# Universiteit Leiden
# ICT in Business

## A Multicriteria Evaluation of Blockchain Technologies in the Healthcare System


Name: Nicolò De Sandre

Date: November 2, 2018

1st supervisor: Simcha Jong Kon Chin
2nd supervisor: Michael Emmerich


MASTER'S THESIS


Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

# *Declaration of Authorship*

I, Nicolò De Sandre, declare that this thesis titled "A multicriteria evaluation of Blockchain Technologies in the Healthcare System", and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed my- self.

- Signed:
- Date:

*"The world is changing very fast. Big will not beat small anymore. It will be the fast beating the slow"*

Rupert Murdoch, CEO of 21st Century Fox

# *Acknowledgements*

I would like to thank, first of all, my Supervisors Prof.dr. S. Jong Kon Chin and, Dr M.T.M. Emmerich, for supporting and believing in my research. Thanks for always finding time out of your busy schedules to answer my questions whenever I run into troubles and to provide wise advice. Your guidance helped me during all the research. It would not have been possible without you.

A very special gratitude also goes to the experts that have been interviewed for this research project: Edward Magrin, Sin Kuang Lo, Giorgio Fedon, Mirko De Maldè, Massimiliano Faudarole, Gabriele Sabbatini, and Guy Newing. Thanks for your precious time, your insight and your expertise. You played a central role in this research.

A special mention to Chiara. Thanks for providing me with continuous encouragement and support in this important period of my life.

Finally, thanks to my life-coaches, mum and dad. Thanks for having supported me along the way. This accomplishment would not have been possible without you. Thank you.

# Abstract

"People have been innovating throughout human history. Innovations allow us to do things better. However, sometimes, these innovations turn into something more. Sometimes they allow us to do better things. That is when they become disruptions."[1]

Blockchain is the disruptive innovation that will change the way we exchange value. While this innovation is being considered for multiple businesses, its potential to revolutionise the healthcare system is also gaining attention. How useful would it be to access, every time we want, and we need, our full history of health records?

Moreover, what if patients could own their medical data? Healthcare system will become patient-centred. On the one hand, the overall quality of healthcare would undoubtedly rise and, on the other hand, costs, risks, and deaths will be likely to decrease. Patients will be able to see a complete picture of their medical history maturing a broader responsibility on their daily routine. They could be the CEO of their health. Doctors will be able to access real-time life-saving data, update records for their patients and so on, avoiding in this way data silos, extra costs and information blocking. However, 'we do not own our data; we just visit them from time to time' and, interoperability between health providers is still a hurdle to overcome. What is the solution then?

This research focuses on how blockchain can optimally adapt and improve the healthcare system. It proposes an analysis of the multiple blockchain solutions, proposed until the time of this research, and their technical features. Different blockchain types, as well as different consensus algorithms, result in different benefits, advantages and limitations regarding their application to the healthcare system. This research aims to find out, through a multicriteria evaluation, how these benefits change with different blockchain technologies.

Keywords: Health Data, Data Ownership, Blockchain, Healthcare.

# Contents

# List Of Figures

# List Of Tables

Chapter 1

# *Introduction*

## Motivation

Being a doctor has always been one of the oldest vocations in the world with crucial importance throughout human history. Medicine, as well as doctors, needs to evolve. It always needed to change, throughout human history, as society, technology and people progressed. Nowadays, industry expanded enormously, cities at the same pace as the population continue to proliferate. Modern medicine is keeping the pace with this exponential growth. It has to. Enormous developments have been made in the medical field to identify and prevent illness.

It is, nowadays, an exciting time for the present and future of medicine. In this new age of smart devices, the digital revolution, self-driving cars, artificial intelligence and so on, technology, initially used as a support to healthcare service has now crucial importance. Blockchain and interconnected IT systems are leading the way.

The choice of this topic was brought up by a deep interest in innovative technologies together with their application to the healthcare system and their consequent adoption and use.

## Problem Definition

Health records are particularly significant in the healthcare field. However, patients have little or no control over their medical records and data; they can not control how they are stored, where, with whom they are shared, and for which purpose. "To obtain paper copies, individuals often have to face the inconvenience of going to a medical department on person, signing forms, paying a fee and, waiting 30 to 60 days to obtain their health information"[2].

Besides data ownership issues, information blocking between different healthcare providers negatively affects their efficiency and effectiveness. Incorrect and incomplete information could lead to tragic medical errors and, in the long term, to a decrease in healthcare system's effectiveness and efficiency. This is mainly due to incorrect and incomplete Electronic Health Records (EHR).

Often individuals act independently and according to their, or their company, self-interest, hoarding in such a way the best interest of the whole group.

Moreover, the healthcare system is not as safe as we think it is. According to many studies, a substantial number of medical errors, besides a considerable increase in healthcare costs, was referred to as a leading cause of death and complications.

## Aims and Objectives

The main aim of this research is to evaluate the applicability of different blockchain technologies in the healthcare system. A multicriteria evaluation is performed, with the help of blockchain and healthcare experts, to determine which type of blockchain network and consensus algorithm suits more the healthcare system properties.

### Research Questions

The following research question attempt to direct the research towards a clarification of the aims and objectives mentioned above.

*(1) Which type of blockchain and consensus algorithm meets and fulfils the essential criteria for a blockchain solution to be applied to the healthcare system?*

## Sub-Questions

(1) *Which are the essential properties for a healthcare blockchain solution that should be considered in a multicriteria evaluation of blockchain technologies like different networks type and consensus algorithms?*

(2) *Should a blockchain solution for the healthcare system be implemented on a public or private, and permissioned or permissionless network? Which are the different benefits and limitations of these types of networks when applied to the healthcare system?*

(3) *Which consensus mechanism fit best in such a blockchain solution in the healthcare system, Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (D-PoS), or Proof of Authority (PoA)? Which are the different benefits and limitations of PoW, PoS, D-Pos and PoA when applied to the healthcare system?*

## Objectives

The successive list of objectives has been identified to address the above research question and the related subquestions.

- Find the main current problems for the healthcare system related to the inadequate use of IT systems in the medical field; and figure out which problem can be solved, or softened, by the adoption of a blockchain based solution in the healthcare system.
- Find the critical properties and benefits that distinguish private/public, permissioned/permissionless blockchain and consensus algorithms; Figure out which properties have the most positive impact on the healthcare system.
- Collect experts' insights, observations and knowledge to perform a multicriteria evaluation of the different blockchain technologies applied to the healthcare system.

## Subject Relevance

The following section ponders on the relevance of blockchain itself, on the relevance of this technology applied to the healthcare system and, finally, on the relevance of this research compared with the body of existing knowledge regarding the application of blockchain to the healthcare system.

### The importance of emerging technologies

What does 'emerging technology' mean? They can be defined as "new technologies that are currently developing or will be developed over the next five to ten years, and which will substantially alter the business and social environment"[3]. It is an innovative technology that is currently undergoing extensive experimentation.  Some of them come to light from theoretical research, others due to commercial research. Where does blockchain come from?

Cryptocurrencies like Bitcoin and Ethereum have grabbed mainstream attention due to the skyrocketing values they reached during the past two years. The secret behind these digital currencies is the technology of the blockchain. Blockchain phenomena started in 2008 when, a white paper "Bitcoin, a peer to peer electronic cash system (Nakamoto) " was published to introduce, indeed, Bitcoin.

Interest in blockchain technology is, nowadays, exponentially growing since this new technology has the potential to impact multiple industries in two major ways. First by providing a digital platform of distributed trust that reduces intermediaries and frauds. Second, it is enhancing industries' efficiency by improving existing structures data flow and transparency. For these reasons, governments, private companies, universities, and research institutes are investing time, money and resources to explore its future potential uses.

According to the Gartner Hype Cycle for emerging technologies, blockchain still has five to ten years for mainstream adoption. The accuracy of this cycle is also due to the consideration of an additional dimension: human attitudes. “Hype Cycles also reflect human attitudes toward technology. Most technologies conform to the Hype Cycle because the invariant in the equation is people, not the technology”[4].

Blockchain technology has just passed the peak of inflated expectations in its cycle as shown in Fig 1.1. Gartner hype cycle points out the level of maturity of blockchain in 2017, and it is sliding into the “Trough of Disillusionment”. In this phase, tests are ongoing, and industries are improving blockchain services based on feedbacks regarding significant problems in its implementation.

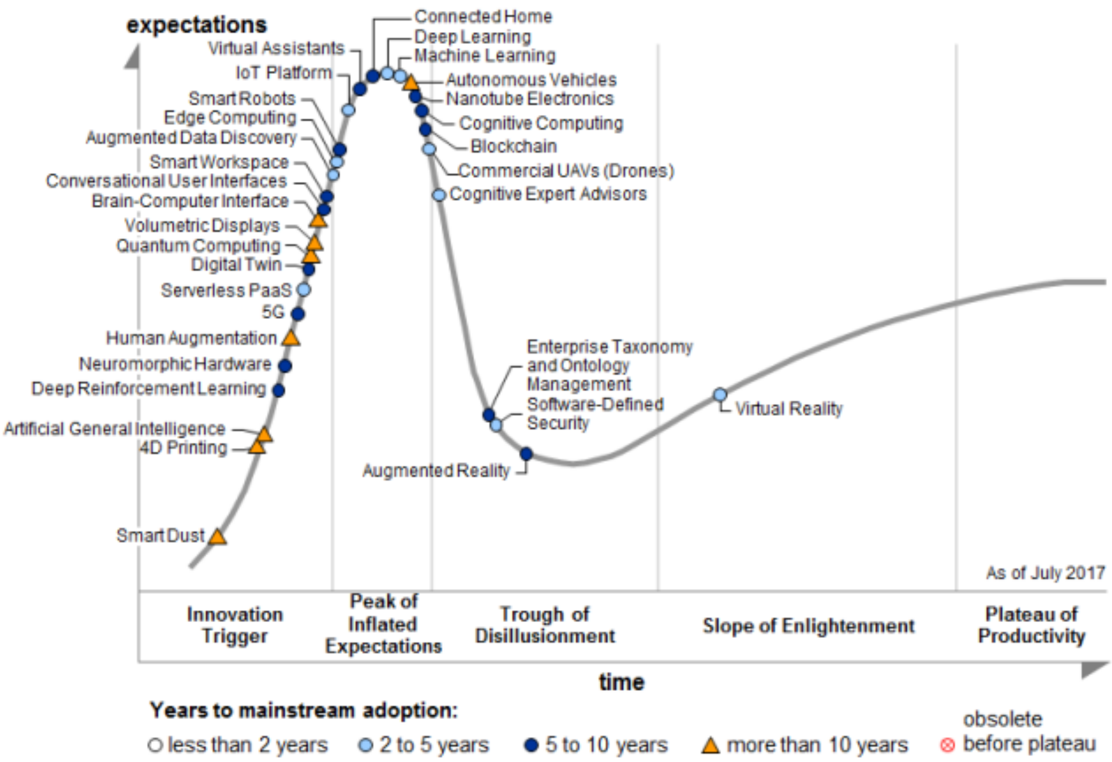



Figure 1.1 Image source: Gartner hype cycle for Emerging Technologies 2017

## Relevance in Healthcare System

This disruptive technology is founding his way to many different industries, one of them, the healthcare industry. It is a fascinating time for healthcare and information technologies; innovation in IT systems is leading to the production of vast amounts of health data scattered across multiple diverse databases. Due to the increasing adoption of Electronic Health Records, health data are now stored online. However, health data ownership, data sharing, interoperability and transparency between health stakeholders are still a problem that has not yet been tackled.

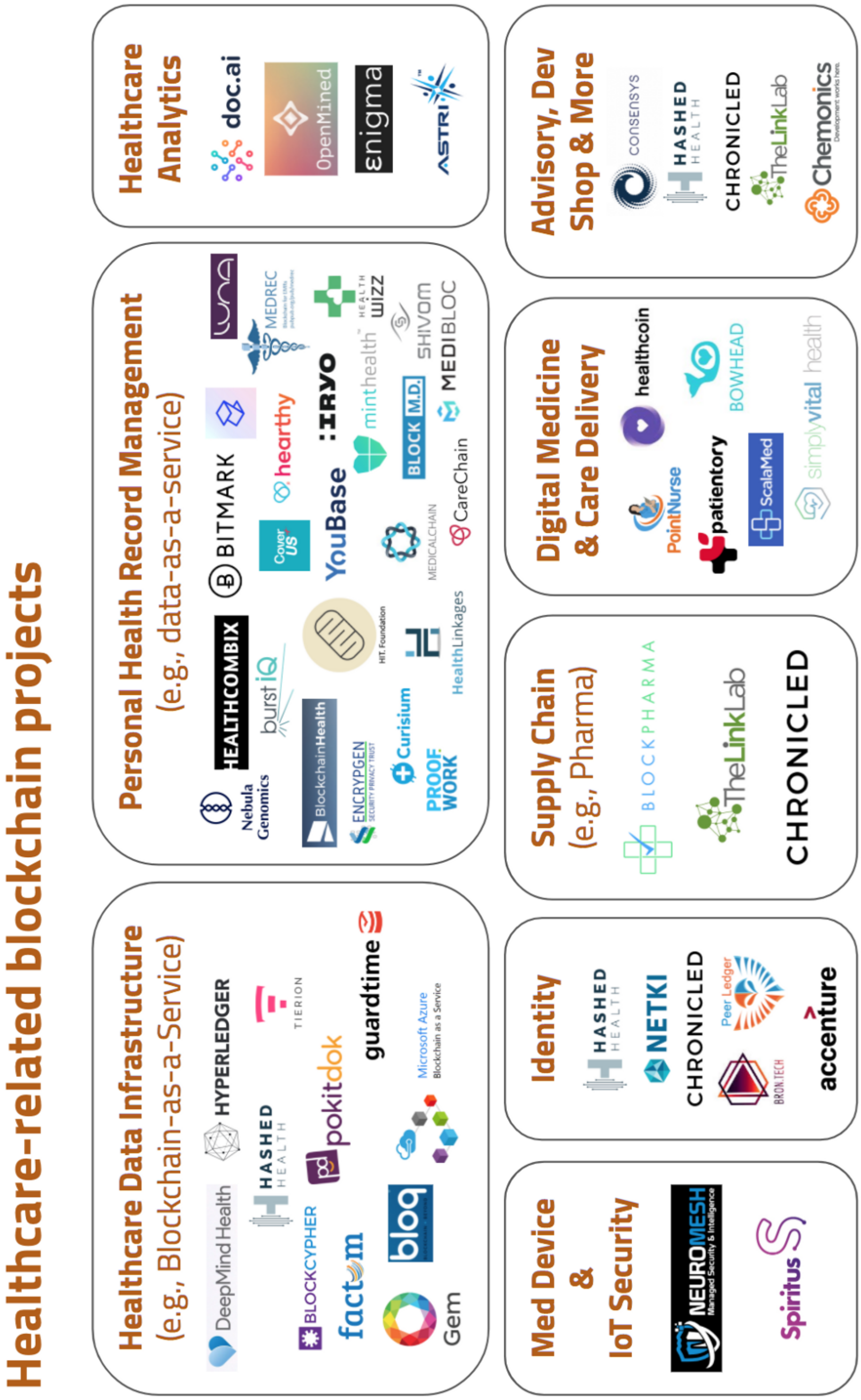



Figure 1.2. Image source: Andy Coravos. Healthcare-related blockchains projects.

