcare professionals (doctors) and patients.	Smart contracts help to manage the patient's information and medical devices. Data processing mechanism is presented in case of criticality from medical devices to increase its efficiency.	(Pham, Tran, & Nakashima, 2018)

Table 3 Continued…

S.No.	Problems in Healthcare	Proposed Solution	How Proposed Solution is Useful	References
5.	Privacy issue during collecting, managing the data of EHRs.	The main components of the solution are: **Ordering service** is a type of administration to provides access to the entities, **Certificate Authority** to uniquely identify each entity, **Blockchain Network Configuration** to interact with blockchain, **Channel configuration** to establish privacy, **smart contracts** to create unique accessor for authorized entities, **channel** to create a private platform, and **nodes** are the network components to store local copies.	Only authorised parties are allowed to access the EHRs with the technique known as channeling integrated with smart contract. Interoperability can be achieved by this solution as proposed solution can interact with EHR platform and other platforms as well.	(Nortey, Yue, Agdedanu, & Adjeisah, 2019)
6.	Access problems for patients and providers to interact with EHRs.	**Ancile** framework is used to overcome these issues. Ancile framework uses six different smart contracts with Ethereum-based blockchain and has three main software components: database manager, Cipher Manager, Ethereum-Go client.	With this solution, patients can have control over their data to track their records and allow the transfer of data securely. Ancile framework provides data privacy and data integrity.	(Dagher, Mohler, Milojkovic, & Marella, 2018)
7.	Data integrity problem in clinical trial process.	The private blockchain to handle the clinical trial data.	Helps in data management of clinical trial process.	(Wong, Bhattacharya, & Butte, 2019)

Table 3 Continued…

S.No.	Problems in Healthcare	Proposed Solution	How Proposed Solution is Useful	References
8.	Interoperability issue while maintaining privacy and integrity of data in healthcare systems	The solution provides a mechanism how interoperability can be achieved by addressing data privacy and data integrity. They use blockchain and smart contracts to achieve the goal.	Interoperability of patients' records can be achieved by using the combination of blockchain and smart contracts.	(Alexaki, Alexandris, Katos, & Petroulakis, 2018)
9.	Storing and sharing large amount of healthcare data	**BlocHIE-** a BLOCkchain-based platform for Healthcare Information Exchange system is proposed which is based upon two loosely-coupled blockchain to handle different types of healthcare data.	This system helps to store and share two kinds of healthcare data: personal healthcare data and electronic medical records.	(Jiang et al., 2018)
10.	Problem of maintaining and sharing large amount of data in EMRs.	**MedBlock** framework is proposed to overcome the given problems. MedBlock is a type of information management system which is based upon the blockchain technology.	Distributed ledger of blockchain helps to access and retrieve the data in EMRs efficiently.	(Fan, Wang, Ren, Li, & Yang, 2018)
11.	Data-integrity problem in eHealth systems.	Blockchain-based eHealth Integrity Model is designed using permissioned blockchain to maintain the information integrity in eHealth systems.	Designed framework can easily integrate with the exiting eHealth systems and provides the data-integrity service and also helps to remove the paper work or documents.	(Hyla & Pejaś, 2019)

Table 3 Continued…

S.No.	Problems in Healthcare	Proposed Solution	How Proposed Solution is Useful	References
12.	Integrity and interoperability issue in EHRs.	The proposed architecture used smart contracts platform which consist of summary contracts to give reference of providers and record relationships to store the metadata of records. The platform can be changed to another blockchain platform according to other preferences.	The proposed solution is compatible with the exiting electronic healthcare systems which makes health providers to maintain the records.	(Yang, Li, & Marstein, 2019)
13.	Patients have no control over their EMRs.	Private and permissioned blockchain are used for the proposed EMR approach which helps to encrypt the patients' information and store in the blockchain transactions.	Blockchain transactions helps the patients to keep control over their EMRs. And, patients can provide access to their EMRs only to trustworthy individuals.	(Oliveira et al., 2019)
14.	Lack of secure information exchange of clinical data.	Present a **FHIRChain** architecture based upon the blockchain and a DApp (Decentralised App) prototype is made based on FHIRChain architecture. They used Ethereum blockchain and three smart contracts for DApp prototype.	Provides effective data sharing by meeting the requirements of ONC.	(P. Zhang, White, Schmidt, Lenz, & Rosenbloom, 2018)

