SAXION UNIVERSITY OF APPLIED SCIENCES

SAXION UNIVERSITY

Bachelor Thesis

BLOCKCHAIN TECHNOLOGY IN HEALTHCARE SYSTEM

HUYNH GIA LAP

481125@student.saxion.nl

481125

Supervised by:

Mr. Ronald Kramer (Saxion University)

Mr. Jan Veuger (Saxion University)

Academic year 2019-2020

May 2020

1. Abstract

Healthcare is a key factor in deciding people's physical and mental well-being, which is why it is often widely recognized as a major contributor to the economy of a country. The quality of society's healthcare system and facilities is considered one of the most important factors in the development of a country. Today almost all medical records are stored in an electronic healthcare record (EHR) system which improves access to clinical data intended to streamline costs. However, EHRs are essentially non-portable and kept on the networks where they were created mainly for purposes of interoperability, security, and liability. This results in a loss of medical quality for the patient and a rise in healthcare costs as the sharing of information between multiple healthcare facilities, spread around different places, is highly dependent on the patient who is not known as the data owner and might not be aware of such treatments obtained.

The objective of this thesis was to investigate is blockchain relevant to the healthcare system and benefits when it was applied to the medical sector. Considering if blockchain can help patient be the owner and have the control of their medical records. With its functions and effectiveness, Blockchain could be the key to change the current health system. While it is not a perfect technology, what blockchain offers can help the healthcare system develop or at least alleviate problems that are occurring.

2. Acknowledge

This thesis represents the final graduation piece inside Saxion University's curriculum. During the last nine months, several different people have helped me during the research execution.

I would like to thank my first supervisor, Ronald Kramer, for giving me the freedom and trust to perform this research in such a novel field of technology, and for always giving me positive feedback during the course of the study. I do want to thank my company coach Jan Veuger for his contribution to my thesis.

Table of contents

3. Introduction

3.1. Problem Description

It is widely known that the quantities of information and data increase every day due to the development of the Internet, especially in the medical field. Medical records play a key role in any practice because it helps to ensure good care for the victim and also become critical in any future conflict or inspection. My company coach- Jan Veuger, considers that blockchain can be a new technology, which innovates the way medical information is recorded and used. Thus, this research focuses on patients' benefit and their records when applying blockchain in the medical sector.

Considering a general rule, medical records of patients are confidential. Only the patients can see them. If anyone wants to see them, they need permission from patients, or at least the permission of the patient's deputy. There is some exclusion to these rules, which are found in the law. It allows other people to see the medical data of patients without their permission.

Nowadays, besides handwritten records, advanced technology makes it possible for patients to access their medical records online. In 2008, it was recorded that less than 10% of healthcare data globally were stored electronically. This has extremely changed within the past 10 years: according to Adane, Muluye and Abebe in their report in 2013, today nearly all patients' records are kept in an electronic healthcare record (EHR) systems. In the 2012 edition of the Physician Sentiment Index, Menachemi & Collum said that 81% of the questioned physicians stated that EHR systems can develop access to clinical data and more than two-thirds believe that an EHR system can enhance patient care with appropriate costs.

In spite of this progress, one big challenge still occurs when it comes to EHR systems: victim information stays largely non-portable. The explanation for this issue is that healthcare data is seen as complex in terms of their data structure and context, which is hard to communicate without a common eco-system and data standard. According to Ivan in his research in 2016, this issue can be defined as an interoperability problem that has developed in part as a result of the independent development of different EHR systems next to each other. Furthermore, healthcare providers act responsibly by interpreting legal criteria such as the United States Health Insurance Portability and Accountability Act (HIPAA). Another argument mentioned in their research in 2016 by Peterson, Deeduvanu, Kanjamala and Boles is that healthcare providers are reluctant to pass information on privacy concerns and fear that other parties may gain a competitive advantage. This results in a lack of continuity of healthcare for the patient as the sharing of information between various healthcare facilities, spread around different areas, is highly dependent on the patient itself who is not recognized as data owner and may not be aware of such treatments received. Consequently, the patient may receive medication and treatments in an inefficient manner, it can lead to a decline in quality and an increase in healthcare costs.

A centralized infrastructure leads to several downsides in the exchange of medical data between various regions and systems. Even if the data structure and semantics could be accepted to address the interoperability issues mentioned, more problems arise with regard to confidentiality, data ownership, data integrity, and liability. For instance, the investigation of benefits can be carried out multiple times, and there is hesitation to share outcomes — which can differ from each other. A complex web of agreements and contracts surrounds data exchange, which is often customized and takes months to set up and manage, and too much money.

Securing data for a centralized network is a difficult job, as possible attacks and vulnerabilities result in a single point of contact that needs confidence for that individual authority. This implies that a great deal of effort is required to ensure that patient information is protected in terms of privacy, ensuring that only approved parties can access the data, reported by Peterson, Deeduvanu, Kanjamala, and Boles. From the ownership perspective and in the legal sense, healthcare providers perceive patient data as their property (Commission, 2012). This creates needless and costly barriers for patients trying to move their medical records to a new place. Present EHR systems are not designed to handle the records of a multi-institutional lifetime. Therefore, patients leave fragmented data around various institutions as life experiences carry them from one health care provider to another. As a result, patients and caregivers lose easy access to past data as healthcare organizations face the burden of keeping records: continuously altering and revising healthcare data in patient contact, trying to catch-up to the illusive valid healthcare profile of the patient. According to Prakash in 2016, this may lead to a bigger issue when it comes to questions of liability not understanding how reliable the patient data really is. For example, international students, when moving to a new country, it is difficult for them to keep track of their individual health status because their medical records are located in their home country and they have to do many check-ups again.

Another problem with regard to the scalability of centrally controlled EHR systems exists. Given that patient data is continuously added, updated or withdrawn to the EHR, it is difficult to predict what kind of infrastructure is capable of managing a continuously that amount of data without impacting the actual output and therefore usability. Therefore, centrally hosted systems may have the potential of upscale computing power in the short term, but due to its predefined data architecture they may face their limits in the long term., reported by Krawiec in his research in 2016.

A technology which might be able to overcome those problems could be the Blockchain technology. This technology allows electronic cash transfer between participants on a strictly peer-to-peer basis without the pressure of going through a middleman, financial institution as an example, managing transactions, and being in charge to avoid double-spending. The basic principle of the Blockchain technology is based on timestamped transactions (blocks) hashed into an ongoing chain of a "hash-based-proof-of-work", forming a record that cannot be changed without redoing the "proof-of-work", better known as Blockchain. It is therefore called a distributed ledger, which records transactions between two parties efficiently and in a verifiable and permanent manner. This concept ignited much media and industry-wide interest to strengthen existing security and scalability issues. Other areas of application such as the sharing of electronic healthcare documents to be able to resolve the difficulties initially identified were reported. In the 2016 and 2017 editions of Gartners Hypecycle for emerging technologies, Blockchain technology has been placed the highest position of the “Peak of Inflated Expectations”. Blockchains in Healthcare are put in the first step of the Hypecycle, named "Innovation Trigger," in which media attention is triggered without an established idea or product.

It is the fact that Blockchain technology is a rather new concept, not many research has been conducted. This illustrates why the need for scientific research is necessary to conclude on the practical potential of the Blockchain technology in the healthcare sector.

3.2. Research Question

Main question: Is blockchain relevant for healthcare and benefits when applying blockchain in the medical sector?

Sub question 1: What are the (dis)advantages of the present used technology in healthcare sector?

Sub question 2: What are the benefits (advantages) of applying Blockchain in the Healthcare?

Sub question 3: Which (public/private) Blockchain (initiative) in this field is the most promising?

Sub question 4: What are the consequences (disadvantages) for the stakeholders if you apply the most promising Blockchain(initiative) in the Healthcare?

3.3. Methodology:

As explained in the introduction, comprehensive research was needed to respond in a scientifically sound way to the initially raised research question. This chapter elaborates on the introduction and provides an insight into how this thesis was carried out. The next section, therefore, describes the research principle that was applied throughout the thesis followed by a description of the research methodology indicating the methods used to address the specified sub-research questions.