The many risks, challenges, limitations and, in a nutshell, problems that the healthcare industry faces every day is motivating healthcare organisations and governments to boost the system efficiency and effectiveness across its multiple functions. The healthcare system is not suffering from a lack of vertical innovation, meaning specific innovative machinery and technologies to cure health disorders; It is suffering from a lack in horizontal innovation, *"the effective transfer of knowledge and technology from one sector to another"*[5]. Interoperable IT systems are an example of horizontal innovation; These IT systems can connect the many islands of information in the healthcare system improving in this way quality and lowering costs. "As health care businesses continue to make strategic acquisitions and vertical integrations, there is a greater need for smooth transitions of IT operations across those integrations while maintaining reliable and transparent services to those on the front lines of care delivery"[6].

Blockchain is an example of horizontal innovation with the capacity to boost vertical innovation in different sectors. It is an enabling technology with the potential to remodel industries' paradigms and enable new business models. For these reasons, governments and private companies are trying to understand how this innovation can enhance the entire healthcare system. Research about the applicability of blockchain has been conducted by US government, Europe, Estonia and many private companies like IBM, Deloitte, and McKinsey. Multiple projects have been started to explore this technology applicability to the healthcare system; on the one hand, to solve problems like IT systems interoperability, health data management and ownership, healthcare analytics; on the other hand, to enhance and improve population health management, pharma supply chain, IoT integration and virtual medical consultants. Figure 1.2 summarises healthcare related blockchain projects.

Nevertheless, some professionals from the industry are still very critical about the potential impact and success of emerging technologies in healthcare. The criticism and concerns are supported by other researchers like Maarten van Limburg which states: "current frameworks for eHealth development suffer from a lack of fitting infrastructures, inability to find funding, complications with scalability, and uncertainties regarding effectiveness and sustainability”[7];

Alternatively, Ton Spil: “Although end users are satisfied and initial objectives are reached in terms of product quality and testing results, most of the innovations never reach the real world”[8]. Is not yet clear which type of impact blockchain will have on the healthcare system, but so far it is evident that it is having one. Besides, it is a new phenomenon that demands further research and understanding of complicated technological notions. This research also takes into account the maturity level in the Gartner Hype Cycle which positions blockchain at the peak of inflated expectations. This makes the technology a challenging object to research due to limited information availability.

## Thesis Structure

The thesis is divided into three main sections, each of them is subdivided into two chapters:

1. Section one consist of “Blockchain” and “Background Theory”; The first examines blockchain technology advancement, applications and properties. The second discusses the main theoretical findings that have been found with the examination of the literature.
2. Section two consists of “Research Methodology” and “Research Design & Implementation”; The first describes the theoretical approach used to attain the aim of the study. The second put the theory into practice by providing a framework to find answers to the aforementioned research questions.
3. Section three consists of “Research Results” and “Discussion & Conclusion”; The first displays the results obtained from experts interviews and surveys. The second elaborates on the results, and analyse them to concisely provide answers to the research questions and indicate possible future works.

# Conclusion

This chapter pointed out the importance of technology innovation, and the disruptive impact that an innovation like blockchain may have on multiple sectors. With the “problem definition” section, is clearly explained which problems is the healthcare system facing; Its significant problems have been listed and is provided with a blueprint of how blockchain could solve or soften them. All these elements highlight the relevance of further studies in blockchain technology applied to the healthcare system even though the topic is being studied by multiple governments and private companies as shown in Fig 1.2. Finally, in the thesis structure section, was given an overview of how the research is structured.

Chapter 2

# *Blockchain*

## Introduction

This chapter provides a detailed description of blockchain technology and a basic understanding of how this technology works, its benefits, applications, but also costs, challenges and limitations. The purpose is to prepare the readers by providing them with all the necessary elements to understand it.

## Background

What is blockchain? Blockchain is a global online database that anyone, anywhere, with an internet connection, can use. It differs from traditional databases since a central figure does not own it, it belongs to anyone.

*"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value"*[9].

*"A blockchain is a distributed, shared, encrypted, chronological, irreversible and incorruptible database and computing system (public/private) with a consensus mechanism (permissioned/permissionless), that adds value by enabling direct interactions between users.*[10]*"*

*"The blockchain is considered to be a General Purpose Technology by a number of researchers. The rise of a GPT can affect the entire economy and examples include the rise of the automobile, the computer and the Internet"*[11].

In his article "A gentle introduction to blockchain technology", Lewis provides an adequate analogy by comparing blockchain to a book. We can think of blockchain as a data structure that regards how data is logically put together and stored. This data are stored in blocks, which belong to a chain. We can say blockchain is a chain of blocks as, in the same way, a book is a chain of pages. Each page in a book contains the text, and, at the top, information about itself like the page and chapter number and name, and the title of the book.

In the same way, each block contains multiple transactions and a header. The header shows the block number and contains technical information about previous blocks and a fingerprint or hash of the data within itself. Like a book is ordered by page number, in blockchain, each block reference to the previous one by the “block’s fingerprint” as you can see in Fig 2.1.

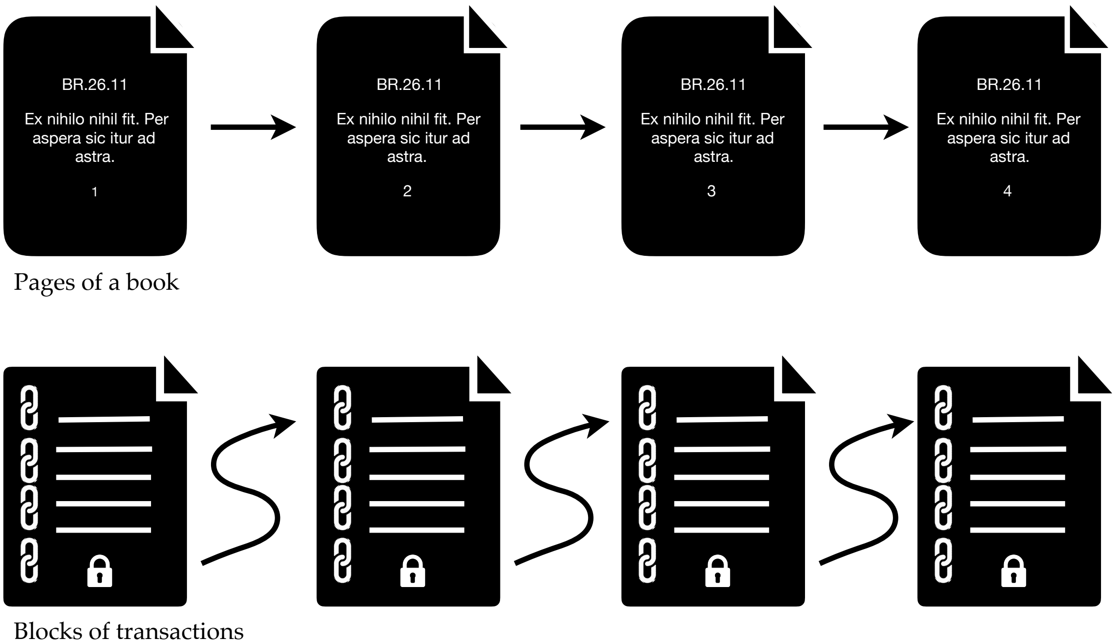



Figure 2.1 Analogy between the Blockchain and the Pages of a Book.

Image Source: Author

# Technology

It all started in 2008 when a white paper "Bitcoin a peer-to-peer electronic cash system" was published under the pseudonym Satoshi Nakamoto. The white paper introduced a fully distributed digital currency system in which data are contained in blocks chained together. Nakamoto introduces it as "A purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution", but it can also be defined as a transactional distributed database shared between all the nodes participating in the peer to peer network open to anyone with an internet connection. Every node has a copy of the ledger containing specific transactions which are accessible only to users that hold the permission to access them. Each node can send a transaction to every node participating in the network without the need for a central authority in the transaction.

The lack of a central authority is one of the distinguishing characteristics of blockchain that makes it a distributed network in which no central authority or person owns the system, yet everyone can use it and help run it.

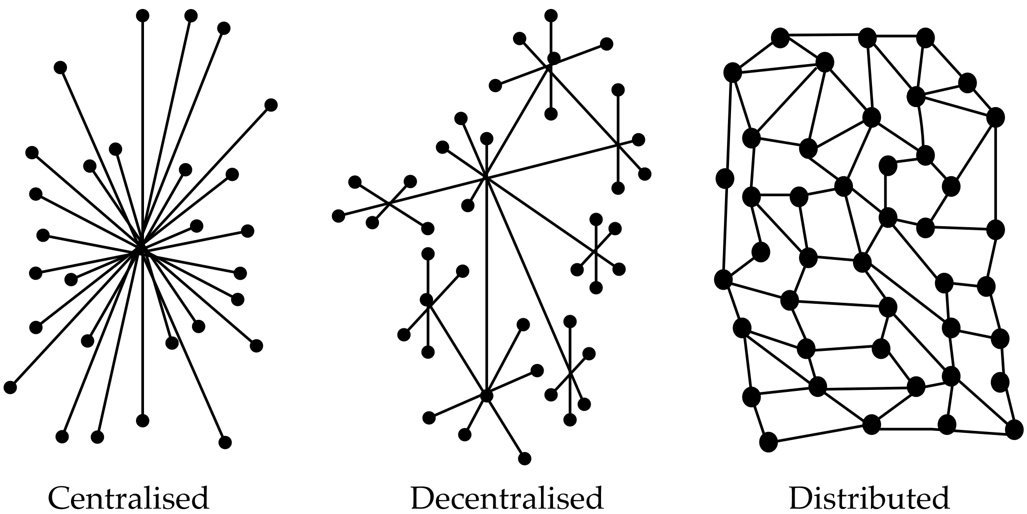



Figure 2.2 Network Types. Image Source: Author

The following bullet points recap blockchains' essential features:

- **Decentralised**: Blockchain core idea is to place trust, not in a single entity rather in the peer to peer network. Indeed, in a decentralised system, decisions are taken in multiple points and, the system behaviour results from the aggregate responses of the nodes participating in the decisions. "Blockchains are politically decentralized, no one controls them. Architecturally decentralized, no infrastructural central point of failure. However, they are logically centralized since there is one commonly agreed state, and the system behaves like a single computer"[12].
- **Distributed:** In a distributed system, once decisions are taken by multiple nodes, information are distributed among all the nodes of the network and, any change will be reflected to all of them. This process cuts out single points of failure. Nodes work in coordination to process a common result (or consensus) in such a way that they look like a single entity. "Distribution reduces risk in data-tampering and frauds due to the number of nodes participating in the network"[13]. In such a way, blockchain provides data authenticity, consistency, timely, accuracy, and availability.
- **Trustless**: Blockchain allows online payments to happen between two parties without the need to trust a central authority to record transactions. Central authorities, like banks, will be replaced by a peer to peer network in which transactions have to be publicly announced and added on the blockchain. "The only way to confirm the absence of a transaction is to be aware of all transactions".[14]
- **Immutable**: Transactions that have been added to the blockchain and so, that are shared across the nodes participating in the network, are almost impossible to be modified or reversed. Unauthorised changes or malicious tampering risks are reduced to the minimum through the use of cryptographic hash like SHA-256 used in Bitcoin Blockchain.

## Blockchain Evolution

This innovative technology has been evolving throughout the last ten years. The first implementation of a distributed ledger technology DLT, blockchain 1.0, led to the creation of Bitcoin and other cryptocurrencies. However, Blockchain represents only the backbone of Bitcoin. After more or less five years the advent of Bitcoin, blockchain began to advance independently from the idea of cryptocurrency. The second generation of blockchain, Ethereum, conceived by Vitalik Buterin was born, and a new concept had been introduced: the smart contract. A smart contract is a small computer program implemented on the blockchain; it allows the nodes of the network to conduct transactions, deals and execute multiple conditions without the need for intermediaries. The third generation, blockchain 3.0, differs from the previous two due to its higher scalability, interoperability, and adaptability. Different protocols and consensus algorithms solved the problems, such as transaction speed and energy consumption, that limited the diffusion of the technology. Moreover, it introduces decentralised applications (DApps). Dapps run on a peer to peer network, a decentralised environment free from the control of a single entity.