Table 3 Continued…

S.No.	Problems in Healthcare	Proposed Solution	How Proposed Solution is Useful	References
15.	Privacy issue while data sharing among cross-organisational EMRs.	**EMRShare** framework is used for cross-organisational data sharing using permissioned blockchain. EMRShare framework is decentralized among different organisations.	Decentralized framework for storing and managing data improves the data sharing among different organisational EMRs.	(Xiao et al., 2018)
16.	Privacy issue while creating, maintaining, and sharing the data among various stakeholders.	**DASS-CARE** Decentralized, Accessible, Scalable, and Secure healthcare framework. Blockchain is used to store the data of different providers.	Blockchain based framework helps to share the data securing while maintaining the privacy of the data.	(Al-Karaki, Gawanmeh, Ayache, & Mashaleh, 2019)
17.	Security issue in health information in remote patient monitoring or with IOT devices.	The proposed framework used the private blockchain based upon Ethereum protocol and smart contracts to communicate between sensors and smart devices.	The proposed framework helps to transfer the data securely.	(Griggs et al., 2018)
18.	Security and privacy issue in patient-driven interoperability.	The framework provides five different mechanism based upon blockchain technology: digital access rules, data aggregation, data liquidity, patient identity, and data immutability.	Helps to facilitate the institution-driven interoperability into patient-driven interoperability.	(Gordon & Catalini, 2018)

Table 3 Continued…

S.No.	Problems in Healthcare	Proposed Solution	How Proposed Solution is Useful	References
19.	Sharing problem in healthcare for research purpose.	The proposed framework has three layers: **Web/Cloud Platforms** for storing patients' data, **Cloud middleware** to securely communicate between layer1 and layer2, and **Blockchain network** for secure data sharing. They used consortium blockchain and different smart contracts.	Helps to securely data sharing and maintain the integrity of data.	(Theodouli, Arakliotis, Moschou, Votis, & Tzovaras, 2018)
20.	Sharing EHRs without any leakage of data.	The proposed scheme consists of three entities**: data owner** which creates the data and indexes using smart contracts, **blockchain**(Ethereum based blockchain) to store the data with their indexes, and **user** (only authorized) can search the indexes for their EHRs.	Smart contracts help to access indexes by authorized individuals to minimize the data leakage problem.	(Chen, Lee, Chang, Choo, & Zhang, 2019)
21.	Interaction with the data while maintaining the privacy of patients in EHRs.	The architecture of the system consists of blockchain for transferring nodes, patients nodes where records are created, and provider networks for creating database of health records.	Patients can have control over their records and can monitor their transactions with the help of blockchain. Having decentralized system can minimize the risk of unauthorized access.	(Vora et al., 2018)

Table 3 Continued…

S.No.	Problems in Healthcare	Proposed Solution	How Proposed Solution is Useful	References
22.	Patient privacy in EHRs.	The proposed framework used the ABS scheme and blockchain technology.	With the help of blockchain, authorized patients can have access to their health records.	(Guo, Shi, Zhao, & Zheng, 2018)
23.	Security issue in EHR.	The proposed system consists of four layers: User management layer to manage the users of the system, EHR generation and view layer for viewing the EHR and logins, EHR storage layer store the EHR into distributed database known as blockchain, and EHR access management layer for accessing and sharing EHR.	Uses multilevel authentication for securing EHR.	(Radhakrishnan, Joseph, & Sudhakar, 2019)
24.	Security and privacy issue in PHI.	Private and consortium blockchains are used for the proposed solution. Private blockchain helps to store the patients' original PHI and consortium blockchain stores the indexed of PHI.	Immutability functionality of the blockchain helps to preserve the privacy and security of the PHI.	(A. Zhang & Lin, 2018)