Research method:

Identification of keywords and database search

Keywords for database analysis were chosen within the framework of the study in order to enter studies in specific fields of health information systems. Keywords for database analysis were chosen within the framework of the study in order to enter studies in specific fields of health information systems. The keyword search was created from the first results to improve the accuracy of the search. In total, combinations of following keywords were used: “blockchain”, ”healthcare technology”, ”current healthcare system”, ”problems in current healthcare system”, “applying blockchain in healthcare sector”.

The research was carried out on academic databases that have a wide repository of academic studies and high popularity in web-based academic researches.. In this context, google, google scholar, Saxion library were used as the academic databases. The initial search resulted in over a thousand articles. Besides academic data, I also looked for journals, which have articles about blockchain to understand more about this new technology. Moreover, I used youtube to watch interviews of famous people on relevant topics and asked my supervisor or company coach for more information.

Refining results:

In this text, the articles' keywords as well as the titles have been checked. The relevance to the context was considered. Moreover, a set of exclusion criteria was applied to collect articles from reliable sources, and to make sure that received articles suits to the context of the research. Criteria for exclusion were stated as follows, considering criteria for the review:

Papers should be published in English language.

Papers should be published within 10 years.

Papers should appear in peer-reviewed journals.

The objective of the papers should be about blockchain or healthcare system or applying blockchain in healthcare sector.

The target sample of the researches should be related to medical system including healthcare records, doctors, patients, healthcare laws, and healthcare providers.

Systematic literature review:

Within the problem investigation process, the aim of a systematic literature review (SLR) was to determine what is already known about the research subject by defining, reviewing and analyzing existing information related to the research questions raised. The aim was to review existing evidence relating to Blockchain technology and healthcare systems, synthesize the importance of blockchain and medical records, and recognize Blockchain technology advantages and disadvantages when implemented throughout the current healthcare field. According to Budgen and Brereton, one of the key criteria for carrying out a literature review was to execute the analysis in a fair and equitable manner by following a predefined search strategy. This provides a clear understanding of the research subject, which makes it less likely that the literature review findings would be biased. There was no restriction on the form of literature, because searching papers, conference proceedings, and grey literature such as technical reports are useful for the systematic review of literature because Blockchain technology is regarded as a new area without much-developed literature. For each sub questions, I applied different methodology with the aim to find the answer to them. In the end, these sub questions can answer the main research question of this thesis.

Sub question 1: What are the (dis)advantages of the present used technology in healthcare sector?

To research this sub question, I choose literature review method. Reviewing academic articles or previous research about present used technology in healthcare sector to find their strength or weakness of these technologies. Besides that, I also watch presentations of many speakers at the CoinGeek London Conference on Youtube channel to collect relevant information.

Sub question 2: What are the benefits (advantages) of applying Blockchain in the Healthcare?

To answer this question, I read articles and book which are related to blockchain to find out which strength of blockchain that can help medical sector become better. In addition, I reviewed previous research that is related to applying blockchain in healthcare to examine the benefits from it to patients and their medical records.

Sub question 3: Which (public/private) Blockchain (initiative) in this field is the most promising? and sub question 4: What are the consequences (disadvantages) for the stakeholders if you apply the most promising Blockchain(initiative) in the Healthcare?

Because Blockchain is a new technology so there are not many scientific research about applying this technology to healthcare. For this question, I reviewed the efficiency of companies that invest in applying Blockchain in medical sector and find out which Blockchain is the most promising. In addition, watch youtube to attend expert meetings to find the consequences for the stakeholders when applying the most promising blockchain in healthcare. Especially, at the Coingeek conference in London, many speakers discuss about the pros and cons of the public blockchain when applying in the medical sector.

3.4. Objective

There is hardly any human activity that has not been significantly impacted by the effect of emerging technology on access to and knowledge exchange. Specifically, substantial changes within the healthcare system may be accomplished. Today, almost all medical records are stored in an electronic healthcare record (EHR) system which improves access to clinical data intended to streamline costs. However, Electronic Health Care Records (EHRs) are essentially non-portable and kept on the systems where they were created primarily for purposes of interoperability, security, and liability. This results in a loss of medical quality for the patient and a rise in healthcare costs as the sharing of information between multiple healthcare facilities, spread around different places, is highly dependent on the patient who is not known as the data owner and may not be aware of such treatments obtained.

The objective of this thesis was to explore how interoperability problems can be addressed within the framework of Electronic Health Care Record systems by taking advantage of the Blockchain technology to accept the patient as the owner of his patient data. To do this, I need to find the answers for each sub-question and then conclude on the main question.

4. Theoretical Framework

This chapter, having defined the research topic and method, describes the results of the systematic review of the literature carried out during the phase of the problem investigation. The aim is to provide a holistic overview of the research topic already known.

Electronic Health Record (EHR)

According to the ISO/TR 20514 standard (Electronic health record – Definition, scope, and context), an EHR is defined as a "repository of information regarding the health status of a subject of care, in computer processable form". Stead et al. (2005) enhanced this definition by arguing that an EHR "refers to any information in electronic form about a person that is needed to manage and improve their health or the health of the population of which they are a part". To fulfill this definition, an EHR is responsible for gathering information through multiple health care systems and from a variety of sources of personal information, said by Stead MD, Kelly, MD, and Kolodner MD, in their report in 2005. More than that, an EHR is considered as a combination of an EMR and PHR.

Electronic Medical Record Systems (EMRS)

In the early 1970s, electronic medical records systems were created to help monitor information about health care and increase the quality of healthcare. EMRSs' main functions are to automate clinical procedures such as the processing of clinical reports, including administrative duties such as arranging and billing or issuing orders from care providers. Electronic Medical Records (EMR) are developed as a by-product of these administrative functions and are thus created based on the specific requirements of the EMRS (Stead MD et al., 2005).

Personal Health Record (PHR)

Personal Health Records refers to a comprehensive electronic data set including the patient's own documents, treatment reports and electronic copies of health care provider data, according to Stead MD et al. However, the key feature of a PHR is under the control by the patient who is also able to alter the data. According to ISO / TR 20514, "a PHR may have the same architecture as an EHR while still satisfying patient requirements, and can be considered in at least four forms:

1/ A self-contained, patient or consumer-controlled EHR;

2/ The same with 1/ but maintained by a third party such as a web service provider;

3/ A component of an EHR managed by a health care provider and regulated by the patient / consumer, at least partially;

4/ The same with 3/ but maintained and controlled completely by the patient/consumer.

Figure 1 shows the major overlap of all three record systems from the functionality perspective.

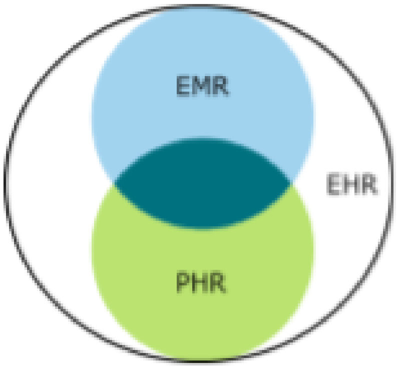


Figure 1: Interrelation EMR, PHR & EHR (own creation in reference to Stead, W., 2005)

Blockchain technology:

Blockchain is simply just a chain of blocks at its most simple level but not in the typical context of those terms. In this sense, when we say "block" and "chain," we're simply thinking about digital information (the "block") that's stored in a public database (the "chain"). "Blocks" are composed of digital pieces of information on the blockchain.

Blocks store transaction details such as the date, time, transactions and also who is involved in the transactions. Blocks store information which differentiates them from other blocks. Each block stores a unique "hash" code that allows us to tell it apart from any other block. Hashes are cryptographic codes generated by special algorithms.

History

Stuart Haber and W. Scott Stornetta identified the first work on a cryptographically secured chain of blocks in 1991. They decided to introduce a program that couldn't tamper with document timestamps. In 1992, Merkle trees were introduced into the design by Bayer, Haber and Stornetta which improved its efficiency by enabling multiple document certificates to be collected in one block.

In 2008, a person (or group of people) known as Satoshi Nakamoto conceptualized the first blockchain. Nakamoto greatly improved the design by using a Hashcash-like method to time-stamp blocks without requiring them to be signed by a trusted party and adding a parameter of difficulty to control the rate at which blocks are added to the chain. Nakamoto adopted the concept in the next year as a central component of the crypto-currency bitcoin, where it acts as the public ledger for all network transactions.. This iterative cycle confirms the validity of the preceding block, all the way back to the initial block of origin.