Finally, blockchain 4.0 aims to make blockchain technology usable for business purposes and bring it closer to mass adoption by exploiting the strong foundations set by the previous versions.

## The Anatomy of a Block

The block is the heart of blockchain where all the transactions are kept. New transactions are validated continuously and added to a new block by miners; This is what orders the blocks in a linear sequence over time and forms a block-chain. A block structure generally consists of two main parts:

- **Header**:

  A block header is an 80-byte long string composed by "4-byte long Bitcoin version number, 32-byte previous block hash, 32-byte long Merkle root, a 4-byte long timestamp of the block, 4-byte long difficulty target for the block (target hash), and 4-byte long nonce used by miners"[15]. Each block is univocally identified by this cryptographic hash, similar to a digital signature, created by hashing the block header (the 80-byte long string) twice with the SHA256 algorithm. This is a unique identifier which means that two blocks will never have the same hash. A second way to distinguish blocks is by referring to their height as shown in Fig 2.3; The 'height' indicates the position of the block in the blockchain.

## Block #500312

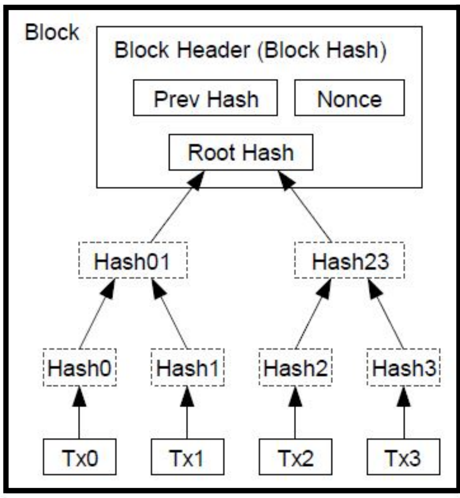
| Summary | |
|---|---|
| Number Of Transactions | 2580 |
| Output Total | $ 82,731,736.67 |
| Estimated Transaction Volume | $ 17,767,650.77 |
| Transaction Fees | $ 54,814.86 |
| Height | 500312 (Main Chain) |
| Timestamp | 2017-12-20 20:02:40 |
| Received Time | 2017-12-20 20:02:40 |
| Relayed By | BTC.TOP |
| Difficulty | 1,873,105,475,221.61 |
| Bits | 402691653 |
| Size | 1093.292 kB |
| Weight | 3992.963 kWU |
| Version | 0x20000000 |
| Nonce | 900685155 |
| Block Reward | $ 95,246.12 |

| Hashes | |
|---|---|
| Hash | 000000000000000000301fcfeb141088a93b77dc0d52571a1185b425256ae2fb |
| Previous Block | 0000000000000000004b1ef0105dc1275b3adfd067aed63a43324929bed64fd7 |
| Next Block(s) | 000000000000000000282ac9977c3d103a3c6bd873b1f7744e8d42b83239baa6 |
| Merkle Root | a89769d0487a29c73057e14d89afafa0c01e02782cba6c89b7018e5129d475cc |

Figure 2.3 Block Information Example. Image Source: Bitcoin Block #500312

As mentioned before, in each block, a header 80-byte long string contains the previous block hash, the hash of the Merkle Root, the nonce, and the target hash. The previous block hash is used to create the current block's hash, so, for every block 'X' we will need the hash of the block 'X-1'.

The Merkle Root is the final value obtained by hashing a Merkle tree. A Merkle tree is a binary tree in which transactions are coupled and hashed together recursively; Merkle trees usually have a branching factor of 2, meaning that each node has up to 2 children. By concatenating together two values at the same height of the tree, hashes are created to encode files, this process is iterated until the final 'Root Hash' of the tree is reached, and the Merkle root hash is obtained, Figure 2.4.




Where, supposing the block contains X transactions:

Tx0 = Transaction 0
Hash0 = Hash of Tx0
Tx1 = Trasaction 1
Hash1 = Hash of Tx1
Hash01 = Hash(Hash0∧Hash1)

**Root Hash=Hash{Hash0→[X/2]∧Hash[(X/2)+1→X]}**

Figure 2.4 Block Header. Image Source: Author

The Nonce is a number that is used only once. For Bitcoin, the nonce is an integer between 0 and 4.294.967.296.

Finally, the 'Target Hash' is a 64-digit hexadecimal number which we will define as 'T'. A hash is an algorithm that converts any sequence of characters and digits into a hexadecimal number of 64 digits. Hexadecimal numbers are more suitable for representing information stored in bytes since 1byte of information corresponds to a two-digit hexadecimal number. In a hexadecimal system, numbers are composed by the ten digits from 0 to 9 (decimal), plus six letters a, b, c, d, e, and f the values of each digit can be seen in Fig 2.5:

| **Decimal system** | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| **Hexadecimal system** | | | | | | | | | | | | | | | |

Figure 2.5 Hexadecimal system. Image Source: Author

- **List of transactions**

  Besides the header, a block contains a list of transactions which have been validated with Proof of Work by a node and added to the blockchain. However, some transactions have been transmitted to the network and are waiting to be verified and reckoned on the blockchain; These transactions form the mempool. The mempool is a pool of unconfirmed transactions that characterises each node in the network. "As blocks are mined and received by nodes, the nodes will remove any unconfirmed transactions in their mempool that are included in the block. So a mempool gets reduced in size every time a block is received"[16]. Transactions in the mempool are selected by mining nodes sorting them also based on transactions fees; In fact, miners have two types of compensations, the block reward, and the transaction fees. The first reward is given every time a block is mined and, it is halved every 210000 blocks are created. It was 50BTC in 2009 and now is 12.5BTC. As of today, this reward provides the greater incentive for miners. The second bounty, "Bitcoin mining fee", is a fee that users have to pay when sending Bitcoins to incentivise miners to mine certain transactions before others. As the "Block Reward" decreases over time, transaction fees will keep miners incentivised.

## Blockchain Types

It is extremely easy to get confused about different blockchains, and their application due to the similarity and complexity of these networks. This chapter aims to clarify the confusion surrounding the different types of blockchain networks by defining and delineating the major types of blockchain and their differences. "In general, four major blockchain types can be distinguished: public permissionless blockchains, public permissioned blockchains, private permissioned blockchains and private permissionless blockchains"[17].

The research takes into account four types of blockchain: Public, Private, Consortium, and Semi-Private. These types are introduced and explained in the following chapter also by addressing their limitation and weaknesses. More in-depth explanations will follow in Chapter 3.

**Public - Permissionless**

In a public blockchain, like Bitcoin, anyone in the world with an internet connection can join and participate in the network, reading, and sending a transaction to all the nodes of the network. No single entity has the power to validate transactions, but all of them, the system is truly democratic. These transactions are transparent and anonymous; for this reason, public blockchains are considered fully decentralised meaning that, any node can participate into the consensus process to determine which blocks containing transactions get added to the chain, red nodes in Table 2.1.

Public blockchains are secured by crypto economics. Cryptoeconomics is "A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralised digital economy. Cryptoeconomics is a practical science that focuses on the design and characterisation of these protocols"[18] By combining economic incentives and cryptographic verification with mechanisms such as PoW for Bitcoin and PoS for Ethereum, nodes are incentivised to join the network. Examples of public blockchains are Bitcoin, Ethereum, Dodgecoin, Monero, Litecoin, etc.

However, this network comes alone also with some drawbacks; First, the massive amount of computational power needed to maintain the distributed ledger at a large scale. Secondly, the low speed of transaction accomplishment, together with the long transaction approval frequency. Also, lastly, the inability to change or revert a general transaction since these networks are designed to be irreversible and nodes have no control over them, they will be permanently recorded.

**Public-Permissioned**

A Public-permissioned blockchain differs from a permissionless one since not all the nodes that participate in the network can take part in the consensus algorithm and validate transactions. The network is still open to everyone; every node can participate. The consensus mechanisms used in these types of blockchain are PoW of PoS in which a simple majority of selected nodes validates the transaction. Green nodes participate in the network but do not take part in the validation of transactions, Table 2.1.

**Private-Permissionless**

A private blockchain is a blockchain where nodes to join the network, which is restricted to certain participants, have to be invited, blue circle Table 2.1. They are designed for enterprise applications, built to accomplish more specific enterprises' tasks. With this type of blockchain, the company running the private blockchain, or the network operator, has the capacity to control the nodes that participate in the network, to change the rules of the last, and to revert or modify transactions. Nevertheless, every node participating in the network has the right to participate in the consensus algorithm, red nodes Table 2.1.

The main advantages over a public blockchain are that they have already overcome the hurdle of the significant amount of power necessary to run a public blockchain; Efficiency is enhanced along with privacy since these networks are restricted, permissioned, and can be joined only through an invitation.

**Private-Permissioned**

In this type of blockchain, the owners of the network, besides choosing who can join the network, are able to restrict who can mine blocks and participate in the specific consensus mechanism of the blockchain's network. This category provides lots of customisation options. These options include selecting nodes participating in the network after verification of their identity, designating different permissions, for each node, to perform only specific tasks, and managing multiple levels of access for nodes. Some nodes, for example, will be able to read, some to write, and some to access information stored on the blockchain depending on their permissions. These properties lead to cheaper and faster transactions because these only need to be validated by the limited number of nodes participating in the network.

This type of network fits perfectly for business and enterprises since these can set the necessary restrictions when configuring the networks and control the activities of the participants. Also, the mining reward, if there is any, is set by the network operators.

Again, in Table 2.1, red for nodes denotes participation in the consensus algorithm, while green nodes only take part in the private blockchain network delineated with a blue circle.

### Summary

The following images summarise what has been discussed so far by the research. Table 2.1 displays the different blockchain types, while Fig 2.6 compares them based on validators' trust and anonymity.

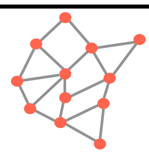
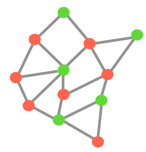
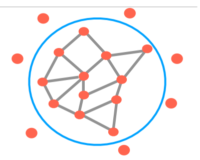
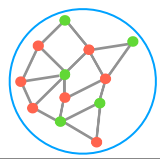
| Blockchain Type | Explanation | Visualization |
|---|---|---|
| Public Permissionless | Everyone can participate in the network, transact and see the full transaction log, and take part in the consensus algorithm to validate data. Bitcoin |  |
| Public Permissioned | Everyone can participate in the network, transact and see the full transaction log. However, only a restricted number of nodes can participate in the consensus algorithm. These nodes are selected by the network itself with PoS or D-PoS. |  |
| Private Permissionless | The blockchain owner selects participants in the network with the ability to transact and see transaction log. All these selected nodes can participate in the consensus algorithm. |  |
| Private Permissioned | The ability to transact and view the transaction log is restricted to the participants in the network. The blockchain owner selects participants in the network and in the consensus aglorithm. |  |

Table 2.1 Summary Blockchain Types. Image Source: Author

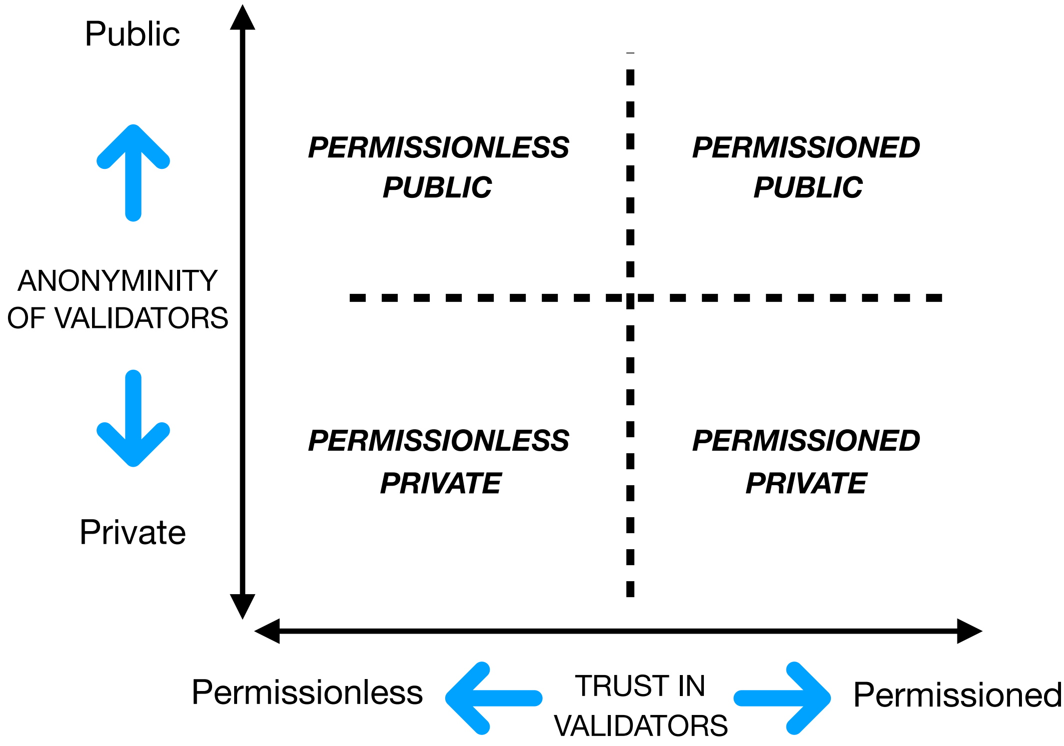



Figure 2.6 Summary Blockchain Matrix. Image Source: Author

## Consensus Algorithms

The following section describes the different consensus algorithms through which transactions are validated and added to a general blockchain. Every type of blockchain fits better with a different consensus algorithm. The research takes into account four different types of consensus algorithm:

**PoW - Proof of Work:**

In a decentralised network such as Bitcoin, running on a public permissionless blockchain, the nodes participating in the network need to find an agreement among the validity, and order of the peer to peer transactions that should be added to the blocks forming the blockchain. In order to do this, miners use Proof of Work consensus algorithm. The last, allows the network to reach consensus and, in the meantime, secures the network. How does it work more technically?