Table 3 Continued…

S.No.	Problems in Healthcare	Proposed Solution	How Proposed Solution is Useful	References
25.	Access problem for patients' medical records.	The proposed system uses the permissioned blockchain such as multichain which provides the easy configuration of settings of block size and block timings.	Multichain makes publishing the data to the blockchain easy which helps to retrieve the data from the blockchain easily. It makes easy to communicate medical records among different institutions.	(Hanley & Tewari, 2018)
26.	Privacy issue while sharing of Medical records.	**MeDShare** system is proposed which is based upon the blockchain technology and uses smart contracts and access control mechanism for tracking the data.	Helps in sharing of data while taking data privacy in account.	(McGhin, Choo, Liu, & He, 2019)
27.	Security and privacy issue in Healthcare systems.	Proposed framework provides the mechanism that determines how and where data will be stored using private blockchain. The data will be stored in the medical servers and their addresses will be stored in the blockchain.	Helpful for efficient and secure accessibility of data.	(Ramani, Kumar, Bracken, Liyanage, & Ylianttila, 2018)

The above table 3 provides a brief summary of problems in healthcare sector, their solution using blockchain technology and how the proposed solutions are helpful for minimizing the problems in healthcare sector. A brief summary of the proposed solutions for respected problems in healthcare are given in table 3 so that, health professionals can have idea about the solution for some specific problems. The new terms from the table 3 are explained below:

- ERM blockchain: External Record Management (ERM) blockchain is used for managing the records and it may consist of any pharmacy bills, test reports, prescriptions, or data generated by healthcare providers.
- OmniPHR Standard: This standard is used for providing some specifications regarding the communication and data storage.
- Cipher Manager: Cipher Manager is responsible for encryption and decryption of keys for cryptography.
- Loosely-coupled blockchain: In this type of blockchain, chains are coupled to store different type of data in different chains.
- ABS Scheme: In Attribute-based signature(ABS), the signatures are not easily forged and provides a strong privacy for signers.
- Two-loosely coupled blockchain: In this, two chains of blockchain are coupled with other to store two different type of data individually in each chain.
- Permissioned blockchain: In this blockchain type, some nodes in the blockchain network have rights to change or alter the data in some blocks in that network.
- Some blockchain types are combined with other technologies to make them more secure. For example, the technologies are smart contracts, ABS scheme, and multilevel authentication.

4. **Analysis:** From Table 3, problems in healthcare are categorised into specific types of issues. Table 4 will provide the specific type of issue from the problems in healthcare and how that issues can be removed by using specific types of blockchain technology with the help of Table 2.

Table 4- problems in healthcare, their specific type of issue, and type of blockchain technology used

S.No.	Problems in Healthcare	Type of Issue	Type of blockchain used
1.	Lack of trust in the data in conventional health systems. Data leakage by insurance companies of patient data.	Trust issue Data leakage	Simple blockchain
2.	Integrity and interoperability problem in personal health records.	Interoperability Data-Integrity	Private blockchain
3.	Privacy issue during data sharing in EMRs.	Privacy issue during sharing of data in EMR/EHRs	Consortium blockchain
4.	Security and privacy issue of the patients' data increase with IoT devices in Healthcare System	Security and privacy issue with IOT devices	Blockchain with smart contracts
5.	Privacy issue during collecting, managing the data of EHRs.	Privacy issue during sharing of data in EHR/EMRs	Hyperledger (permissioned private) blockchain with smart contracts
6.	Access problems for patients and providers to interact with EHRs.	Access problem	Ethereum-based blockchain with smart contracts
7.	Data integrity problem in clinical trial process.	Data-Integrity	Private blockchain
8.	Interoperability issue while maintaining privacy and integrity of data in healthcare systems	Interoperability	Blockchain with smart contracts