Blockchain Core Components

Various Blockchain technology definitions have been proposed throughout the SLR whereas there is no standard one. In their 2014 study, Linn and Koo described a Blockchain as follows: “A Blockchain is a peer-to-peer (P2P) distributed ledger technology for a new generation of transactional applications that establishes transparency and trust.” Based on this definition it is possible to derive three main technologies on which the Blockchain technology is based: private key cryptography, P2P networks, and network protocols. None of them are new, but the orchestration and application are new.

Private key cryptography main purpose is to create a secure digital identifiable reference to enforce strong ownership control. This reference is focused on the possession and combination of private and public key establishing a user authentication-responsible digital signature. The aim of using a P2P network in the sense of Blockchain is to achieve consensus among network members (nodes), which confirm that they were simultaneously witnessing the same exchange of information (transaction) via mathematical verification. The use of cryptographic keys in P2P networks results in a useful method of digital interaction considered to be tamper-proof. A transaction from A is achieved by taking its private key, announcing a network transaction, and adding it to B's public key. The network protocol enforces rules for the formation and concatenation of "blocks," preserving a transaction history by hashing a newly created block to the previous one, leading to the creation of the "Blockchain”. The protocol's objective is to prevent the use of the same information in different transactions leading to potential double-spending, and to ensure that the blocks are considered legitimate and trustworthy (Liang et al., 2017; Nakamoto, 2008; Petek, 2017). To achieve this aim, it is important to note that the size of the network (number of nodes) is essential to support its own protection. Permission-less blockchains use the economic theory, which is called "the tragedy of the commons," to draw computing resources to support the network and make it stable (Hardin, 1970). Miners' function offering computing power to support the network by earning a reward for block formation (in the case of the Bitcoin Blockchain, Bitcoins). Therefore, a person's self-interest is used to help serve the public need (Petek, 2017)

Mizrahi et al. defined the mining process according to the Proof-of-Work (PoW) principle as follows:

1. A miner collects transactions that are transmitted over the network and use her hash power to try to create a block by repeatedly invoking a hash function on data that consists of the transactions she saw fit to include, the previous block's hash, its public key address, and a nonce.
2. When a miner succeeds in producing a block, which means her block data hash is smaller than the current competition goal, she broadcasts her block to the network.
3. When other miners see that this block is valid, i.e. it corresponds to the hash of the previous block and meets the current difficulty goal, and see that it is the longest extension of the block chain (a.k.a. Blockchain) they are aware of, they move on to continue expanding the blockchain from this block "(Bentov, Lee, Mizrahi, & Rosenfeld, 2014).

In conclusion, all transactions are held in the Blockchain and are exchanged between all nodes. The combination of the above-mentioned three components ensures verifiable and unchangeable transactions; manipulates resistance, accountability and integrity of the distributed data because there is no single point of failure in the network (Zhang, 2015).

The primary interface that is responsible for communicating with the Blockchain is a wallet that proposes and accepts cryptographic records reflecting the value of transactions made. A user's public key is used in a wallet's address to ensure security across the network and the user authentication uses the private key. It should be remembered that the wallet is not a central component of a Blockchain network and thus does not have the same safety features (Yli-Huumo et al. , 2016).

A component that leads to a more flexible Blockchains application is known as a smart contract. Smart contracts are seen as an application that automatically transfers digital assets across the Blockchain network based on arbitrary pre-specified rules. This can be, for example, a currency withdrawal rule or user access right predefined. The network of mutually distrusting nodes performs smart contracts sequentially, without the arbitration of a trusted authority. This idea was first implemented by the Ethereum Blockchain including the functionality that transactions or function calls from other contracts can trigger and execute smart contracts. (Bartoletti & Pompianu, 2017; Buterin, 2014; Zhang, 2015).

Blockchain Types

In general, Blockchain technologies can be classified into three types: permission-less, permissioned and hybrid systems.

The key feature of Blockchains without permission, such as Bitcoin or Ethereum, is that node identities are either pseudonymous or anonymous with the possibility of entering and leaving the network at their will, and supplying hashing power by miners. The design of permissionless Blockchains is useful for the exchange of values where node recognition is negligible as long as consensus exists. This design might not be sufficient for business applications due to a variety of factors, such as increased risk of network instability for nodes that unexpectedly quit the network and thus hinder the throughput, which should be avoided in particular for healthcare data (Dubovitskaya, Xu, Ryu, Schumacher, & Wang, 2017).

Permissioned blockchains provide similar functionality to permission-less Blockchains, but function in environments where users have checked identities and are allowed to participate by accepting unique user access rights. This may be useful for business applications where defined nodes are needed for legal and enforcement reasons. As a consequence, the process for achieving consensus among the distributed nodes, achieved via PoW for permission-less Blockchains, can be achieved based on state machine replication algorithm, according to Dubovitskaya et al. in 2017. The SLR reported that byzantine-fault-tolerance (BFT) algorithms are widely used to achieve consensus in permissioned Blockchains. Pease, Shostak, & Lamport (1980) explain that, in the presence of up to f Byzantine faulty nodes, at least 3f+1 nodes are required to achieve consensus (Gervais et al., 2016; Vukolić, 2017). Note that BFT implementations can only scale to a limited number of nodes, resulting in more network participants, this could lead to worse performance but faster compared to PoW. In addition, this definition includes a (logically) centralized identity management where trusted parties issue identities and cryptographic certificates that are deemed a drawback to permission-less environments (Luu et al., 2016). Examples of permissioned Blockchains include Ripple, Hyperledger-Fabric / Sawtooth and Tendermint.

The hybrid systems approach is to take advantage of the Blockchain characteristics defined without getting its drawbacks or advancing over the existing architecture. Due to the variety of solutions available, it is difficult to achieve a general characterisation and classification of such hybrid technologies. An example of such a technology will be the "tangle," which is IOTA's underlying technology and is known to be a directed acyclic graph (DAG) for transaction storage. The tangle has been built without transaction fees for Internet-of-Things (IoT) applications that have a high transaction throughput. This particularly happens through the indirect validation of at least two transactions directly and other transactions in the sub-tangle. This allows validations to be carried out in parallel while the network remains decentralized without the need for PoW. This theory makes the device highly scalable as long as there are enough nodes involved (Popov, 2017). By adopting the concept of "blockchainifying" a large data base such as NoSQL (in the case of BigchainDB, a MongoDB) with consensus algorithms (BFT) on top of the database layer, BigchainDB can be viewed as another hybrid technology. Blockchain features such as decentralization, immutability, and built-in asset development and transfer support are guaranteed with reasonably high scalability (about 1000 transactions per second) compared to traditional Blockchain solutions (Mcconaghy et al . , 2016).

Advantages and Disadvantages of Blockchain technology

The potential of blockchain as a decentralized form of record-keeping, for all its complexity, is almost limitless. From improved user privacy and enhanced protection to lower transaction costs and fewer errors, blockchain technology will see applications beyond the above-mentioned applications.

Advantages:

- Accuracy of the Chain

Transactions are accepted by a network of thousands or millions of computers on the blockchain network. This removes virtually all human intervention in the verification process, resulting in less human error, and more reliable evidence recording. Even if a computer on the network were to make a technical mistake, one copy of the blockchain would just make the error. To order for the mistake to spread to the rest of the blockchain, at least 51 percent of the computers on the network will need to be made — a virtual impossibility.

- Cost Reductions

Consumers usually pay a bank to validate a transaction, a notary who signs a contract, or a marriage minister. Blockchain removes the need for authentication by third parties and, with this, their related costs. Business owners incur a small fee if, for example, they accept payments using credit cards, because banks have to process such transactions. On the other hand, Bitcoin has no central authority and almost no transaction fees.

- Decentralization

Blockchain has no central place to store all of its information. Instead, the blockchain is copied and distributed over a computer network. Whenever a new block is added to the blockchain, each computer on the network updates its blockchain to represent the change. Blockchain is more difficult to tamper with by spreading the information across a network, rather than keeping it in one central database. If a copy of the blockchain falls into a hacker's possession, then just one copy of the database will be compromised, rather than the entire network.