A peer-to-peer electronic cash system paper describes the proof-of-work algorithm as "scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash"[19]. As explained before in "The Anatomy of a Block" section, a block header contains the previous block hash, the hash of the Merkle Root, the nonce, and the target hash as you can see in Fig 2.4.

"The block is generated and added to the chain by taking the hash of the block contents, adding a random string of numbers, the nonce, and hashing the block again. If the hash meets the requirement of the target, then the block is added to the blockchain. The lower the target, the smaller the set of valid hashes."[20]

Miners have to find a nonce such that:

**[SHA256 (SHA256 of Block Header contents + Nonce)] < 'Target Hash'**

Here the '+' symbol stands for concatenation of strings. The mining exercise is an iterative process of brute force in which a block header is hashed repeatedly by miners by altering the nonce value. "Mining is a competitive process, but it is more of a lottery than a race"[21]. In fact, due to the low, single probability of success, it is unpredictable which node in the network will generate the new block. Figure 2.7 displays an example of this process:

*The string we are going to do work on is "Hi there!". The aim is to find a nonce, a variation of it that SHA256 hashes to a valued beginning with 0:*


*The block content is "Hi there!". The 5 tested nonce values are 1-2-3-11-12; The one that satisfies our difficulty target is the last one "12". In general, with a difficulty target 'k', the aim is to produce a nonce with 'k' leading zeros.*

Figure 2.7 Hashing Process. Image Source: Author

Through this exercise, miners attempt to find the correct nonce value and create a proof of work. When this value is found, the first miner that obtained it broadcasts the result to all the other nodes participating in the network, the block is added to the blockchain and, in this way, all the transaction that it contains are validated. Proof of work makes it extremely difficult to tamper or modify any transaction contained in the blockchain since every alteration would require to re-mine not only the interested block but all its successors and redoing all the work they contain.

**PoS - Proof of Stake:**

This consensus algorithm, PoS, is an alternative process to verify transactions on a blockchain adopted by different cryptocurrencies like Ethereum, Dash, Neo, and many others. Its adoption is gaining popularity in the cryptocurrency world due to its benefits when compared to the traditional proof of work. The additional benefits and the problems this type of consensus algorithm can solve are:

Efficiency in energy consumption: less computational power required to validate a block. "The Bitcoin network can be estimated to consume at least 2.55 gigawatts of electricity currently, and potentially 7.67 gigawatts in the future, making it comparable with countries such as Ireland (3.1 gigawatts) and Austria (8.2 gigawatts)"[22]. Ethereum community is exploiting the proof of stake algorithm for a greener and cheaper distributed form of consensus.

Lower the risk of a 51% attack by the use of economic penalties which make 51% attacks vastly more expensive to carry out than proof of work, depending on the value of a cryptocurrency. If an attacker tries to buy 51% of the total number of coins, the market reacts by fast price appreciation.

How does it work? In this type of consensus algorithm, the main protagonist is no more the miner but, is a validator. Validators, or forgers, are chosen in a deterministic way by considering their wealth, or stake in a currency, and the age of that stake within the blockchain's network. The greater and older the stake, the more likely a validator will be selected, in the election process, to mint or forge the candidate block. In the case a validator refuses to mint a block, PoS includes a large group of back up validators that would substitute the first validator. Selecting the forger considering the size of his stake alone, would result in a permanent advantage for the richer validators. Two main methods of selections have been implemented: 'Randomized Block Selection' and the 'Coin Age-Based Selection'. On the contrary, with proof of work rich people can exploit the power of economies at scale since the price that they pay for mining tools and electricity does not increase with a linear slope, instead, the more they buy, the better prices they will get. With PoS, a validator, by minting a new block, will check the validity of all the transactions contained in the last. If everything checks out, the node sign off on the block and adds it to the chain. As a reward, the validators will receive the fees associated with the transactions contained in the block, not anymore the block reward, such as the ones in Bitcoin network. Similarly, if validators approve fraudulent transactions, they will lose a part of their stake, as well as their privilege to be part of the network consensus. Fraudulent transactions can be detected by checking if it was correctly signed with the matching key and if the money has not already being spent. As long as validators' stake is greater than the transaction fees that they would receive as a reward, the will not be incentivised in validating fraudulent transactions since they will lose more money than they gain. When a node stops being a validator, his stake and all the transaction fees that he got will be released after a certain period. This is necessary to check whether some of the blocks that have been validated were fraudulent or not, and to punish the validator in the first case.

**D-PoS - Delegated Proof of Stake:**

It is an alternative consensus algorithm, invented by Daniel Larimer, based on the traditional proof of stake, with the only difference in how validators are selected. Instead of having coins at stake, nodes in the network can vote to select witnesses; these are other nodes they trust to validate transactions. These votes are weighted considering the size of the stake of each node taking part in the election process. These witnesses are not affected by their stake, even nodes with a relatively small stake can be elected if they had received enough votes, and they will earn the right to become validators and add transactions to the blockchain. “The top N witnesses by total approval are selected. The number (N) of witnesses is defined such that at least 50% of voting stakeholders believe there is sufficient decentralisation. When stakeholders express their desired number of witnesses, they must also vote for at least that many witnesses”.[23]

The slate of active witnesses is daily updated, they all have a timeboxed turn to produce a block, if they fail, the next witness will produce the block, lowering the probability of having two competing chains due to blocks added at the same time. In this way, on the one hand, everyone can check the network performances by monitoring witnesses’ participation rate and, on the other hand, the election process is continuously iterated in such a way that each witness has the risk to be replaced by a more trusted node that gets more votes. Besides this, validator nodes can also be voted out by other users, when they are not trusted anymore, or when they fail to produce blocks. The more the network grows, the more intensive become the competition to become or remain a validator, the main incentives against malicious behaviour are a loss of income, deriving from the transactions fees, and nodes’ reputation.

Nodes participating in a network based on delegated proof of stake do not vote for only witnesses, but, they also elect a group of delegates. These delegates have the duty of supervising the network, and the performance of the blockchain protocol, without any right though, on transactions’ validation and block production. They have the privilege of proposing changes to the network such as modifying the size of a block or the transactions’ fees, and nodes will vote whether to adopt or not the proposed modification. The role of a delegate does not include any financial reward like transaction fees, unlike witnesses and, has no direct power in the network since every proposed modification has to be approved.

To conclude, delegated proof of stake speeds up transactions and blocks creation since the deterministic selection of blocks validators allows transactions to be validated in an average of just one second. This consensus algorithm incentivises decentralisation since shareholders keep the control of the network, and, decreases energy consumption when compared to proof of work algorithm.

**PoA - Proof of Authority:**

Proof of Authority is an alternative consensus algorithm, a modified Proof of Stake in which a validator's identity replace the role of the stake and, the nodes validating blocks are the ones explicitly allowed to do so. This peculiarity of Proof of Authority diversifies it from PoS since it allows to take into account the different interests that two nodes, even with the same amount of stake, may have in the network. A set of selected authorities has to create new blocks and secure the blockchain. The majority of the authorities have to agree on the current status of the transactions, and to sign off the chain; only then, it can be added to the blockchain and become permanent. The identity of a validator denotes the "congruity between a validator's identification on a platform with his official documents, i.e. certainty that a validator is exactly whom that person represents to be."[24] A robust process at asses whether the validators are whom they claim to be or not is needed, and difficult eligibility ensures validators to be a scarce resource, this incentivises them to retain the position they have earned since it is unpleasant to lose. "Individuals whose identity, and reputation is at stake for the securing of a network are incentivized to preserve the network."[25]

To recap, with PoA consensus is essential to: first, establish that validators' identity is true, and second, make validators' eligibility for staking hard to obtain through multiple exams. This creates integrity and transparency within the validators and the network, ensuring trust and lowering the risk fo nefarious threats.

# Conclusion

This chapter introduced the new technology of blockchain, explaining when and how it was created along with its evolution over the past ten years. A detailed description of the anatomy of a general block and its contents is given, focusing on the features that make each block unique and immutable. Successively, the chapter explained the different types of blockchains and where they are most likely to be implemented, delineating in this way their major differences, benefits and downsides. Finally, the different Consensus Algorithms, to agree on the current status of a blockchain, are introduced and elucidated considering for each one, benefits and limitations, as well as their general adoption in the cryptocurrencies world. The consensus protocols above described are the most commonly used algorithms. Nevertheless, they are not the only ones, Proof of Activity, Proof of Capacity, Proof of Burn and Proof of Elapsed Time are an example of other protocols with their benefits, and constraints. They are not considered in the research due to their limited applicability to a hypothetic healthcare blockchain. Table 2.2 outlines the different consensus algorithm and where they are being used.

| Consensus Algorithm | Resource Used | Examples of use |
|---|---|---|
| PoW | Computing Power | Bitcoin, BitcoinCash, Namecoin, Ethereum, Litecoin, Monero, Zcash, Zcoin |
| PoS | Ownership of tokens | Peercoin, BestChain, Blakestar, Buzzcoin NavCoin, Leo, Reddcoin, Linda, Neblio |
| D-PoS | Ownership of tokens and peer reputation | Bitshares, ONZ, Lisk, ARK, Rise, Oxycoin, NEO |
| PoA | Certified authorities, randomly selected | Parity PoA |

Table 2.2 Consensus Algorithms. Image Source: Author

Table 2.3 summarises the key features and concepts of blockchain in chapter 2.

| Features | Options | Definition |
|---|---|---|
| **Data Access** | Private | Only a selected set of nodes can transact and view transaction log in the system |
| | Public | Anyone can transact and view transaction log |
| **Consensus Participation** | Permissioned | Only a selected set of nodes participate in the consus algorithm and validate transactions. |
| | Permissionless | Anyone can participate in the consus algorithm and validate transactions. |
| **Consensus Algorithm** | PoW | High decentralisation, everyone can participate, high energy consumption transaction speed: low. |
| | PoS | Based on the stake of participants. High decentralisation since validators are selected based on their stake |
| | D-PoS | Based on their stake, participants can vote for witnesses and validators. High decentralisation. Trasaction speed: High |
| | PoA | Less decentralised, need for a trusted authority to validate data on the blockchain. Transaction speed: fast |

Table 2.3 Blockchain Features. Image Source: Author

Blockchain is truly useful when four conditions are met: “multiple parties generate transactions that change information in a shared repository, parties need to trust that the transactions are valid, intermediaries are inefficient or not trusted as arbiters of truth, and enhanced security is needed to ensure the integrity of the system.”[26] Chapter three focuses on the knowledge produced, until the time of this research, referring to the applicability of blockchain to solve healthcare system’s problems.

Chapter 3

# *Literature Review*

## Introduction

Chapter three summarises and presents the relevant literature about the application of blockchain to the healthcare system. The studies and researches displayed are not older than five years. This means that all the data and literature reviewed have been published after the end of 2012. The chapter is separated into four parts. The first part, 'Methodology', explains how the literature review was carried out. The second part, 'Problem Statement' underlines the major problems found in the literature reviewed. The third part, 'Proposed Solutions', summarises the relevant scientific papers that were taken into consideration for the research. The fourth part, 'Conclusion' sums up the major issues found in the literature review and the facets of the topic that have not yet been studied.