Table 4 Continued…

S.No.	Problems in Healthcare	Type of Issue	Type of blockchain used
9.	Storing and sharing large amount of healthcare data (EMRs/PHD)	Information exchange	Two loosely-coupled blockchains
10.	Problem of maintaining and sharing large amount of data in EMRs.	Data Management Privacy issue during sharing of data in EMR/EHRs	Simple blockchain
11.	Data-integrity problem in eHealth systems.	Data-Integrity	Permissioned blockchain
12.	Integrity and interoperability issue in EHRs.	Interoperability	Blockchain with smart contracts
13.	Patients have no control over their EMRs.	Patient Control	Private and permissioned blockchain
14.	Lack of secure information exchange of clinical data.	Data Sharing	Ethereum-based blockchain with smart contracts
15.	Privacy issue while data sharing among cross-organisational EMRs.	Privacy issue during sharing of data in EMR/EHRs	Permissioned blockchain
16.	Privacy issue while creating, maintaining, and sharing the data among various stakeholders.	Data management Data Sharing	Simple blockchain
17.	Security issue in health information in remote patient monitoring or with IOT devices.	Security issue with IOT devices (remote patient monitoring)	Ethereum-based private blockchain with smart contracts
18.	Security and privacy issue in patient-driven interoperability.	interoperability	Simple blockchain

Table 4 Continued…

S.No.	Problems in Healthcare	Type of Issue	Type of blockchain used
19.	Sharing problem in healthcare for research purpose.	Data Sharing Access problem	Consortium blockchain with smart contracts
20.	Sharing EHRs without any leakage of data.	Data Leakage	Ethereum-based blockchain with smart contracts
21.	Interaction with the data while maintaining the privacy of patients in EHRs.	Privacy	Simple blockchain
22.	Patient privacy in EHRs.	Privacy	Blockchain with ABS scheme
23.	Security issue in EHRs.	Security	Blockchain with multilevel Authentication
24.	Security and privacy issue in PHI.	Security and privacy (PHI)	Private and consortium blockchain
25.	Access problem for patients' medical records.	Access problem	Permissioned blockchain
26.	Privacy issue while sharing of Medical records.	Data Sharing	Blockchain with smart contracts
27.	Security and privacy issue in Healthcare systems.	Security Privacy	Private blockchain

Table 4 presents the issues as defined by the associated papers from Table 3. These issues are listed in the third column, and the suggested blockchain solution in column 4. It should be noted that in the papers that the issues are not unique but the solutions to address them are different. For instance, the issue of data leakage can be addressed by the use of a simple blockchain or an Ethereum based blockchain with smart contracts (S.no 1 and 20). Whereas, data integrity can use private blockchains or permissioned blockchains (S.no. 2,7 and 11). In some papers (S.no. 6, 14 and 19), different issues such as access problem and data sharing problem can be overcome by using same blockchain types that are Ethereum-based blockchain with smart contracts and consortium blockchain with smart smarts. For privacy and security problem, one solution is common that is using private blockchain (S.no.27), but some papers (S.no. 22 and 23) provides different solutions. For example, security issue can be controlled by using blockchain with multilevel Authentication and Privacy issue can be get controlled by blockchain with ABS scheme. There are three different solutions are for addressing the privacy issue during sharing of data in EMR/EHRs (S.no.3, 5 and 15), and three different solutions are: using consortium blockchain; permissioned private blockchain with smart contracts; Permissioned blockchain. For security and privacy issue with IOT devices (remote patient monitoring), two solutions are provided in different papers(S.no. 4 and 17).

Results

After conducting the systematised review, Table 5 shows the results on which specific type of issue in healthcare, and which type of blockchain technology is useful to overcome that issue. The resulting information in Table 5 is derived from the Table 4.