- Efficient Transactions

It may take up to a few days to settle transactions put through a central authority. For instance, if you attempt to deposit a check on Friday night, you may not actually see funds in your account until Monday morning. Whereas financial institutions operate five days a week during business hours, blockchain operates 24 hours a day, seven days a week. Transactions can be completed in about ten minutes, and after a few hours, it can be considered safe. This is particularly useful for cross-border transactions, which typically take much longer due to time zone problems and the fact that both parties have to validate the processing of payments.

- Private Transactions

Many blockchain networks function as public databases, meaning that anybody with an internet connection may display a list of the transaction history of the network. While users can access transaction details, they can not access identity information regarding users making those transactions. It is widely assumed that blockchain networks such as bitcoin are anonymous when they are in reality just confidential.

That is, when a user makes public transactions, the blockchain registers their unique code, called a public key, rather than their personal information. Although a person's identity is always connected to their blockchain address, this prevents hackers from stealing personal information from a customer, as may happen when a bank is hacked.

- Secure Transactions

If a transaction is recorded the blockchain network must check its validity. Thousands or even millions of computers running through the blockchain to confirm that the purchase details are right. After the transaction has been validated by a computer, it is added to the blockchain in the form of a block. Every block on the blockchain has its own unique hash in it, along with the block's unique hash before it. When the information on a block is changed in some way, the hash code on that block changes — however, the hash code on the block after it does not. The disparity makes it incredibly difficult to alter without warning details about the blockchain.

Disadvantages:

While the blockchain is experiencing major upsides, its adoption still poses significant challenges. Today's roadblocks on using blockchain technology are not only technological. In the most part, the main obstacles are political and regulatory, to say nothing of the thousands of hours of custom software design and back-end programming required to incorporate blockchain into existing business networks. Here are few of the obstacles that stand in the way of widespread blockchain adoption.

- It’s New:

Since 2008, when a white paper called "Bitcoin: A Peer-to-Peer Electronic Cash System" was released by Satoshi Nakamoto, there has been much talk to this day about what blockchain can enable. Many businesses are clamoring to develop healthcare capabilities with blockchain, but very little is ready for development. Innovation teams are reviewing design proofs but tend to be reluctant to step into full use. The platforms are complex, their capabilities are evolving, and support resources are scattered around the same. To read more about blockchain systems, check out Hyperledger and Etherium.

- It’s Misunderstood:

Blockchain credibility has been founded on Bitcoin and many are struggling in health care to see the connection and equate it with the risk of privacy. Though fascinating possibilities are being explored around token-based healthcare systems — check out the announcement made by Hashed Health on Bramble as a good example — the scenario I describe above is not a token-based blockchain, and most likely would not be publicly “mined.” Instead, they will handle the blockchain inside a semi-private environment. While the patient will eventually be in charge of their chain data, the fact is that the entities that help the patient would eventually be the validating sources of patient information. Such ambiguity about blockchain in the public or private domain confuses development.

- It Requires Collaboration:

The above scenario also requires that all the companies that support patient care align themselves with the need to improve how data is managed. They must be ready to accept the pace of sharing of information and the transparency on the process that will offer blockchain-enabled patient data management. They need to come together and adopt modern standards of reading and writing, and invest in new technologies.

Blockchain also has the power to alter the economics and influence of the parties, and some are not in a rush to alter the dynamics. The good news is collaboration is happening! As an example, Change Healthcare offers real-time claims submission and remittance on blockchain and HealthVerity company, which offers blockchain-enabled consent management.

5. Sub-question 1: What are the disadvantages of the present used technology in the healthcare sector?

It has been shown that Electronic Health Record (EHR) play significant roles in the health care system. The major factors for EHR's rising role and implementation in healthcare systems include the need to enhance healthcare delivery quality, patient safety, improved access to healthcare services and, more fundamentally, the need to reduce medical spending costs. EHR has become very helpful in the system of healthcare in different ways, ranging from clinical care application to administrative function, clinical research function, financial application and healthcare reporting. EHR is not only a digital version of a paper medical record but also offers the following clinical functions: physician order entry, comprehensive view of patient information and data, access to knowledge databases, support for clinical decision making and comprehensive communication.

There has been an increasing interest in EHR adoption in a number of countries recently. This is attributable to an growing awareness that a stronger health information technology (HIT) is essential for delivering a better quality treatment at lower prices. EHR has been recognized as a key integral part of an efficient information system for health care which guarantees positive health consequences. EHR is described as " a repository of patient data in digital form, stored and exchanged securely, and accessible by multiple authorized users," according to the International Organization for Standardization (ISO), “It contains retrospective, concurrent, and prospective information and its primary purpose is to support continuing, efficient, and quality integrated health”.

It holds major functions in the healthcare system, and has been integrated in the healthcare system in particular ways. Many researches conducted in various healthcare conditions have shown that wide and reasonable application of EHR in the healthcare system can help healthcare professionals minimize medical errors, achieve greater effective coordination of treatment, strengthen patient safety and quality of treatment, and reduce cost of health care. For instance, by making information accessible electronically for a specific patient, health care information systems can help avoid ordering of repeated tests and procedures, thus reducing consumer's expenditure on health care services. Furthermore, the availability of medical records in digital form will lessen the expenditure on the storage, recovery and patient charts transporting in the health record department.

Different options for classifying EHR-Architectures were noted in the SLR. Two wide categories of shareable and non-shareable EHR-Systems were recognized. Without the possibility of exchanging EHRs outside the immediate boundaries of a single healthcare organization, non-shareable EHR-Systems may be viewed as a stand-alone solution. The features of a shareable EHR-System are that data on healthcare can be exchanged among various levels (i.e. across different clinical fields, different applications or through different EHR-Nodes). Although for EHR-Architectures there is no formally specified classification, the following three distinctions could be defined: centralized architecture, de-centralized architecture, and semi- centralized architecture further described below. (Al Jarullah & El-Masri, 2012; International Organization For Standardization, 2005)

- Centralised-Architecture

It can be compared between the centralized architecture and the classical client-server infrastructure. You may equate the unified architecture with the conventional client-server network. Comprehensive or simplified types of EHRs are transmitted within this type of architecture to a central (preferably nationwide) network that is considered the repository for all patient records. The data transmission method is understood as the "push-model" through which the healthcare provider periodically or in near-real time "pushes" the patient data to a central repository. The benefits of such an architecture are the simplicity of the program, the efficiency and the response time to queries. Notable drawbacks in terms of data context and codification are relevant to interoperability concerns. Other disadvantages, as stated briefly in the introduction, are the increasing risk of possible attacks on the central repository requiring a high measure of protection resulting in higher design requirements and costs (Al Jarullah & El-Masri, 2012). In Europe, Denmark, Finland, England and Estonia have adapted this strategy on a worldwide scale.

- De-Centralised Architecture

It is possible to equate de-centralized architecture with traditional peer-to - peer infrastructures. All EHRs will be handled by the respective health care provider and managed locally. A central repository will maintain references showing where the patient data was stored. This principle is known as the "pull-model" where any time an EHR patient is released, an agent stored on the central reference repository will request all the data that is required from the various providers. Therefore, patient data is only generated on request, which contributes to the benefits of data consistency when accessing the latest version of the EHR locally. This is considered to secure patient data better than central privacy and security-related systems, because patient data remains at the source, rather than being duplicated in a central database. Disadvantages in terms of query efficiency have been found by accessing the EHR due to inevitable latency and incompatible security models for the data collection process. It is understood that such an architecture is appealing in principle, but the performance-related disadvantages (i.e. efficient distributed queries, short latencies and compatible security models) need to be addressed in order to provide a effective de-centralized EHR (Al Jarullah & El-Masri, 2012). That architecture is adopted in Europe in the Netherlands known as AORTA and Austria known as ELGA.

- Semi-Centralised Architecture

AlJarullah et al. (2013) present an architecture that benefits from both centralized and de-centralized architecture in the paper "A Novel Network Architecture for the National Incorporation of Electronic Health Records: A Semi-Centralized Approach" This architecture centrally maintains the summarized EHRs and provides a reference to the comprehensive EHR stored locally by the healthcare provider. “The idea to allow the clinicians to have an idea of what is included inside the patient’s EHRs at each healthcare provider from a central location and to have a general view of the patient’s medical history, and when needed, retrieve the complete EHR of the patient from a remote healthcare provider’s system”, said in the paper. This architecture has the benefit of easy access to condensed EHRs with the option of retrieving the full record as needed while preserving interoperability. While this architecture takes advantage of both the centralized and de-centralized approach, regarding this architecture no countries in Europe have a national EHR.