## Methodology

This section consists of an explanation of how the literature review about the theoretical concept of blockchain, and its applicability to the healthcare system, was carried out. Initially, a literature review about blockchain technology was performed to evaluate its current maturity level, potentialities and limitations. Secondly, the focus of the literature review shifts toward the applicability of blockchain to a specific industry: the healthcare. Both of them were carried out by using the following research engines and databases: Google Scholar, Google, Science direct, and Leiden Univerisity Libraries Catalogues. The analysed literature was found by searching the following keywords: "Blockchain", "Blockchain and Healthcare System", "Health Data Management", "Information Blocking", "Electronic Health Records", "Private and Public Blockchain", "MedRec", "Consensus Algorithms". The third step narrows down the focus to the relevant literature to collect relevant knowledge to answer the research questions. The final step results from the collection, analysis, understanding and categorisation of the entire literature taken into account in the research. This step aims to collect insights that are subsequently analysed to fill the gap found in the existing literature.

| Input | Process | Output |
|---|---|---|
| General terms about blockchain technology and its properties. | Desk Research. Gathering and analyzing information, already available and accessible on internet and Google Scholar. | Overview of blockchain technology, its maturity level, applications, properties, limitations and benefits. |
| More specific terms about blockchain technologies applied to healthcare system. | Secondary Research. Finding and collecting existing literature about blockchain applied to the healthcare system. | Gaps in earlier research, research questions, research relevance and a suitable design for the research. |
| Relevant terms regarding:<br>- Topic of the research questions<br>- The aim of the research | Grounded Theory Approach. Construction of theory with inductive approach, through methodic gathering and analysis of information. | Sensitized concepts, clustered in multiple tables. Lists of properties, issues and benefits regarding blockchain and the healthcare system. |
| Semi-Structured Interviews to blockchain and healthcare experts to answer RQs and gain general insights. | Analysis of the qualitative data<br>- Summarisation of meaning<br>- Categorisation of meaning<br>- Narration of meaning | Manageable and valuable insights with the creation of tables and frameworks to answer the research questions. |

Table 3.1 Research Methodology: Input-Process-Output. Source: Author

## Problem Statement

The majority of the population receives care from more than one caregiver or provider, like a physician, hospital, pharmacy, school clinics, or public health sites and so on. This fragmented nature of care affects its efficiency and quality and, does not ensure continuity of care through all its stages which can be achieved through a more patient-centred system, and through the shared use of IT interoperable systems, and Electronic Healthcare Records (EHR). Research on these problems had been carried out, and a growing body of scientific evidence supports the use of innovative technologies for the healthcare system to improve its efficiency and quality. Interoperable IT systems will support the adoption and use of EHR to share health data and, it will provide a seamless health experience for both patients and medicians. An EHR is a digital record containing information about the health of an individual. "An EHR should have the following attributes: accessibility and availability (continuous access to patient data or timely access to other information resources), reliability (ensures data integrity and permanence of original information in agreed format and for given time), usability and flexibility (support multiple user views and user-friendly interactions such as input and output of data), integration (enables the integration of different administrative and clinical systems), performance (provides information normally within a few seconds) confidentiality and auditability (providing an audit trail that documents the interactions, and authentication of information using user identification, e.g. digital signatures)."[27]

Why are electronic health records needed? Patients have no control over their medical records and medical data, they can not control how and where these are stored, and with whom they are shared. Moreover, medical stakeholders often act according to their company interest, hoarding in this way the interest of the patients and, it is a general belief in the medical community that patients are unable to handle their medical records. These problems result in fragmented personal medical data scattered and blocked across multiple healthcare institutions and providers for multiple reasons. "To obtain paper copies, individuals often have to face the inconvenience of going to a medical department on person, signing forms, paying a fee and, waiting 30 to 60 days to obtain their health information"[28].

Health data, according to Topol, "need to be accessible anywhere and always available to the originator; controlled by the person they came from; unique and verifiable as belonging to a real person; privacy enabled and secure; Independent from any third party; and able to solve the data provenance problem, that is, when, where and from whom the data came. It is critical for individuals to seize ownership of their data for the real benefits, of a new data-driven high-definition era of medicine to be actualised."[29]

How does this fragmentation nature of medical data affect the healthcare system? Incorrect and incomplete information, due to information blocking and poor medical data management, lead to daily tragic medical errors and, in the long term, decrease healthcare system's effectiveness and efficiency. According to many studies, a substantial number of medical errors, besides a considerable increase in healthcare costs, was the leading cause of death and complications. "According to the US department of health and human services, an estimated 20% of preventable medical errors are due to the lack of immediate access to health information. Of the estimated 400'000 annually preventable medical errors leading to death, we can project that approximately 80'000 people die every year."[30] Today, 220 people died due to the steep access to the necessary medical information. If we consider the US healthcare system " in 49 of the 50 states of the US, medical data are owned by doctors and hospitals."[31]

Health data ownership and information blocking are two of the major problems affecting the current healthcare system. The dimension of these problems captured the attention of the US Office of the National Coordinator (ONC) which, recently also released a report about information blocking. "Information blocking occurs when people or entities knowingly and unreasonably interfere with the exchange or use of electronic health information."[32] Likewise, the ownership, privacy and security of individual health information are the critical factors that are leading the research for an interoperable and scalable IT system to better manage patients' medical data.

## Conclusion

All the characteristics previously mentioned generate a centralised model for most of the healthcare providers. Such a model is negatively affecting the general healthcare system quality as well as patients' data integrity, ownership, privacy, and accessibility. However, according to many institutions, researchers and experts, this centralised model is coming to an imminent end. Even though "today electronic health record adoption is the highest it has ever been"[33], the advancement in new IT and Health technologies have led to a growing curiosity about how blockchain could be applied to the healthcare system, and to the discovery of new opportunities that can end the fragmented nature of EHR across multiple healthcare providers. Blockchain technology could lead to a shift in the way healthcare and medicine are practised. Although the adoption of innovative technologies seems quite irresistible, significant entry adoption barriers need to be passed. The main entry barriers for the adoption of interoperable IT systems between healthcare providers and personal electronic health records include costs, technical issues, system interoperability, and medical data privacy and confidentiality.

## Proposed Solutions

This section provides a systematic overview of the literature that has been produced about the topic of innovation in healthcare system through blockchain technology. The aim is to summarise and compare the major solutions proposed for the aforementioned problems.

**Encouraging blockchain adoption**

*"The federal government has invested over $28 billion to accelerate the development and adoption of health information technology: health IT."*[34] *The purpose is to avoid information blocking, enhance interoperability, and share more efficiently electronic health information.*

The Office of the National Coordinator for Health Information Technology (ONC) at the forefront of the administration's health IT efforts, aims to support the adoption of health information technology and to promote a nationwide health information exchange. It is organisationally located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS). ONC, together with partners, the state, consumers and the private sector, aims to achieve interoperable health IT infrastructure in 10 years, its vision is to "better inform decision making to improve individual health, community health and, population health."[35] By building a robust IT system for Health providers and patients, we could provide every single individual with a personal, digital record of their health over their lifespan. All these measures aim to shift from a provider-centred to a patient-centred healthcare system. The three primary critical factor for success, according to ONC are the exchange of electronic health information, availability of electronic health information and, the use of electronic health information. ONC's major goals are below summarised:

- *2015-2017: Send, receive, find and use priority data domains to improve healthcare quality and outcomes.*[36]
- *2018-2020: Expand data sources and users in the interoperable health IT ecosystem to improve health and lower costs.*[37]
- *2021-2024: Achieve nationwide interoperability to enable a learning health system, with the person at the centre of a system that can continuously improve care, public health, and science through real-time data access.*[38]

To reach these goals, HSS together with the ONC proposed a challenge in July 2016 with monetary awards, to encourage Blockchain adoption in the Health Information Technology field. This resulted in 15 scientific papers covering different topics about the use of Blockchain in healthcare services. All these white papers led to multiple, new opportunities regarding the implementation of blockchain in the medical field. The major discoveries are summarised and subsequently reported in this chapter.

### Blockchain and Health IT: Algorithms, Privacy, and Data.

This paper addresses the threats of data security, confidentiality, integrity, and availability of Precision Medicine Initiative PMI data. Centralised IT systems and databases can not continuously assure security and data integrity. "Perimeter defences such as hardware and software intrusion detection systems, fail to secure vital health IT infrastructures."[39] The proposed solution is the OPAL/Enigma Project which "creates a peer to peer network that enables parties to jointly store and analyse data with complete privacy"[40]. The last is an encrypted platform based on blockchain technology, that provides a secure environment to store and analyse healthcare data and a permanent and auditable record of transactions. The aim is to "resolve the tension between data sharing and privacy, in order to unlock the potential value of data"[41]. A system of permissioned distributed ledgers implemented on blockchain like OPAL/Enigma can track every modification of data, being in this way, auditable, trustworthy, and transparent. This system maximises security maintains the privacy of individuals while performing analysis on their medical data. Data will be queried but, only through "queries that are permissioned by digital identity credentials for specific data operations defined by legally binding smart contracts"[42]. With OPAL/Enigma, patients will be the owners of their medical data, these, instead of being stored in a centralised database, will be "transformed into shares and disperse on the peer to peer network of nodes. Only the data owner would know the location of the shares, and can fetch these from the nodes as needed."[43]

To conclude, OPAL/Enigma solution allows information to flow seamlessly and securely, by empowering patients with secure data ownership, enhancing population health management, and lowering healthcare costs.

### Blockchain: Securing a new Health Interoperability Experience.

This paper, from Accenture, proposes to integrate current health IT investments with a permissioned blockchain distributed ledger technology (DLT). The aim is to tackle medical data management major problems. First, through cryptographic techniques like private and public keys, secured and trusted care records will be created and, personal medical records will be added to the blockchain. Second, nodes participating in this network have verified "by preserving an immutable record of the declared identities of both patients and healthcare professionals."[44]

The aim is to empower patients by saving consent decisions on the blockchain and accessing them whenever needed. "By capturing patient consent statements in an immutable blockchain, healthcare professionals and others involved in the care cycle are able to trust those statements and act upon them accordingly. In addition, patients are able to add consent statements at any point in their care journey confident that the blockchain will hold them securely."[45]

Blockchain application to the healthcare system with the aforementioned two aspects will improve both clinician and patients experience.

**Blockchain Technologies:**

**"A whitepaper discussing how the claims process can be improved"**

Further research, by Kyle Culver, focused on how smart contracts executed on blockchain can improve the claims process and healthcare experience in general for all stakeholders. The main problem addressed here is administration costs associated with Billing and Insurance-Related (BIR) activities. "BIR costs are projected to reach $315 billion by 2018, up over 100% from 2007." [46] Moreover, "The complexity required to navigate these processes total up to 3.8 hours for the average American physician a week, the equivalent of more than three workweeks a year on interactions with payers"[47].

The solution proposed is a platform based on blockchain technologies on which smart contracts can be implemented to support every patient-provider health agreement to remove every intermediary from this sensitive process. "Smart agreements between stakeholders replaces ambiguity with clarity, driving down administrative cost and processing time across the healthcare industry."[48] This solution aims to improve standardisation, interoperability, and medical research.

**Deloitte: Blockchain, opportunities for Healthcare.**

The blockchain solution proposed by Deloitte aims to unlock the real value of interoperability to eliminate the frictions and costs of health intermediaries. The main problems addressed are interoperability and medical records accessibility. Deloitte believes that nationwide interoperability between health IT systems can be earned through a 'Consortium Blockchain' accessible only by health stakeholders and selected participants. Participation and data mining will be incentivised through financial compensation or, aggregated health data as a reward. On such a blockchain, medical data could be stored in two different ways: "On-chain, directly stored on the blockchain and, Off-chain data with links stored on the blockchain that act as pointers to information stored in separate, traditional databases."[49] Participants will connect and access the blockchain with a set of private and public keys which will allow them to visualise and share every health-relevant information. Smart contracts are also part of Deloitte's solution. They provide rules for processing and storing information on the blockchain; these information will be provided by an Application Program Interface API available to all the nodes participating in the network.

Notwithstanding the unique opportunities to reduce costs and enhance health IT systems' interoperability, Deloitte states the immaturity level of blockchain, "several technical, organizational, and behavioural economics challenges must be addressed before a healthcare blockchain can be adopted by organizations nationwide."[50]

**Blockchain: The Chain of Trust and its Potential to Transform Healthcare**

IBM, in its white paper about blockchain potential to transform healthcare, exposes the multiple pain points of healthcare industry, and the relative benefits that blockchain could introduce. Blockchain can enhance interoperability, accessibility, and data integrity by eliminating data silos, aggregating clinical data from Electronic Medical Record (EMR), and driving seamless interoperability between healthcare organisations.

Moreover, data integrity, privacy and security will be ensured through encryption and cryptology of records distributed in a peer to peer network. Healthcare experience and consumer engagement will be improved with better risk management and a more holistic view due to connected healthcare ecosystems. General complexity, frauds and abuses will be lowered with the implementation of smart contracts. These will provide network management in such a way that abuse of sensitive data, false claims, improper billing and corruption will be reduced. However, the paper points out the current challenges that blockchain has to go through before it is going to be adopted on a large scale. Scalability is one of the significant challenges since “blockchain is not well suited for high-performance transactions. It is not useful as a transaction processing replacement, and is unsuitable for low value, high volume of transactions.”[51]

**ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks**

This white paper describes ModelChain “a private Blockchain based, privacy-preserving healthcare predictive modelling framework”. This framework aims to integrate online machine learning with blockchain through a new consensus algorithm explicitly developed for ModelChain: Proof of Information algorithm. This new algorithm is implemented using blockchain 2.0 technologies, and on the last, will run smart contracts. ModelChain will solve the following interoperability problems stated in the Nationwide Interoperability Roadmap: Building upon the existing IT infrastructure; Maintaining modularity; Protecting privacy and security in all aspects of interoperability.

**Blockchain for Health Data and its potential use in Health IT and Healthcare related research.**

This paper aims to provide a blockchain solution to address the problems of Health IT interoperable systems, one of the main challenges according to the Office of the National Coordinator for Health Information Technology. The paper proposes the use of a public blockchain as an access control manager to health records that are stored off blockchain. This blockchain network has to be public and, to include technological solutions for three key elements: scalability, access security, and scalability. Scalability will be reached through users' unique identifiers stored on the blockchain linked to the healthcare record location, in this way, the information on the blockchain will serve as an index or pointer to a data lake containing, off-chain, the actual encrypted medical data. Data lakes provide scalability by storing a wide range of encrypted and digitally signed medical data. Access security and data privacy will be achieved through sets of access permissions designated by the patients to provide or revoke access to healthcare providers. To conclude, blockchain combined with data lakes will support a wide variety of medical data distributed across multiple servers with no single point of failure. Open API will be used to share data between health IT systems and health blockchain, providing interoperability that will positively support Patient-Centered Outcome Research PCOR, and the Precision Medicine Initiative PMI.