Table 5- Type of issue in healthcare, and type of blockchain used

S.No.	Types of Issues	Type of blockchain used
1.	Trust Issue	Simple blockchain
2.	Data leakage	Simple blockchain Ethereum-based blockchain with smart contracts
3.	Interoperability	Blockchain with smart contracts Private blockchain
4.	Data-Integrity	Permissioned blockchain Private blockchain
5.	Privacy issue during sharing of data in EHR/EMRs	Consortium blockchain Permissioned private blockchain with smart contracts Permissioned blockchain
6.	Security and privacy issue with IOT devices (remote patient monitoring)	Blockchain with smart contracts Ethereum-based private blockchain with smart contracts
7.	Access problem	Ethereum-based blockchain with smart contracts Consortium blockchain with smart contracts Permissioned blockchain
8.	Information exchange	Two loosely-coupled blockchains
9.	Data management	Simple blockchain
10.	Patient control	Private and permissioned blockchain
11.	Data sharing	Ethereum-based blockchain with smart contracts Consortium blockchain with smart contracts Blockchain with smart contracts
12.	Privacy	Blockchain with ABS scheme Private blockchain
13.	Security	Blockchain with multilevel Authentication Private blockchain
14.	Security and privacy issue (PHI)	Private and consortium blockchain

Discussion

Health data is very sensitive, so storing and handling these types of data is very important. Sometimes health data is stored in different health service providers, and these different service providers have their own privacy issues for sharing data with other service providers. Due to this, data becomes unavailable in times of need and patients have to undergo the test again. If data is stored in such manner that all health providers can access that data in times need by providing proper security and privacy to that data. When the data will be available at all times, the time period or cost for curing the diseases will also be reduced. There is need of such technology which can help to store the health data while considering security and privacy issues in such way that all health providers can access that information.

Blockchain technology provides a common platform for storing and handling the health data in a secure way. In blockchain, data is stored in immutable form which makes it secure for handling health data. In addition, blockchain technology helps in the health information exchange among different service providers. Blockchain technology has a successful rate of secure and confident use in the healthcare field.

The idea of blockchain technology comes from the paper: "Bitcoin: A peer-to-peer electronic cash system" which was published by Nakamoto (Nakamoto, 2008). From that time the use of blockchain in different fields was begun; however, most of research on blockchain in healthcare has been done since 2015. For systematised review in this research, papers published in the years 2018 and 2019 are mostly used so that the latest research on blockchain in healthcare can be evaluated.

The research question is "**How is blockchain being used in healthcare to address security and privacy issues?"** Using a systematised review, different problems in the health sector are identified. The problems are not only related to privacy and security but are also related to data leakage, sharing of data, data-integrity, and other problems that are given in Table 5. These different types of issues in the health field can be resolved by using blockchain technology. Table 5 describes these different types of issues in the health field and which specific type of blockchain technology is useful for overcoming an issue. A summary of these is as follows:

- For security and privacy issues in healthcare, blockchain technology with ABS scheme and blockchain with multilevel authentication can be used respectively. Private blockchain is the common solution for both types of issues: security and privacy issues in healthcare.

- Private and consortium blockchain can be used for overcoming security and privacy issue in PHI. For security and privacy issue with IoT devices (with remote patient monitoring), blockchain with smart contracts and Ethereum-based private blockchain with smart contracts can be used.
- For the privacy issue while sharing of data in EHR/EMRs, there are three solutions with different types of blockchain technologies: consortium blockchain, permissioned private blockchain with smart contracts and permissioned blockchain.
- For trust issue and data management in healthcare, simple blockchain technology can be used.
- For data-integrity and patient control problems, private and permissioned blockchains can be used as a solution.
- Using two loosely-coupled blockchains, the information exchange problem can be resolved, whereas, for interoperability, blockchain with smart contracts and private blockchain can be used.
- For the access problem and data sharing problem, three different solutions are provided. However, two solutions in both of them are the same, i.e. Ethereum-based blockchain with smart contracts and consortium blockchain with smart contracts. Only the third solution is different which is permissioned blockchain for solving the access problem and blockchain with smart contracts for the data sharing problem.
- With the help of Ethereum-based blockchain with smart contracts, data leakage problem can be resolved.

After an overall analysis, there are some types of blockchain which can help resolve more than one issue in healthcare. Any healthcare provider suffering from any problem that is discussed in Table 5 can use that information for resolving their issue. Table 5 can clearly help them to identify which type of blockchain technology they can use for their specific type of issue. However, it is important to be aware of one disadvantage of using this blockchain technology in healthcare, which is the limited storage capacity. As the amount of data in the health field is rapidly increasing day by day, a problem may occur in the future due to blockchain data being stored in immutable form. Consequently, storing such a huge amount of data in blockchain in immutable form may eventually create an issue of inadequate storage capacity.