Despite the increasing literature on the advantages of various EHR functionalities, some authors have found possible drawbacks associated with this strategy. Which include financial problems, process improvements, temporary efficiency loss associated with the implementation of EHR, privacy and security concerns, and other unintended impacts.

Financial difficulties, including the cost of adoption and implementation, continuing maintenance costs, revenue loss associated with temporary productivity loss, and revenue decreases, pose a disincentive for hospitals and physicians to embrace and incorporate an EHR. The cost of adopting and implementing EHR involves purchasing and updating hardware and software, converting paper charts into electronic ones, and training end-users. In both the inpatient and outpatient settings, many studies have documented those costs. In a survey conducted in a 280-bed acute care hospital in 2002, the overall estimated cost for a 7-year-long EHR implementation project was around US$ 19 million. Early researchers calculated an initial average cost of US$ 50,000–US$70,000 per physician for a three-physician office in the ambulatory setting. Nevertheless, as EHR technologies have become more popular over the past decade, the system's initial cost has shrunk drastically. One industry group projected a cost of about US$ 14,000 per physician in the initial year of implementation for a six-physician practice and US$ 19,000 per physician with three or fewer physicians, for hardware, software, utilities, and telecommunications. Likewise, a recent report reports initial software, preparation, and implementation costs of US$ 22,038 and equipment costs of US$ 13,000 per Full-time-equivalent (FTE) provider in a primary care practice for individuals or small groups.

An EHR's maintenance costs can be expensive as well. Hardware should be replaced, and software should regularly be upgraded. Additionally, suppliers must provide ongoing training and assistance to an EHR's end-users. An approximate ongoing EHR maintenance costs averaged US$ 8412 per FTE provider per year according to one study conducted on 14 single or small group primary care practices. A total of 91% of this expense had to do with hardware replacement, manufacturer software repair and service costs, and compensation for employees or external contractors in the information systems. Many estimates of continuing maintenance costs in a medical group of five for the first year after implementation were about US$ 17,100 per physician.

The cost of EHR adoption, implementation, and ongoing maintenance is exacerbated by the fact that many of an EHR's financial benefits usually do not accrue to the vendor (who is expected to make the initial investment) but to the third-party payers in the form of averted errors and increased efficiencies, which result in decreased claims payments. This misalignment of health care organizations resources combined with the high upfront costs poses a barrier to the adoption and implementation of an EHR, especially for smaller practices. In reality, doctors often cite initial costs and ongoing maintenance costs as the greatest obstacles to an EHR being adopted and enforced.

Another downside to an EHR is work-flow interruption for medical personnel and suppliers, which results in temporary productivity losses. The productivity loss results from end-users learning the new program, which can contribute to sales losses. One research involving several internal medicine clinics reported a productivity loss of 20% in the first month, 10% in the second month and 5% in the third month, with productivity returning to its original rate later. In that report, the productivity loss led in the first year to a loss of revenue of US$ 11,200 per provider. In a sample of one to six FTE providers in solo and small-group primary care practices, revenue losses from decreased visits during the initial stages of an EHR averaged around US$ 7,500 per FTE provider. Whether doctors worked longer hours during this stage or that patient visits depended on that. Finally, researchers found that end-users of the EHR spent 134.2 hours on implementing activities related to having and understanding a new program. Such hours spent on non-clinical tasks had an average cost of 10,325 US dollars per doctor.

Following introduction of the EHR, further decreases in revenue are likely. Because EHRs are often associated with fewer redundancies, fewer errors and shorter lengths of stay, it is conceivable that a given provider may avoid certain billable transactions which, while superfluous, may have created reimbursements from third-party payers, especially in a fee-for-service payment system. Although reimbursement rates can vary for each entity, these declines may be offset by increased revenue generated by efficiencies achieved by an EHR program.

Another potential drawback of EHRs is the possibility of patient privacy violations, which is a growing problem for patients because of the increasing volume of electronically transmitted health information. To address some of these issues, policy makers have taken action to ensure patient data protection and privacy. For instance, recent legislation has introduced regulations specifically related to the electronic sharing of health information which strengthen existing privacy and security policies in the Health Insurance Portability and Accountability Act. Moreover, all EHR systems require an audit feature that enables system operators to recognize each person who has accessed every element of a given medical record. Many hospitals and doctors impose stringent, no tolerance policies for workers who have unauthorized access to the archives. A hospital in Arizona, for example, fired multiple employees after they illegally accessed the records of victims who were hospitalized during a shooting involving a US Congresswoman in January 2011. While privacy is likely to continue to be a problem for patients, governments and individual organisations are taking several measures to ensure that EHRs comply with the stringent laws and regulations designed to protect the privacy of clinical information.

EHRs may cause many unintended effects, such as increased medical errors, negative feelings, power system changes, and technology over-dependence. As stated earlier, due to poorly configured device interfaces or lack of end-user training, researchers have found an association between using CPOE and increased medical errors. In addition, end users of an EHR can experience strong emotional responses as they struggle to adjust to new technology and workflow disruptions. Changes in an organisation's power structure can also arise due to an EHR being introduced. Overreliance on technology can also be a issue for providers, as they are more dependent on it. Organizations should ensure that basic medical care can still be delivered without technology, especially in periods when device failure can be crucial. Although there are many unintended consequences of EHRs, they are beneficial, particularly at the level of community, while balancing the advantages and disadvantages of such systems.

In conclusion, for the question “What are the disadvantages of the present used technology in the healthcare sector?”, EHR plays an important role in the medical profession in general and patient data management in particular. Although applying EHR to the healthcare system can help healthcare professionals reduce medical errors, achieve more effective treatment coordination, enhance patient safety and quality of treatment, and reduce health care costs, there are many disadvantages of this system. The first one is the cost of adoption and implementation, the cost of maintenance are high, healthcare departments may spend a lot of money for the initial use of the EHR system. Moreover, the EHR system affects negatively the work-flow of employees, this could the loss in revenue associated with temporary productivity loss and the decline in revenue pose a disincentive for hospitals and doctors to accept and integrate an EHR. Besides financial drawbacks, EHR faces many challenges such as: increased medical errors, negative feelings, shifts in the power system and over-reliance on technology. The biggest disadvantage of the current EHR system is the infringements of the patient's privacy. Due to these downsides, the healthcare industry need new technology, which can help it overcome or at least reduce these problems.

6. Sub-question 2: What are the benefits (advantages) of applying Blockchain in the Healthcare?

Blockchain technology will overcome many of the challenges the healthcare industry currently faces. These issues concern medical data (security, interoperability, accessibility), medical research, clinical trials, chain of medical supply, and quality of drugs. Even the largest health care firms are troubled by these issues. Blockchain's ability to provide unprecedented data efficiency will disrupt healthcare. It also ensures flexibility, interconnection, accountability and protection in the access to data.

Most medical institutions currently employ outdated and inconvenient methods to handle medical data. This includes numerous e-health reports, data on prescription medications, information on insurance, and medical data for patients. Improper management of data affects the care of patients, as well as the pace of that care. The problem is worsened by the fact that most health care services have their own methods of processing and accessing medical data in the healthcare sector.

The transparency of information

Medical data on patients are spread across many medical facilities, insurance providers, and physicians. Today, the medical records and history of a patient are something of a puzzle. This jumbling of data results in a lack of credibility and precision. This refers in particular to drug prescriptions, health recipes, and diagnostics. These factors all have an impact on proper treatment. Difficulties in gathering accurate data on patients can also often mean the difference between life and death. Currently there is no universal data storage system, nor are acceptable standards in place. This is where Blockchain and medical sector will come together to develop healthcare applications.

Using Blockchain technology in healthcare may make a difference to data management world. The technology will make the sharing of medical data more effective, safer and more transparent across the entire health care sector. Imagine a network on healthcare institutes where they do not own personal data of a patient. The details are all part of the blockchain. The patients are identified through their hash identification which will be their unique identifier. The hashing allows the ID to be unique, and protects the user's privacy. The blockchain can also aid in building a platform for the exchange of patient information. Through this way, it would be possible to actively facilitate the exchange of information between the different institutes in order to avoid any kind of info blocking. But what if we still have some malicious actors who seek to block or tamper with information? In this case two of the most important aspects of the blockchain should step up to deal with this situation: First, the blockchain is a transparent tool. Anyone who is part of the network will look at the blockchain to see how each transaction happens and whether or not any of the relevant information is passed through. Second, we got anti-tampering. If anyone wants to block the data then it will dramatically alter the hash through the snowball effect. Every block in the blockchain stores the data hash that is stored in the preceding block. When the data within any of the blocks alters, a chain reaction is set up which could freeze the entire blockchain. Because this is a theoretical impossibility, any data that is within the blockchain can not be tampered with.