**A Blockchain-Based Approach to Health Information Exchange Networks**

A possible solution is described in "A blockchain based approach to health information exchange networks." The major goal of this paper is to present a feasible solution to "effectively and securely share healthcare information within a data sharing network based on blockchain"[52] What is addressed is the problem of sharing data between different technical architectures and infrastructures. The proposed solution implemented on the blockchain addresses the interoperability problem from two different perspectives:

- Structure: "Heterogeneous structures decrease the effectiveness of analysis and reduce understandability and semantics. To combat this, industry-wide standards have been advanced"[53].
- Semantics: "Refers to the use of terminologies and vocabularies to describe data meaning, or to codify the data"[54].

The blockchain solution proposed in the paper uses Fast Healthcare Interoperability Resources (FHIR). This is defined as "an emerging standard that depicts data formats and elements, along with providing publicly accessible Application Programming Interfaces (APIs) for the purpose of exchanging Electronic Health Records"[55].

Such a solution provides institutions with data control and keeps sensitive medical data off-chain. In this system, each block of transactions is added to the blockchain at regulars interval of times. The consensus algorithm used is Proof of Interoperability (PoI), an alternative method similar to PoS that solves some of the of disadvantages of PoW.

During the election process "each node is required to submit a random number to be used for miner election. This set of random numbers is collected on line 1 and is hashed together with the block hash to produce a new number. The next miner then becomes the node whose Public Key is closest to this value. This process serves two purposes: (1) The probability of becoming a miner for any node in the network N should be $1/|N|$, and (2) the random number used for election is seeded by all participating nodes in the network. This prevents a node from generating a non-random number and electing itself or a chosen collaborator"[56]. However, this consensus algorithm is not considered in the research due to its low adoption. Besides, the paper does not talk about private, public, permissioned, permissionless network, which is a critical factor when considering which consensus algorithm to adopt. PoI, according to experts, would not be efficient in a public network and, would be less efficient than PoS or D-PoS in a private network.

**Estonia eHealth**

Since 2016, Estonian government implemented a Keyless Signature Infrastructure (KSI) blockchain solution to secure health records of its 1.3 million residents. "Unlike traditional digital signature approaches, e.g.. Public Key Infrastructure (PKI) that depends on asymmetric key cryptography, KSI uses only hash function cryptography, allowing verification to rely only on the security of hash-functions and the availability of a public ledger commonly referred to as a blockchain"[57] KSI advantages are:

Scalability: "KSI blockchain scales at O(t) complexity, it grows linearly with time and independently from the number of transactions"[58]. Every medical record can be signed and stored using KSI avoiding the use of excessive computational power required by PoW algorithm and, in this way, enhancing scalability.

Settlement time: "The number of participants in KSI blockchain distributed consensus protocol is limited. By limiting the number of participants, it becomes possible to achieve consensus synchronously, eliminating the need for Proof of Work and ensuring settlement can occur within one second"[59] With this type of blockchain, a user submits a hash-value of his medical data to the system. The last, sign it into the KSI infrastructure and then returns a unique signature "which provides cryptographic proof of the time of signature, integrity of the signed data, as well as attribution of origin, i.e. which entity generated the signature"[60] In the Estonian E-health system, ledgers are saved on a backbone built on blockchain technology. This notifies and timestamps each access or modification to a patient's EHR which can be accessed with the use of an electronic ID-Card.

This blockchain solution revolutionised the healthcare system on a national scale by providing health data integrity, privacy, and security, three critical factors according to the Estonian government.

**A Case Study for Blockchain in Healthcare: "MedRec": A prototype for Electronic Health Records and Medical Research Data**

MedRec, a prototype for electronic health records and medical research data was presented by the MIT in its white paper: 'A case study for blockchain in Healthcare' (August 2016). MedRec is a "novel, decentralized record management system to handle EHRs, using blockchain technology"[61]. The fragmented nature of medical data that are scattered across multiple organisations and healthcare providers reflects the inefficiency of how these records are managed and this knowledge exploited. Patients have complicated, and sometimes expensive access to their medical data, "interoperability challenges between hospitals systems pose additional barriers to effective data sharing"[62] and incentivises information blocking. MedRec solution, implemented on the blockchain addresses four main issues "fragmented, slow access to medical data; system interoperability; patient agency; improved data quality and quantity for medical research"[63]

Indeed, MedRec gives patients "a comprehensive, immutable log and easy access to their medical information across providers and treatment sites"[64] and, it provides confidentiality, security and, records authenticity and auditability. Besides that, patients can now be informed and engaged about every update to their health records. Patients will be informed about every update to their medical record by the implementation and use of smart contracts on the blockchain which will automate and track patient-providers transactions with the relative's permissions to access health data. "Providers can add a new record associated with a particular patient and, patients can authorize sharing of records between providers"[65] Blockchain will support three types of contracts:

1. Registrar Contract to map participants identification;
2. Patient-Provider Relationship Contract to allow specific nodes of the system to manage and store medical records for others;
3. Summary Contracts that represent patients' previous and current transactions with other nodes in the system;

MIT states that MedRec proposition is to "restore comprehensive patient agency over healthcare information across providers and treatment sites, empowering citizens with the data they need to make informed decisions around their care"[66]. MedRec system addresses as well the ONC Interoperability Roadmap's first outcome: "Individuals have access to the longitudinal electronic health information, can contribute to the information and, can direct it to any electronic location"[67] What is not explicitly addressed by this paper is:

- Whether or not, a public blockchain implementing Proof of Work consensus algorithm will provide an interoperable, scalable, secure and costs saving solution. This issue is addressed later on in the research.
- The security of individual providers databases, on which patients data will be anonymously saved. Security issues regarding health providers databases are not addressed by the research.

Figure 3.2 pinpoint what has not been addressed by MIT in the MedRec prototype, i.e. whether using a public blockchain with a mining-bounty mechanism based on PoW would work or not.

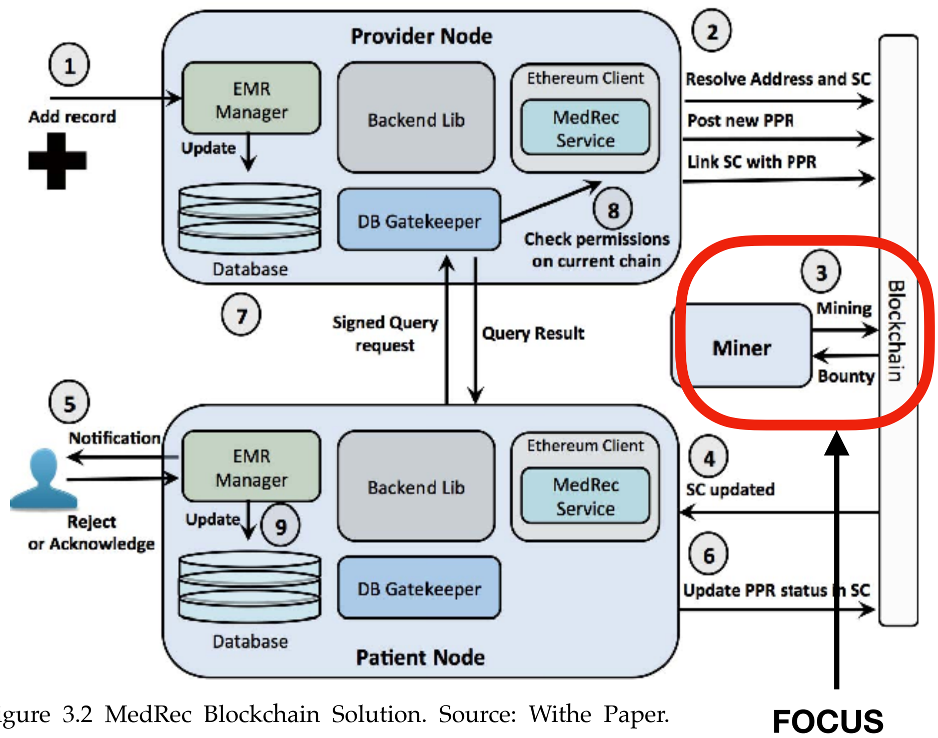



Figure 3.2 MedRec Blockchain Solution. Source: Withe Paper. "MedRec" prototype for electronic health records and medical research data.

The proposed solution to the mining problem is to involve medical researchers in the blockchain network. They will mine transactions on an Ethereum network, "in return for privacy-preserving, medical metadata in the form of transaction fees"[68]. Ariel Ekblaw continues "the cost to mine on MedRec will be held constant across participants, thus equalizing access to data and bringing in stakeholders outside of just academia and Big Pharma"[69]. In this way, researchers will be incentivised to mine in the network, and in return, they will access aggregate, anonymised medical data. Patients and healthcare providers will be able to decide which data to include in the available mining bounties. "This opens an opportunity to observe wide-reaching patterns in medical treatment, while still preserving the privacy of individuals and lowering the overhead associated with traditional research trials"[70].

## Conclusion

As blockchain technology becomes more used in many different areas, governments and private companies are also looking at its potential use in the healthcare system. Blockchain could drive a shift to a more patient-centered healthcare system, where patients' entire life cycle is tracked to assist them, by empowering patients with control over their medical data and by enhancing care-providers interoperability. Chapter 3 started with a general literature review regarding the problems of the healthcare system. The focus is then narrowed down to the research questions and objective with a more critical review of the most relevant papers concerning the topic. These papers are summarised and compared to highlight issues, missing aspects, and gaps of knowledge in the existing literature. Highlighting these issues facilitated the collection of data to provide new insights to solve the issues found in the literature review.

## Contribution to the existing knowledge

The research intends to enrich the existing body of knowledge concerning the possible application of blockchain technologies to the healthcare sector and to cover the current gap of knowledge regarding the evaluation of different network types and consensus algorithms applied to the healthcare system. The problems addressed by the RQs in Chapter 1 are not yet being explored. Numerous solutions, summarised in Chapter 3, have been proposed until the time of this research. Each one has different technical properties, benefits and drawbacks. However, these solutions and the online literature do not provide a clear evaluation of the benefits and limitations that different types of consensus algorithms and blockchain network types would bring to the healthcare system.

For these reasons, this research aims to provide a multicriteria evaluation of blockchain technologies in the healthcare system to establish which type of blockchain and consensus algorithm fits the best with the healthcare system's properties. The issues found in the literature review are summarised below:

- Different papers address different specific problems of the healthcare system, nevertheless, there is not a clear blockchain solution preferred over others which addresses all the problems of the healthcare system.
- Even though multiple papers describing blockchain solutions have been proposed, there is still a lot of ambiguity about which type of blockchain and consensus algorithm these solutions should adopt.
- There is a lack of online literature evaluating the adoption, and consecutive impact, of different types of blockchain networks and consensus algorithms in the healthcare system.

In order to answer the research questions and provide a scientific evaluation, a deeper understanding of blockchain technologies, and of the prototypes proposed so far to solve the healthcare system's problems, is required. The research uses an inductive approach aiming to build a theory from the insights collected. This knowledge will be obtained by summarising, comparing, and evaluating the solutions aforementioned with the help of blockchain, and IT healthcare experts. With multiple interviews to blockchain and healthcare experts, it will be possible to address the major issues found in the literature review and to find out which properties of blockchain technologies are necessary to implement such a solution in the healthcare system.

Chapter 4

# *Design & Implementation*

## Introduction

This chapter aims to explain how the research is going to be carried out. Specifically, how data will be collected in order to answer the aforementioned research question, and sub-questions. The research Design & Implementation is an overview of the main steps and methods necessary to reach the aim of the research.

## Theoretical Framework

The following section aims to explain how the design of the research was delineated. To elaborate on a suitable research design, the research refers to the 'research onion diagram' illustrated below in Fig 3.3. The diagram was used to execute the study in a well-structured way by dividing it into different layers peeled off during the research.

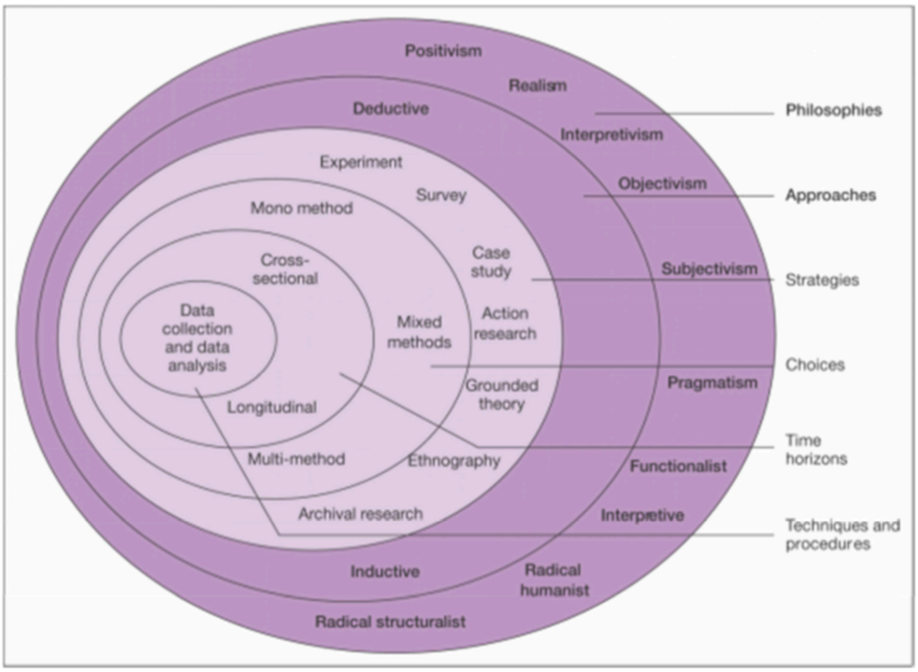



Figure 3.3 Onion Diagram. Source: Saunders,M., Lewis,P., and Thornhill, A. *Research Methods for Business Students*.