Conclusion

Handling a patient's data securely in the healthcare sector is very important. Mismatched medical data may cause very serious problems to the patient's welfare as well as to the healthcare service provider. Sometimes a patient's data may be stored in different health service providers, which may lead to the unavailability of data in times of need. This may occur because of different privacy policies of different health service providers. Blockchain technology stores the data in immutable form and is not controlled by any central authority. An unintentional or unauthorised alteration to a patient's data stored in blockchain is impossible, which makes it safe for handling health data and for access by health professionals. Blockchain technology has the efficiency to handle the health data securely.

After conducting a systematised review, security and privacy issues in the healthcare sector were identified and the question of how these problems can be resolved by using what type of blockchain technology was answered. The possible solutions are based upon the different types of blockchain technology. Security and privacy issues are identified in both the older and modern healthcare systems, with IoT devices, with remote patient monitoring, with PHI, and privacy issues with EHR, EMRs while sharing data. In addition to security and privacy issues, there is also potential for other issues to arise in healthcare, such as data leakage, trust issues, data-integrity problems, data management problems, information exchange problems, and interoperability problems. This study has shown how all of these problems can be overcome by using blockchain technology to securely manage health data.

For any health service provider experiencing issues related to privacy, security, data leakage, trust issue, data-integrity, data management, information exchange, interoperability, this research offers solutions to address those issues with specific types of blockchain technology. For security and privacy issues in healthcare, blockchain technology with ABS scheme and blockchain with multilevel authentication can be used respectively. But private blockchain can be used for both security and privacy issue in healthcare. For security and privacy issue with IoT devices (with remote patient monitoring), blockchain with smart contracts and Ethereum-based private blockchain with smart contracts can be used. There are three solutions for privacy issue while sharing data in EHR/EMRs: consortium blockchain, permissioned private blockchain with smart contracts and permissioned blockchain.

For trust issue and data management in healthcare, simple blockchain technology can be used. For data-integrity and patient control problems, private and permissioned blockchains can be used as a solution. Data leakage problem can be resolved by using Ethereum-based blockchain with smart contracts. Using two loosely-coupled blockchains, the information exchange problem can be resolved. For interoperability problem in healthcare, blockchain with smart contracts and private blockchain can be used.

For the access problem and data sharing problem, three different solutions are provided. However, two solutions in both of them are the same, i.e. Ethereum-based blockchain with smart contracts and consortium blockchain with smart contracts. Only the third solution is different which is permissioned blockchain for solving the access problem and blockchain with smart contracts for the data sharing problem. Therefore, this study has achieved its aim to provide information on specific types of blockchain technology for application to specific issues in the health field.

An important area for future research is the question of handling huge amounts of data storage in the health field, due to the limited capacity of blockchain. As has been pointed out, the problem with the blockchain technology is that data is stored in immutable form, which may create problem in future. Therefore, it is vital that further research investigates a solution to the limitations in blockchain storage capacity, which will enable the revolutionary technology to continue to benefit patient welfare and the effectiveness of the healthcare system.

References

Al-Karaki, J. N., Gawanmeh, A., Ayache, M., & Mashaleh, A. (2019, 24-28 June 2019). *DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain.* Paper presented at the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC).

Al-Megren, S., Alsalamah, S., Altoaimy, L., Alsalamah, H., Soltanisehat, L., Almutairi, E., & Pentland, A. S. (2018, 30 July-3 Aug. 2018). *Blockchain Use Cases in Digital Sectors: A Review of the Literature.* Paper presented at the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).

Alexaki, S., Alexandris, G., Katos, V., & Petroulakis, E. N. (2018, 17-19 Sept. 2018). *Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions.* Paper presented at the 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD).