The consistency of information

In spite of being considered an unethical activity, information blocking in the healthcare sector has been a problem. In the medical sector, reported by Blockgeek blocking data of patients is recognized as the result of “an unreasonable constraint imposed on the exchange of patient data or electronic health information”. According to the U.S. Office of the National Coordinator for Health Information Technology, there are three conditions for blocking information: interference; knowledge; there is no justification why data should not be accessible.

It goes without saying that information blocking activities involving unnecessary intervention and perception are an enormous detrimental to successful practice in healthcare. Blocking can be attributed to laws that discourage knowledge sharing as well as activities that make sharing highly impractical. The explanation for that is very plain. Hospitals do not want to miss out on patients and want to make going to another hospital as difficult as possible for them to want to. This should have been a draconian practice in this digital era but various surveys and studies say otherwise. Following survey of 60 HIE leaders. It has been discovered that the blocking of information is extremely widespread and that the various steps taken to curb it remain extremely inefficient. In fact, 50 percent of respondents who have been surveyed by Adler-Milstein have reportedly been involved in information blocking with health IT companies. A quarter of these respondents have said this practice is guilty to hospitals and health systems. According to the researchers one of the following methods will curb information blocking:

- By increasing clarity so that every action which has been taken by members can be accounted for.
- Good financial rewards should be given so that the participants would like to exchange data
- A collaborative partnership between health-care IT firms, hospitals and HIE could further prevent blocking of information.

Blockchain technology can help set up medical records from Blockchain. This reduces unnecessary administrative costs and also enables better use of health data. In addition, the use of the software can reduce the need to contact various intermediaries to oversee the exchange of essential health information. As stated earlier, the medical data of a single patient can be split across several facilities, doctors, and insurance providers. This means the whole medical history of a patient is always distorted or incomplete. Virtual medical records stored on a Blockchain can help health sector parties unite all parts of the health data puzzle. Therefore, with patient's records, the medications they've received, completed procedures, facilities used, and other details will also be up-to-date and digestible by anyone concerned. It will go a long way towards simplifying the key role of health care professionals, which is to provide patients with reliable, timely and proper treatment. Through using Blockchain technology in the healthcare field, service providers will still have a clear image of the medical record of any given patient. It is crucial to note and recognize that all past health data is immutable in a Blockchain and healthcare environment, and any improvements to that data are obvious.

The guarantee of information storage.

Effective control of medical data is one of the main advantages of Blockchain and healthcare. Many problems that concern the healthcare sector can be avoided, including interoperability, data completion, abuse, and even data loss during a disaster. It is worth noting also that Blockchain technology will work wonders in terms of recovery from the disaster. Critical to providing adequate medical services is the ability to ensure that health data is correct. Exposure to appropriate medical records means that health care providers can provide an accurate diagnosis. This is further emphasized by the fact that any modifications to it are almost impossible until any data reaches a Blockchain. It is worth noting that medical information can be processed in a Blockchain from various sources, such as patient files, wearables, mobile devices, labs, EMR's, etc. Healthcare blockchain will help in reducing medical companies' costs.

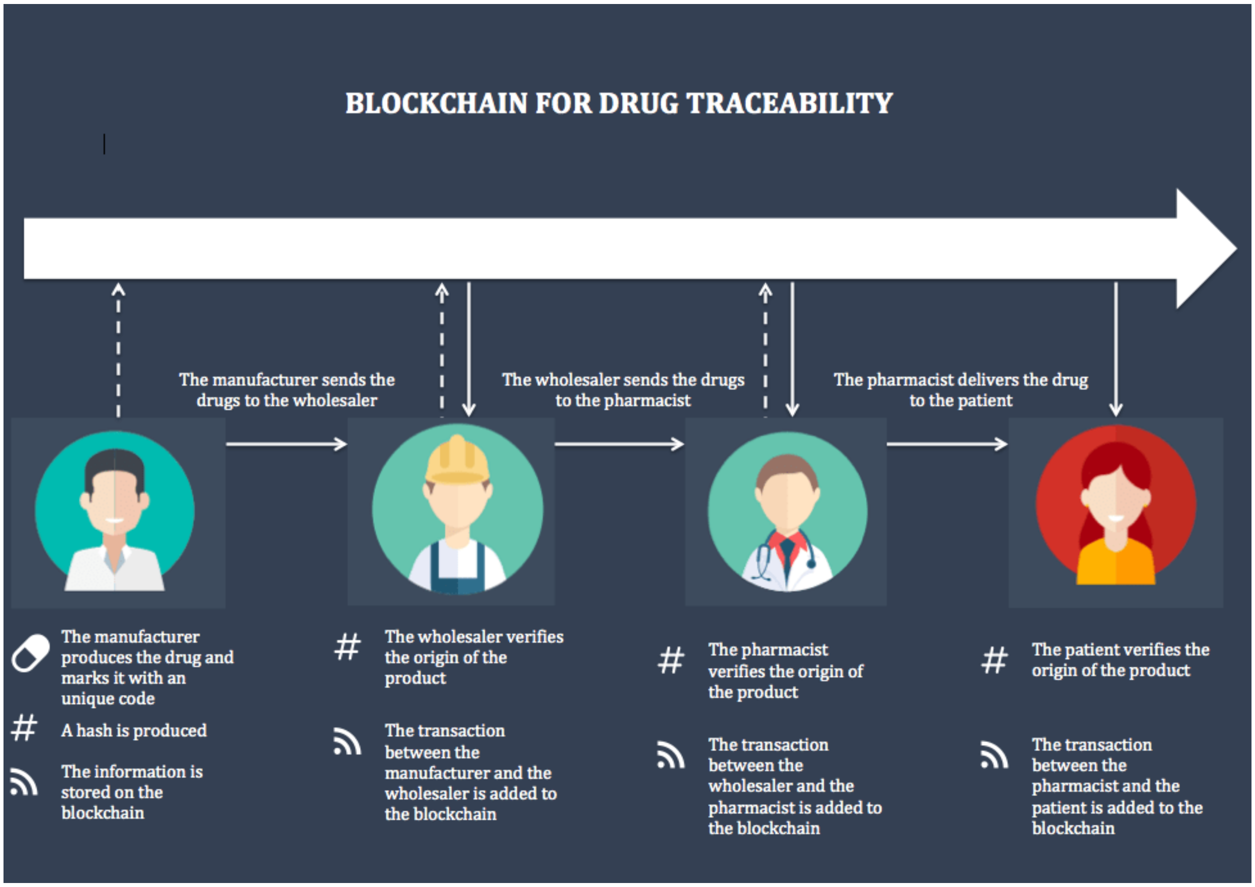
Reducing fake drug status

Falsification of medications or fake drugs is a major concern in the pharmaceutical industry. Below are some metrics reported by the Health Research Funding Organisation:

- Ten to thirty percent of the drugs which are sold in developing countries are counterfeit;
- The counterfeit drug market is worth $200 billion a year;
- Sales of counterfeit products on the Internet constitute $75 billion of the global market;
- The bulk of counterfeit drugs are manufactured in India and China;
- In 2014, about 60 different Pfizer medicines and products were being counterfeited around the world.;
- WHO estimates that 16% of counterfeit drugs contain the wrong ingredients, while 17% contain the wrong levels of necessary ingredients.

Another important field in the healthcare sector where use can be made of Blockchain and healthcare is medication traceability-not only prescription traceability but even counterfeit drugs. All data entered in a Blockchain is permanent and marked with time. It, in addition to prescription mishandling, reduces the possibility of counterfeit products to enter the black market. Regardless of the type of product they produce, Drug companies need to have an incredibly safe supply chain. Pharmaceutical products are stolen regularly from the supply chain to be illegally marketed to different customers. These companies also lose money for counterfeit drugs, almost $200 billion per annum. In a more financial viewpoint, product counterfeiting causes an annual loss for the European pharmaceutical industry of €10.2 billion, and 37,700 jobs are lost as producers hire fewer workers than they would if fake medicines were not there.