## Research Layers

**Philosophical Context**

Regarding the 'philosophical context', the research follows a Pragmatist and Interpretivist approach. "Pragmatists recognise that there are many different ways of interpreting the world and undertaking research, that no single point of view can ever give the entire picture and that there may be multiple realities"[71], concepts are relevant only if they support the research questions objectives. "Interpretive researchers assume that access to reality (given or socially constructed) is only through social constructions such as language, consciousness, shared meanings, and instruments"[72]. This context helped to understand the need to evaluate the different blockchain prototypes and solutions proposed by researchers with different experiences, approaches and social constructs.

**Research Approach**

The research approach used for this study is mostly inductive, notwithstanding that the deductive and inductive approaches are not mutually exclusive. Approaching this research with the right method, and the type of reasoning had been essential to carry out scientific results. This study adopted mostly inductive reasoning to draw conclusions from existing evidence and enrich our body of knowledge through the study of current literature and the collection of qualitative data through multiple experts interviews.

**Research Strategy**

The research strategy refers to how the work and the results were carried out. The strategy used is the 'Case Study Research', through the assessment of multiple case studies, new key insights and knowledge are used to draw generalisations. This type of strategy is effective in comparing different project, companies, and cases to draw scientific conclusions.

**Research Choices**

These choices include the mono method, the mixed method, and the multi-method. This study, in particular, adopted the multi-method approach. Data collection and analysis will be carried out mostly through the collection of qualitative data with multiple experts interviews, and by analysing the existing body of knowledge concerning healthcare and blockchain systems.

**Time Horizons**

Besides the method, this study can be defined as cross-sectional since, it investigates a particular matter at a given point in time, like a snapshot. The investigation is concerned with the study of blockchain phenomenon applicability to healthcare system at a specific time of the research. Conversely, a longitudinal study investigates a matter across a long time-frame. However, the new knowledge that was published during the time of the study had continuously been analysed and compared with the ongoing research.

**Data Collection and Analysis**

Data Collection and Analysis depend on the methodological approach used. This research utilises both primary and secondary qualitative data. Primary qualitative data will be collected thought blockchain experts and medical professionals interviews. Non-numerical data, participants' insight, knowledge, opinions, and relationships between these, are analysed using data collection techniques and analytical procedures. Secondary data, information that has already been processed by other field experts, are derived from the scientific papers and studies of other researchers analysed in the literature review.

# Research Design

This section aims to put into practice what has been planned in the 'Theoretical Framework'. There are multiple research design: the descriptive, explanatory, and the exploratory.

This research design can be defined as exploratory since it "is an exploration of an issue that takes place before enough is known to conduct a formulaic research project. It is usually used in order to inform further research in the subject area"[73]

This research uses literature review, expert interviews, qualitative data analysis, and case studies as research methods to turn theory into practice and to answer the following research questions:

*"Which type of blockchain and consensus algorithm meets and fulfils the essential criteria for a blockchain solution to be applied to the healthcare system?"*

Hence, only crucial elements that fall within the following four categories will be examined:

I. *'Healthcare System's Problems'* related to the not adequate use of IT systems
II. *'Blockchain Solutions' Benefits'* to the healthcare system
III. Different *'Blockchains' Types'* and their potential effects on Blockchain solutions' benefits to the healthcare system
IV. Different '*Consensus Algorithms'* and their potential effects on Blockchain attributes.

## Quality of the Research

It is important to determine beforehand the overall quality of the research that is being carried out to understand whether it is going to build accurate knowledge and theories, or not. Research quality can be judged considering two major elements: ‘Reliability & External Validity’, and ‘Construct Validity’.

- *Reliability & External Validity:* data collection and analysis should produce the same findings if repeated by someone else in the future. This means that interviewing different experts will produce the same results. The importance is not the result itself, but it is understanding ‘to what extent interviewing different experts would produce similar results’. Reliability is strongly dependent on structured and methodological research.
- *Construct Validity:* it is is "the degree to which a test measures what it claims, or purports, to be measuring”[74] To what extent will the research measure what it originally wanted to test? To answer this question is essential to understand how much the sample of blockchain experts is representative of the content test was initially designed to measure.

## Conducting Interviews

A total of seven interviews with blockchain experts were carried out during the entire research. The interviews had two different natures:

- *Scoping Interviews:* To explain and clarify blockchain properties and healthcare system’s problems. These interviews influenced the composition of Tables 5.1, 5.2, 5.3 and 5.4 and Fig 5.1 reported in Step One, Two, and Three of Chapter 5.
- *Formal Validation Interviews:* with Blockchain Professionals and Medical Experts, to gather information on Blockchain applicability to the healthcare system; and to validate the information collected, and modelled across the different matrixes, with the first scoping interviews.

The first interviews were conducted in an unstructured manner in order to promote discussion and explore key areas and aspects that arose during the interview. "The informal nature of an unstructured interview enables a researcher to gain a clearer understanding of the area by being able to encourage discussion and learn about new aspects of Blockchain"[75] The second type of interview were conducted in a semi-structured manner considering that they benefited from the insights obtained from the previous ones. The semi-structured interviews' document is reported in the appendix.

### Blockchain Interview Sampling

Experts were selected based on two, not mutually exclusive, criteria: expertise in blockchain technology, and expertise in healthcare technology systems. The experts' provenance and company (when allowed) are listed in the table below:

| # | Interview Type | Country | Company and Position | Experience |
|---|---|---|---|---|
| 1 | Scoping Interview | Australia | Researcher, Post Doc University of South Wales | 3 years |
| 2 | Scoping Interview | Malta | Blockchain Consultant, Codit Belgium | 1 year |
| 3 | Validation Interview | Italy | CEO, Founder Minded Security | 7 years |
| 4 | Validation Interview | Italy | Preseident Blockchain association Italy, CEO Lynkeus | 5 years |
| 5 | Validation Interview | Italy | Blockchain Expert | 5 years |
| 6 | Validation Interview | Italy | CEO Next generation Currency | 2 years |
| 7 | Validation Interview | Australia | CEO Kinect, driving BC solution in healthcare | 4 years |
| 8 | Validation Interview | Belgium | Blockchain Consultant, Codit Belgium | 1 year |

Table 4.1: 'Conducted interviews list'. Source: author

### Interview Protocol

Interviewees were contacted via Skype call and face to face when possible and were held in English and Italian. Every interview was recorded with the explicit permission of each professional interviewed, and the records were then partially transcribed. The interviews conducted, had the aim of identifying which blockchain's attributes result in which benefits, and how these benefits change in intensity due to the type of blockchain, and consensus algorithm adopted.

**Interview Data Evaluation**

The semi-structured nature of the interviews resulted in two different analysis. One for the data collected with specific structured questions, closed ended-questions. The other one for data collected in the final part of every interview. This part aimed to promote free discussion to explore experts' knowledge, experiences and suggestions through open-ended questions.

- *Open-ended questions:* The qualitative data collected with Open-ended questions have been analysed following three major steps: 'Summarisation of Meaning', 'Categorisation of Meaning', and 'Narration of meaning' as presented in Chapter 5. Interviews were transcripted, when relevant to the research, to tag and code relevant lines and quotes. Tagging and coding helped the identification of patterns and affinities to connect and interrelate the insights collected and used to build Tables 5.4, 5.6, and 5.7.
- *Close-ended questions:* These questions served to systematically rank blockchain properties and their effects in multiple tables. Table 5.3 collected experts' evaluation of technical properties, and not, of blockchain, that would have influenced its future adoption. Experts ranked these influences from 1 to 5. Table 5.4 was built with close-ended questions in scoping structured interviews. Here, experts had to answer whether specific properties of a blockchain solution would bring higher benefits with the adoption of different types of networks and consensus algorithms or not. The properties in Table 5.6 and 5.7 defined using open-ended questions have been successively ranked asking close-ended questions to experts. Findings are then used to draw results for the final part of Chapter 5.

Chapter 5

# *Research results*

## Introduction

Chapter 5 presents the main findings from the literature review, and experts interviews. It is divided into five steps. ‘Step One’ demarcating healthcare systems’ problems from the literature review. ‘Step Two’ finding blockchain effects on healthcare problems. ‘Step Three’ Root Causes of blockchain effects. selecting blockchain benefits that may change accordingly to the type of blockchain and consensus algorithm adopted. ‘Step Four’ evaluate and quantify this intensity changes through summarisation and categorisation of meaning. ’Step Five’ find the best blockchain solution that can be applied to the healthcare system through the narration of meaning.

## Step One: “Finding the healthcare system’s problems”

Table 5.1 summarises the problems found with the literature review conducted in Chapter 3. The problems were selected based on their importance and affiliation with medical IT systems. Indeed, the table lists only problems that, directly and not, resulted from the improper or incorrect use of various health IT systems. These problems, according to experts, could be solved by the adoption of a scalable blockchain solution capable of enhancing interoperability and providing a more effective and efficient medical data management. Indeed, as stated in multiple papers analysed in Chapter 3, a shift toward a patient-centered healthcare system can be obtained through a scalable blockchain solution that provides interoperability and better medical data management. Such a solution, as illustrated in Fig 5.1, would enhance population health management, medical research, patient engagement and the overall quality of the healthcare system.

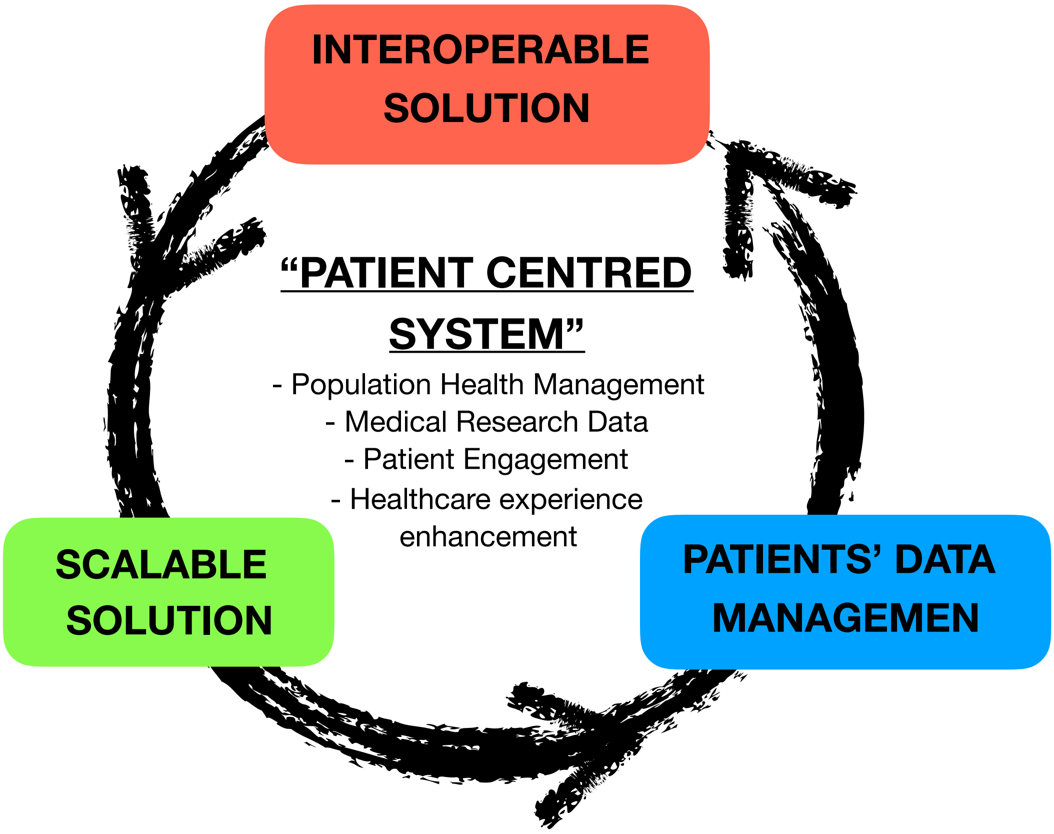



Figure 5.1: Aspects of a more patient centred system. Source: Author

| Healthcare System Problems | Impact | Source |
|---|---|---|
| Different IT Systems | *Interoperability, Scalability* | 1-2-3-4-5-7-9-10-11-12-13-15-16 |
| Information Blocking | *Interoperability* | 5-7-9-10-16 |
| Incomplete, Incorrect Medical Data | *Interoperability, Patients' Data Management* | 1-4-5-8-9-16 |
| Health Data Privacy | *Patients' Data Management* | 1-5-8-11-12-14 |
| Health Data Security | *Patients' Data Management* | 1-4-8-11-12-14 |
| Health Data Accessibility | *Patients' Data Management* | 1-4-5-8-9-16 |
| Data Silos | *Interoperability* | 2-5-16 |
| Data Complexity | *Interoperability* | 1-6-13-16 |
| Claim Process Complexity | *Patients' Data Management* | 3-11-14-15-16 |
| High Care Costs | *Patients' Data Management* | 3-5-7-13-15-16 |

Table 5.1: Healthcare system's problems. Source: Author

All these problems result in a healthcare system characterised by high costs, funnel vision, low transparency, and a not patient-centred attitude. As previously stated, a blockchain solution in order to be effective should be scalable, provide systems interoperability, and better patients' data management. The next section, 'Step Two' lists Primary and Secondary effects in Table 5.2, to asses their type of impact.