Alketbi, A., Nasir, Q., & Talib, M. A. (2018, 25-26 Feb. 2018). *Blockchain for government services — Use cases, security benefits and challenges.* Paper presented at the 2018 15th Learning and Technology Conference (L&T).

Asad Ali, S., Aisha Zahid, J., Muhammad, Z., Kainat, A., Aiman, K., & Georgia, S. (2019). Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography, 3*(1), 3. doi:10.3390/cryptography3010003

Aung, Y. N., & Tantidham, T. (2017, 2-3 Nov. 2017). *Review of Ethereum: Smart home case study.* Paper presented at the 2017 2nd International Conference on Information Technology (INCIT).

Barr-Walker, J. (2017). Evidence-based information needs of public health workers: a systematized review. *Journal of the Medical Library Association : JMLA, 105*(1), 69-79. doi:10.5195/jmla.2017.109

Baucherel, K. (2018). History and Applications of Blockchain Technology.

Chakraborty, S., Aich, S., & Kim, H. (2019, 17-20 Feb. 2019). *A Secure Healthcare System Design Framework using Blockchain Technology.* Paper presented at the 2019 21st International Conference on Advanced Communication Technology (ICACT).

Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems, 95*, 420-429. doi:https://doi.org/10.1016/j.future.2019.01.018

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. J. A. I. (2016). Blockchain technology: Beyond bitcoin. *2*(6-10), 71.

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283-297. doi:https://doi.org/10.1016/j.scs.2018.02.014

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). *A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data.* Paper presented at the Proceedings of IEEE open & big data conference.

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems, 42*(8), 1-11. doi:http://dx.doi.org/10.1007/s10916-018-0993-7

Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Computational and Structural Biotechnology Journal, 16*, 224-230. doi:https://doi.org/10.1016/j.csbj.2018.06.003

Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. In (Vol. 26, pp. 91-108). Oxford, UK.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems, 42*(7), 1-7. doi:http://dx.doi.org/10.1007/s10916-018-0982-x

Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. *IEEE Access, 6*, 11676-11686. doi:10.1109/ACCESS.2018.2801266

Hanley, M., & Tewari, H. (2018, 8-12 Oct. 2018). *Managing Lifetime Healthcare Data on the Blockchain.* Paper presented at the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Hyla, T., & Pejaś, J. (2019). eHealth Integrity Model Based on Permissioned Blockchain. *Future Internet, 11*(3). doi:http://dx.doi.org/10.3390/fi11030076

Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018, 18-20 June 2018). *BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange.* Paper presented at the 2018 IEEE International Conference on Smart Computing (SMARTCOMP).

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. J. J. o. t. A. M. I. A. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *24*(6), 1211-1220.

Linn, L. A., & Koo, M. B. (2016). *Blockchain for health data and its potential use in health it and health care related research.* Paper presented at the ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST.

Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018, 9-13 Dec. 2018). *BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records.* Paper presented at the 2018 IEEE Global Communications Conference (GLOBECOM).

Lu, Q., & Xu, X. (2017). Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. *IEEE Software, 34*(6), 21-27. doi:10.1109/MS.2017.4121227

Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics, 35*(8), 2337-2354. doi:https://doi.org/10.1016/j.tele.2018.10.004

Marko, H., Marko, K., Aida, K., & Lili Nemec, Z. (2018). A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry, 10*(10), 470. doi:10.3390/sym10100470

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications, 135*, 62-75. doi:https://doi.org/10.1016/j.jnca.2019.02.027

Meng, W., Wang, J., Wang, X., Liu, J., Yu, Z., Li, J., . . . Chow, S. S. M. (2018). Position paper on blockchain technology: Smart contract and applications. In (Vol. 11058, pp. 474-483).

Mettler, M. (2016). *Blockchain technology in healthcare: The revolution starts here.* Paper presented at the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom).

Mohanta, B. K., Panda, S. S., & Jena, D. (2018, 10-12 July 2018). *An Overview of Smart Contract and Use Cases in Blockchain Technology.* Paper presented at the 2018 9th

International Conference on Computing, Communication and Networking Technologies (ICCCNT).