The companies which register a product on the blockchain must be trustworthy to ensure the validity and traceability of the products. Therefore, it is only fair for private blockchains operated by a central authority to ensure that fake drugs are not registered. Entry to the "drug blockchain" will then be a claim by a corporation that the products they manufacture are genuine. The companies determine which supply chain actors operate as miners. It may be suppliers, distributors or retailers. Depending on the supply chain role, each individual will have different rights: laboratories can register drugs while wholesalers can only confirm transactions. When a drug is made, a hash is created which contains all the relevant product details. The information is stored on the blockchain each time the drug travels from one individual to another (example: from the producer to the distributor), making it easy to track the drug. In December 2019, many businesses such as KPMG, Merck, Walmart, and IBM completed the Drug Supply Chain Security Act (DSCSA) Interoperability Pilot as part of the U.S. Food and Drug Administration (FDA) DSCSA Pilot Project Program. The results of the pilot show that using blockchain technology can dramatically reduce the time taken to track a prescription drug — from up to 16 weeks to 2 seconds. Besides providing visibility of the supply chain, the pilot leverages blockchain to improve the protection of patients and patient safety. The application helps users to locate, investigate, and interact easily and efficiently about a particular criminal or illegal drug product. Moreover, if a problem is found and a sample needs to be removed from the market, blockchain technologies make it easier for the manufacturer to locate its drugs and thus prevent any complications. Blockchain technologies help with two key issues when it comes to drug traceability: firstly, it helps businesses to track their drugs down the supply chain, creating an airtight network, impermeable to counterfeit goods. Secondly, it also helps stakeholders, and especially laboratories, to take a posteriori action in the case of a problem by recognizing the exact position of their drugs.


BLOCKCHAIN FOR DRUG TRACEABILITY
The manufacturer sends the drugs to the wholesaler
The wholesaler sends the drugs to the pharmacist
The pharmacist delivers the drug to the patient
The manufacturer produces the drug and marks it with an unique code
A hash is produced
The information is stored on the blockchain
The wholesaler verifies the origin of the product
The transaction between the manufacturer and the wholesaler is added to the blockchain
The pharmacist verifies the origin of the product
The transaction between the wholesaler and the pharmacist is added to the blockchain
The patient verifies the origin of the product
The transaction between the pharmacist and the patient is added to the blockchain

In conclusion, for this question “What are the benefits (advantages) of applying Blockchain in Healthcare?”, Blockchain is more than a technology, it is a movement that, through trust, transparency, and collaboration, will help all industries redefine their most important relationships. Much research shows that Blockchain technology can be applied in many industries including the medical sector. In the healthcare sector, companies are enhancing patient care by enabling their blockchain platform to ensure trust, data provenance, and efficiency. With its function, blockchain can make patients' data be more transparent, consistent, and store it in a safe area. More than that, this advanced technology can help medical institution track their drug, which could lead to a decline in fake drug status. From patient's perspective, applying blockchain in medical field can help them access and manage their medical data easier and safer.

7. Sub question 3: Which (public/private) Blockchain (initiative) in this field is the most promising?

Implementations of blockchain can be either public or private. Anybody can participate in a public deployment, and the network is open to everyone. There is usually some motivation for public versions to allow users to enter the blockchain. Bitcoin, currently the world's largest public blockchain, is the most commonly recognized example of a decentralized blockchain. In a private blockchain, all of the participants are known. It needs an invitation to participate in a private blockchain. Private blockchains usually operate on a permissioned network to further limit network participation. An example of a private blockchain implementation would be to grant licenses to a regulatory authority for participation in the network. The primary use of a public blockchain is to decentralize the networks and offer secure transparency. Contrastly, when more control and privacy are needed, private and consortium (semi-private) blockchains are preferred.

There are three types of blockchains: public, private, and consortium. There are major similarities of three types: Firstly, it is an append-only ledger – to qualify as a blockchain, a system needs to follow the chain of blocks structure, wherein each block is linked to the last. If blockchain is the set of cells in a spreadsheet, the blocks are the individual cells. Secondly, a peer network – each Network participant holds a copy of the blockchain. Such participants are called nodes, and they communicate in a peer-to-peer fashion. Thirdly, a mechanism – there must be a mechanism for nodes to agree on the correctness of network-wide transactions to ensure that no fake data are written into the chain. Besides these similarities, each type has different aspects. The table below sums up some of the major differences.

	Public blockchain	Private blockchain	Consortium blockchain
Permissionless?	YES	NO	NO
Who can read?	Anyone	Invited users only	Depends
Who can write?	Anyone	Approved participants	Approved participants
Ownership	No body	Single entity	Multiple entities
Participants known?	No	Yes	Yes
Transaction speed	Slow	Fast	Fast

The pros and cons of public blockchain:

One of the greatest advantages of public blockchain is that there is no need for trust. All are registered, public, and is unchangeable. Everybody is motivated to do what is best for network development. There is no need for intermediaries. The other major benefit is that of security. When more people operate on the network, every form of attack becomes more difficult to be a success. Banding together and taking the power of the network is virtually impossible for malicious actors. Transparency is the final piece of what makes public blockchain succeed. All transaction-related data are open to verification by the public.

With public blockchain one of the biggest problems is block size. This system can lack scaling (block size), this could lead to congestion, and it negatively affects the speed of this system. Public blockchains like Bitcoin are incredibly sluggish, managing just seven transactions per second to process. Public blockchains are slow because it takes time to reach a consensus for the network. In addition, public blockchain needs more time to process a single block than private blockchain. Indeed, the more use is made of a public blockchain, the slower it gets as more transactions clog the network.

The pros and cons of private blockchain:

Speed is one major benefit of private blockchain. Private blockchains have even fewer participants, ensuring that it takes the network less time to reach consensus. As a result, there could be more transactions. Thousands of transactions per second can be handled by private blockchains. If you equate this with seven transactions per second made by Bitcoin, this is a big difference. Private blockchains are also far more scalable. The network is able to handle more transactions because only a few nodes are allowed and responsible for handling the data. The decision-making process is much quicker due to its centralized existence.

However, one of the greatest drawbacks is the centralization of private blockchain. Blockchain was designed to prevent centralization, and because of its proprietary network, private blockchain ultimately is centralized. As for private blockchain, trust is also a bigger problem. A private blockchain network's credibility depends on the legitimacy of the nodes that are approved. They need to be trustworthy as the transactions are checked and validated. Record validity can not be independently confirmed either. Security is another Private blockchain issue. For fewer nodes, having the leverage of the network is easier for malicious actors. Unfortunately, there is much more chance of a private blockchain being hacked or getting data manipulated.

Public blockchains have many benefits but do this type actually fit for the healthcare industry? The answer maybe not so much. As I mentioned before, one of the disadvantages of public implementations is speed. Firstly, as has been highly well reported, there is a storage problem for the blocks in bitcoin and ethereum. Bitcoin has a little more than 1 mb of space per block which is simply not enough to run the kind of transactions and store the kind of data needed by healthcare institutions. Then we have the issues with the performance, which have been very well reported as well. Bitcoin only can handle 7-8 transactions per second. The confirmation period for the block is 10 minutes which only adds to the latency. With nearly zero latency, major healthcare institutes have to deal with large blocks of transactions every day. In fact, any kind of latency can potentially endanger life. More than that, public blockchains, especially those following the proof-of-work protocol such as Bitcoin, require a huge amount of computational power to solve hard puzzles. As such, investing too much money on consensus processes is completely unsustainable for such institutes. Lastly, public blockchains are open chains which are another downside in itself. In the care providers' perspective, why would healthcare institutes seek to connect with each other in a network where everyone can join in and become a part of it. Medical institutes deal with highly confidential and sensitive data, why would they want to associate with someone outside their circles? In addition, this circumstance may lead to the patient being seduced amongst healthcare providers.

The primary drawback of the private blockchain is its lack of validators and rewards. Transactions rely on validators, the greater the number of validators on the system, the more secure and the less likely it will be hacked. Private blockchains lack this incentive because they are designed for only one organization with little or no interoperability strictly for internal use. Fewer validators are possible, and only one central organization is responsible for overseeing the validation process, meaning that it is not capable of becoming a self-sustaining, evolving mechanism and is far less flexible. The system could die without validator incentives which is not optimal when it comes to creating a system for long-term use.