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering, 59*(3), 183-187. doi:10.1007/s12599-017-0467-3

Nortey, R. N., Yue, L., Agdedanu, P. R., & Adjeisah, M. (2019, 15-18 March 2019). *Privacy Module for Distributed Electronic Health Records(EHRs) Using the Blockchain.* Paper presented at the 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA).

Oliveira, M. T. d., Reis, L. H. A., Carrano, R. C., Seixas, F. L., Saade, D. C. M., Albuquerque, C. V., . . . Mattos, D. M. F. (2019, 20-24 May 2019). *Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications.* Paper presented at the ICC 2019 - 2019 IEEE International Conference on Communications (ICC).

Pham, H. L., Tran, T. H., & Nakashima, Y. (2018, 9-13 Dec. 2018). *A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract.* Paper presented at the 2018 IEEE Globecom Workshops (GC Wkshps).

Qiu, J., Liang, X., Shetty, S., & Bowden, D. (2018, 16-19 Sept. 2018). *Towards Secure and Smart Healthcare in Smart Cities Using Blockchain.* Paper presented at the 2018 IEEE International Smart Cities Conference (ISC2).

Radhakrishnan, B., Joseph, A. S., & Sudhakar, S. (2019, 15-16 March 2019). *Securing Blockchain based Electronic Health Record using Multilevel Authentication.* Paper presented at the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS).

Ramani, V., Kumar, T., Bracken, A., Liyanage, M., & Ylianttila, M. (2018, 9-13 Dec. 2018). *Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems.* Paper presented at the 2018 IEEE Global Communications Conference (GLOBECOM).

Roehrs, A., da Costa, C. A., da Rosa Righi, R., da Silva, V. F., Goldim, J. R., & Schmidt, D. C. (2019). Analyzing the performance of a blockchain-based personal health record implementation. *Journal of Biomedical Informatics, 92,* 103140. doi:https://doi.org/10.1016/j.jbi.2019.103140

Rouhani, S., & Deters, R. (2017, 24-26 Nov. 2017). *Performance analysis of ethereum transactions in private blockchain.* Paper presented at the 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS).

Singhal, B. (2018). *Beginning Blockchain A Beginner's Guide to Building Blockchain Solutions*: Berkeley, CA : Apress : Imprint: Apress.

Theodouli, A., Arakliotis, S., Moschou, K., Votis, K., & Tzovaras, D. (2018, 1-3 Aug. 2018). *On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing.* Paper presented at the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. P. C. (2018, 9-13 Dec. 2018). *BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records.* Paper presented at the 2018 IEEE Globecom Workshops (GC Wkshps).

Wang, X., Feng, Q., & Chai, J. (2018, 8-9 Dec. 2018). *The Research of Consortium Blockchain Dynamic Consensus Based on Data Transaction Evaluation.* Paper presented at the 2018 11th International Symposium on Computational Intelligence and Design (ISCID).

Wong, D. R., Bhattacharya, S., & Butte, A. J. (2019). Prototype of running clinical trials in an untrustworthy environment using blockchain. *Nature Communications, 10*, 1-8. doi:http://dx.doi.org/10.1038/s41467-019-08874-y

Xiao, Z., Li, Z., Liu, Y., Feng, L., Zhang, W., Lertwuthikarn, T., & Goh, R. S. M. (2018, 11-13 Dec. 2018). *EMRShare: A Cross-Organizational Medical Data Sharing and Management Framework Using Permissioned Blockchain.* Paper presented at the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS).

Yang, G., Li, C., & Marstein, K. E. (2019). A blockchain-based architecture for securing electronic health record systems. *Concurrency and Computation: Practice and Experience*. doi:10.1002/cpe.5479

Zhang, A., & Lin, X. (2018). Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *Journal of Medical Systems, 42*(8), 1-18. doi:http://dx.doi.org/10.1007/s10916-018-0995-5

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational* *and Structural Biotechnology Journal, 16*, 267-278. doi:https://doi.org/10.1016/j.csbj.2018.07.004