Applying blockchain in the healthcare sector is still in its infancy. To fully exploit blockchain's added value, a number of issues still need to be addressed, including in the areas of privacy, governance and digital identity. Personally, I think in current situation of healthcare systems, consortium blockchain is the most suitable one among three types. In consortium platform, the blocks can only be read by authorized viewers, and only designated nodes can execute smart contracts and verify new blocks; Limiting audiences to only participating parties such as care providers, device manufacturers and patients themselves would help minimize unnecessary information disclosure by allowing authentication to access the application. In blockchain management consortium style, the nodes in the blockchain are operated by a set of pre-approved members, and a valid block must contain signatures from a minimum number of members (i.e. 10 of 15). This structure would require numerous healthcare companies to participate in the scheme, while retaining a decentralized management measure. In addition, it will ensure that no rogue nodes can collude by using only pre-authorized verification (mining) nodes to inject false transactions into the chain, as well as removing the need to pay currency for proof-of-work. On the opposite, protocols such as Practical Byzantine Fault Tolerance (PBFT) can be used to achieve consensus, as the participating nodes are identified and tested. Stakeholders within the system (hospitals, pharmacies, etc.) are likewise incentivized to onboard new members to the consortium because with each additional participant, they can form a more comprehensive dataset. Rules can be predefined mutually so that the consortium can securely add new provider members into the system.

In conclusion, for this question: Which (public/private) Blockchain (initiative) in this field is the most promising? I choose the consortium blockchain because consortiums blockchain is a big compromise for businesses, as it enables connectivity between various departments and organizations while also allowing decision-makers the power to limit data access and validation. The proposed consortium blockchain makes it necessary to reach a majority of signatures from consortium members to make a block legitimate, prohibiting one party from manipulating the ledger. Moreover, no sensitive patient data is stored directly on the blockchain, thus not everyone can view patient data. This promotes transparency for patients and allows them to better manage their own healthcare data.

8. Sub question 4: What are the consequences (disadvantages) for the stakeholders if you apply the most promising Blockchain(initiative) in the Healthcare?

- Data storage:

A blockchain's principal weakness is the size of the ledger. If the entire ledger needs to be stored on each node, then the ledger must obviously be limited in size, otherwise, the node hosting device will not have the memory to store the ledger. To tackle this problem, the app maker can use additional storage systems like Ethereum Swarm, which is a decentralized cloud storage. Actual medical records can be stored on it, every medical record has a specific swarm hash, which together with the decryption key forms the root chunk. Only those who know the root chunk connection are allowed to access the content. Thus the root chunks are stored safely via the blockchain in smart contracts and are only released under strict conditions. The blockchain ledger now records the transactions often acts as a separate form of protection for both the patient and the health care provider, as its accurate record may be useful for settling disputes and tracking procedures.

- Data ownership:

In a consortium blockchain, authentication must be present for the parties that could possibly be using the data. To be more clear, patients have the right to view but not edit their own data, while healthcare professionals have the right to edit the thresholds of their patients for smart contracts. However, every participant is known on the platform. To solve the problem of data ownership and control, the controller can employ multi-signature contracts (multisig). In this case, Multisig allows two parties, the patient and the hospital, to each use their private keys to sign an authentication transaction. This way, the patient can not change the record without the hospital's permission, but they have control over who can access their data.

- Real-time data:

An essential element of every healthcare system is the need to collect and act upon real-time data. Although consortium type can be faster compared to public blockchain, there is still not 100% real-time data. Block test times may be manipulated but some slight delay will still be introduced. As mentioned, the smart device gathers and aggregates sensor data at small intervals, but sends aggregated data at larger intervals of time. Instant information is important because it affects the patient's health and treatment, but there is currently not much research to reduce the processing time of blockchain.

- Requiring approval from participant:

In a consortium-style blockchain, in order to avoid the existence of rogue miners, some human-based verification must take place before a new node is introduced to the network using a consensus method. In addition, a sufficient number of nodes must be available online at any time to satisfy the criteria for supplying the minimum number of validation signatures and preserving the validity of the consensus algorithm. Applying blockchain in medical sector is a new field so limitations occur are acceptable, and some of these limitations may be overcome with future development.

- Privacy challenge:

While the storage of patient health data in the Blockchain can have significant potential benefits for interoperability and immediate availability, there are also significant risks due to data transparency, as will Blockchain manager or miner maintains a full copy of Blockchain data. In specific, even though encryption is implemented, it is also likely that the latest encryption mechanisms will be compromised in the future or that weaknesses in the encryption systems used that possibly result in future decryption and compromising of private information.

Summary, in this question: What are the consequences (disadvantages) for the stakeholders if you apply the most promising Blockchain(initiative) in the Healthcare, although I think consortium blockchain is the most suitable type for the medical field at the moment, there are many imperfections occurs. The problems regarding data storage, data ownership, real-time transaction, participant’s approval and privacy. As I said before, applying blockchain in healthcare industry is infancy so limitations are acceptable, and some of these limitations can be tackle with and further research and future development.

9. Conclusion

Main question: Is blockchain relevant for healthcare and benefits when applying blockchain in the edical sector?

With all the things I mentioned in my four sub-questions, I think blockchain is relevant with healthcare sector because blockchain significantly increases security and accessibility, and this technology can be applied in many different fields of the medical system, such as the storing and sharing of medical records and insurance information in healthcare facilities, mobile applications and remote monitoring systems, as well as clinical trials. Currently, there is not much research about the role of Blockchain in the healthcare fields, but more work becomes available daily. In reality, many big companies are trying to apply this advanced technology in healthcare system. Blockchain is currently one of the most active areas of software research, and it can change the healthcare hierarchy by returning authority to the patient over medical records and health data. This transition of authority will lead to a move towards patient-centered treatment overall; the blockchain movement for patients is just beginning and I think it will develop in the near future.

10. Disclaimer

Before doing this thesis, I did not have any knowledge about the healthcare system and blockchain technology. By working on this thesis, I have a chance to review many articles and research about the current medical system and the EHRs. It helps me broaden my horizon of the medical system of many countries. More than that, I also have a general knowledge about blockchain technology, how it works, and benefits from it. In addition, I can learn how to make a research paper and have the possibility to interact and learn from my supervisor and my company coach. In the future, I hope to have a chance to make a more in-deep research about blockchain and apply this in the healthcare sector.

REFERENCE LIST:

Hannah S Chen, Juliet T Jarrell, Kristy A Carpenter, David S Cohen, and Xudong Huang, Blockchain in Healthcare: A Patient-Centered Model, 2019.

Erik Lau, Decoding the hype: Blockchain in Healthcare: A Software Architecture for the provision of a patient summary to overcome interoperability issues, 2019.

Nancy Collins, Nutrition 411: Common Problems in Medical Record Documentation, 2009.

Journal H (2018) Largest Healthcare Data Breaches of 2018. HIPAA Journal.

Nakamoto S, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

Yue X, Wang H, Jin D, Mingqiang Li, Jiang Wei, Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst 40: 218, 2016.

Griggs KN, Ossipova O, Kohlios CP, Alessandro N Baccarini, Howson Emily A, et al. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med Syst 42: 130, 2018.

DOMINIQUE HURLEY, The Advantages and Disadvantages of Blockchain in Healthcare, June 21, 2018.

Odekunle Florence F, Current Roles and Applications of Electronic Health Record in the Healthcare System.

Nir Menachemi and Taleah H Collum, Benefits and drawbacks of electronic health record systems, 2011 May 11.

Blockgeeks, ,2019, Blockchain in healthcare: The Ultimate use case?

Maria Redka, Blockchain and Healthcare: Use Cases Today and Opportunities for the Future, November 15, 2018.

IBM Blockchain Pulse, Protect Pharmaceutical Product Integrity with the Pharmaceutical Utility Network, December 16, 2019.

Quora, What are the use cases for blockchain tech in healthcare?, December 17, 2018.

Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, Thaier Hayajneh, Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring, 21 March 2018.

Peng Zhang, Douglas C. Schmidt, Jules White, Gunther Lenz, Blockchain Technology Use Cases in Healthcare, 2018.