# Step Two: "Blockchain effects on healthcare problems"

Step two summarises, using the existing online literature from Chapter 3, the benefits that blockchain solutions would bring to the healthcare system. These benefits are listed in Table 5.2. The 'Type of effect' column refers to who or what, solving a specific problem, will benefit. A 'Primary Effect' impacts the organisational context of the healthcare system itself. A 'Secondary Effect' influences the healthcare stakeholders in the network. So a 'Tertiary Effect' interests the society, and how care is provided to a broader perspective. The papers, sources of this list of benefits, are listed in the next paragraph 'List of 15 white papers'. These papers were collected by the US Office of the National Coordinator for Health Information Technology during a challenge to support the development of more patient-centered care through the adoption of a blockchain solution.

| Benefits of BC on the HC system | Type of effect | Source |
|---|---|---|
| IT Systems Interoperability | *Primary Effect* | 1-2-3-4-5-7-8-9-10-11-12-13-14-15 |
| Health Information Exchange | *Primary Effect* | 1-2-5-12-13-14-15 |
| Avoid Information blocking | *Primary Effect* | 5-9-12-13-15 |
| Health Data Ownership | *Secondary Effect* | 1-2-4-5-78-9-10-12 |
| Patients Longitudinal Health Records | *Secondary Effect* | 2-4-5-9-11-15 |
| Health Data Security | *Secondary Effect* | 1-2-6-7-8-9-10-11-12-14 |
| Health Data Privacy | *Secondary Effect* | 1-2-5-6-7-8-9-10-11-12-13-14 |
| Health Data Integrity | *Secondary Effect* | 1-2-4-5-7-8-9-12-14 |
| Health Data Accessibility | *Secondary Effect* | 4-5-8-9-11-12-13-14 |
| Health Data Availability | *Secondary Effect* | 1-9-11 |
| Devices integration (IoT) | *Secondary Effect* | 2-6-8 |
| Population Health Management | *Tertiary Effect* | 1-4-5-11-12-15 |
| Medical Research Data | *Tertiary Effect* | 1-2-3-4-8-9-10-11-12-13-14 |
| Reduced Costs | *Primary Effect* | 1-2-3-4-7-8-13 |
| Patient Engagement | *Tertiary Effect* | 2-6-8-11-13-15 |
| Complinance to HIPAA regulations | *Secondary Effect* | 8-9-10-15 |
| Healthcare Experience Enhancement | *Tertiary Effect* | 2-3-6-12-13-15 |
| Smart Contracts Implementation | *Primary Effect* | 1-3-4-5-9-13-14 |
| Transparent Processes | *Primary Effect* | 1-3-4-7-15 |
| Enhanced claim process | *Primary Effect* | 3-4-7-8 |

Table 5.2: 'Effect of a blockchain solution on healthcare system'. Source: Author

## List of 15 white papers

The following list presents the 15 white papers that have been read and analysed in the literature review. "A challenge held by the US Department of Health and Human Services (HHS) to encourage Blockchain use in the Health Information Technology field resulted in 15 winning whitepapers". The challenge was announced in July 2016 by ONC Department for Health Information Technology. Paper 16 refers to ONC's 'Report to Congress'.

1. "Blockchain and Health IT: Algorithms, Privacy, and Data. Allison Ackerman Shrier, Anne Chang, Nadia Diakun-Thibault, Luca Forni, Fernando Landa, Jerry Mayo, Raul van Riezen" MIT
2. Blockchain: Securing a new health interoperability experience. Brodersen ; Kalis ; Leong ; Mitchell ; Pupo ; Truscott ; Accenture
3. Blockchain technologies. A white paper discussing how the claim process can be improved. Kyle Culver. Humana
4. Blockchain. Opportunities for Healthcare. RJ Krawiec, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai. Deloitte
5. A Case Study for Blockchain in Healthcare: 'MedRec' Prototype for Electronic Health Records and Medical Research Data. Ariel Ekblaw, Asaph Azaria, John Halamka, Andrew Lippman. MIT Media Lab
6. The Use of a Blockchain to Foster the Development of Patient-Reported Outcome Measures. J. Goldwater, National Quality Forum.
7. Powering the Physician Patient Relationship with 'HIE of One' Blockchain Health. Adrian Gropper
8. Blockchain: The Chain of Trust and its Potential to Transform Healthcare. IBM Global Business Services Public Sector Team
9. Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records. Drew Ivan

10. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. Tsung-Ting Kuo, Chun-Nan Hsu, and Lucila Ohno-Machado.

| Technical aspects (and not) of blockchain | Impact on blockchain adoption |
|---|---|
| Adoption Easiness | ★★ |
| Network Speed | ★★★★★ |
| Innovation Readiness | ★★★ |
| Trasaction Fees | ★★ |
| Consumption Costs | ★★★ |
| Authentication Control | ★★★ |
| Integration Readiness | ★★ |
| Network Control | ★★★ |

Table 5.3: Technical properties and not of a blockchain solution with impact on its adoptability. Source: Author

11. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research. Laure A. Linn Martha B. Koo.
12. A Blockchain-Based Approach to Health Information Exchange Networks Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Boles. Mayo Clinic
13. Adoption of block-chain to enable the scalability and adoption of Accountable Care. Ramkrishna Prakash.
14. A Blockchain profile for medicaid applicants and recipients. Kathi Vian, Alessandro Voto, and Katherine Haynes-Sanstead.
15. Blockchain and alternative payments models. King Yip.
16. ONC 'Report on Health Information Blocking', Department of Health and Human Services.

## Step Three: "Root causes of blockchain effects"

In this section, blockchain benefits and properties are clustered depending on their impact on solutions' interoperability or scalability or patients' data management. Results are displayed in Table 5.4. This table takes into account:

- Only the benefits of blockchain listed in Table 5.2 with primary and secondary effects since these are directly ascribable to the technical properties of blockchain. Benefits giving a tertiary type of effects are not considered since they do not directly result from the technical aspects of a blockchain solution.
- Other properties of blockchain (listed in Table 5.3) that influence the quality of a blockchain solution, and its acceptability. The table was made with the help of a blockchain consultant and, every property was ranked interviewing experts.

As mentioned before, properties are then clustered in Table 5.4 considering which aspect of the healthcare system they will improve: scalability, interoperability or, patients' data management. Columns f(x) indicates whether the strength, intensity of a benefit depends on the 'Type of Blockchain' (BT) or 'Consensus Algorithm' (CA) adopted. The following three tables were generated and elaborated with the help of a blockchain expert that has been interviewed twice.

| **Scalability** | **f(x)** | **Patients' Data Management** | **f(x)** | **Interoperability** | **f(x)** |
|---|---|---|---|---|---|
| Adoption Easiness | CA | Data Integrity | - | Health Information Exchange | - |
| Network Speed | CA | Data Privacy & Security | - | Smart Contracts Adoption | BT |
| Innovation Readiness | BT | Data Accessibility & Availability | - | Network Control | BT |
| Transaction Fee/Costs | CA | Data Ownership | - | Health Data Access | - |
| Consumption Costs | CA | Integration readiness (IoT) | BT | | |
| | | Longitudinal Health data | - | | |
| | | Authentication Control | BT | | |

Table 5.4: Properties of a blockchain solution clustered based on their impact on the three essential features of a good health IT system. Source: Author

The following two Table 5.5a and 5.5b define for every attribute listed before in Table 5.4.

| **Health Data Management** | ***The process of developing, executing and ensuring policies, practices and health data properties to properly manage medical data.*** |
| --- | --- |
| Data Integrity | Refers to the accuracy of medical data. In the healthcare system, data can not be modified without permission. Records' immutability is one of the main benefits of blockchain, different types of consensus algorithm can mitigate data tampering and modification. |
| Data Privacy | Refers to the practice of maintaining the confidentiality of patient records. The advent of electronic medical records (EMR) has raised new concerns about privacy, |
| Data Accessibility | Refers to the degree to which healthcare stakeholders can access medical data, one of the major problems of the healthcare system. With blockchain, different users will have different rights and levels of access, handled by smart contracts. |
| Data Security | Refers to personal health data protection against unauthorised access, use, disclosure, modification, inspection, or destruction. Security is enhanced through data encryption and cryptology. |
| Data Ownership | To which degree patients, own and control their medical data stored in Electronic Medical Records EMR or Electronic Health Records EHR? Blockchain will solve the problem of lack of clear data ownership by shifting a patient centred system in which patients own their medical records. |
| Longitudinal Health data | Refers to the span of time that patients' health data cover. Longitudinal health data picture of the patients' health across a life-long time frame. |
| Integration readiness | Refers to the degree to which medical data and EMR or EHR of patients already collected by doctors and care providers can be integrated in such a blockchain solution. |
| Authentication Control | The degree to which extent different types blockchain can better use authentication control to provide data security, privacy and integrity. The use of encryption keys will handle patients' identity confirmation. |

Table 5.5a: Properties definition. Source: Author

| | |
|---|---|
| **Interoperability** | ***Ability of healthcare stakeholders like Hospitals, Doctors, General Practitioners, Patients to exchange, read and use Medical Data spread across different providers*** |
| Health Information Exchange | Ability of healthcare stakeholders like hospitals, doctors, general practitioners, and patients to exchange, read and use medical information like EMR or EHR to make informed health decisions. Data exchange through a common blockchain will strengthen transparency and efficiency and, reduce data silos and information blocking. |
| Smart Contracts Adoption | To which extent Smart Contracts can be implemented on different types of blockchain to reduce intermediaries, enhance efficiency in medical claims and bills. Smart contracts automate and track patient-provider relationships to execute certain actions on external databases (which will contain patients' raw medical data) |
| Health Data Access | To which extent different health stakeholders can access medical data stored in a different provider database |
| Network Control | To which extent trust is centralised to one, few or countless participants in the network. The degree of control over the network can reduce frauds and abuses with the help of some blockchain features like traceability, accountability and time-stamped protocols. |
| **Scalability** | ***To which extent is a blockchain solution like Medrec scalable and, it can be enlarged to accommodate its wide adoption in the healthcare system.*** |
| Consumption Costs | Costs for consumption of hardware resources needed to run a blockchain network, and to validate data on it. |
| Transaction Fees | To which extent can different consensus algorithms allow you to exploit transaction fees at your advantage (e.g. charge fee for stakeholders, when medical data need to be validated, to pay hardware consumption, or charge small fees on a public blockchain to reduce garbage transactions). |
| Innovation Readiness | To which extent different types of blockchain can support the future integration and exploitation of innovative technologies such as AI, IoT, Virtual Reality and, Big Data. Innovation readiness is a critical feature for health IT systems to easily integrate technologies that could improve the average quality of life. |
| Adoption Easiness | To which extent different consensus algorithms will influence the adoption of a blockchain solution. Diverse consensus algorithms have different complexities, time and power consumption, these features discourage medical stakeholders to adopt and use them. |
| Network Speed | To which extent different consensus algorithms will affect the speed to which medical transactions are validated and added to the blockchain. |

Table 5.5b: Properties definition. Source: Author

## Step Four: "Evaluation of root causes"

This passage is characterised by two major processes: Summarisation, and Categorisation of Meaning. Attributes, whose intensity depends on the type of blockchain (BT) or consensus algorithm (CA) adopted, are listed in Table 5.6 and 5.7. Experts interviews guided the evaluation of each attribute considering blockchain type and the consensus algorithm adopted. The first step to evaluate the interviews has been the 'Summarisation of meaning'. Only the key insights were extracted from the transcripts, and their most important aspects for the research were highlighted. The second step, the 'Categorisation of meaning', involved the search for common codes and similar perspectives within the 'Summarisation of Meaning'. Searching for connections and relationships between codes and looking at the occurrence of specific keywords, lead to the creation of different categories of meaning regarding experts' opinions on different types of blockchain and consensus algorithm applicability to the healthcare system. These two steps were necessary to systematically evaluate the attributes in Table 5.6 and 5.7 to provide the final input for 'Step Five: Results'.

Every expert that had been interviewed was asked to weight from 0 to 2 every blockchain property that depends on the network type and the consensus algorithm. A weight of 0 was used for attributes that were considered difficult to execute on a particular type of blockchain or with a specific consensus algorithm. A weight of 1 was used when a determined network type or consensus algorithm was qualified, suited to provide a specific feature. A weight of 2 was always used to indicate the best network type or consensus algorithm for a specific attribute. Elements were weighted and not exclusively chosen since 'the perfect solution' does not exist but different solutions have different advantages and limitations. Weighting granted the research to understand the line of thought of experts in blockchain and healthcare. Below, in the two tables, are reported the major key insights collected with experts' interviews.

| Blockchain Features | Public Permissioned | Public Permissionless | Private Permissioned | Private Permissionless |
|---|---|---|---|---|
| Innovation Readiness | 0 | 0 | 14 | 8 |
| Integration Readiness | 0 | 0 | 14 | 8 |
| Authentication Control | 3 | 2 | 14 | 7 |
| Smart Contracts Adoption | 0 | 0 | 14 | 14 |
| Network Control | 4 | 0 | 14 | 8 |

Table 5.6: Summarisation of meaning. Intensity of benefits based on blockchain network type. Source: Author

| Effect | PoW | PoS | D-PoS | PoA |
|---|---|---|---|---|
| Network Speed | 0 | 8 | 11 | 12 |
| Consumption Costs | 0 | 8 | 9 | 13 |
| Adoption Easiness | 6 | 10 | 11 | 11 |
| Transaction Fee/Costs | 10 | 9 | 11 | 0 |

Table 5.7: Summarisation of meaning. Intensity of benefits based of consensus algorithm type Source: Author

The final weights are the sum of every expert's vote. Seven experts have been interviewed so far. Some quotes from the experts:

- Massimiliano Faudarole: *"Nowadays, we attend conferences where is explained why a blockchain was adopted, without talking about any technical property, almost as if it had to "convince" that adopting a blockchain is a good solution".*

- Giorgio Fedon: *"Proof of Authority, if you have trusted entities, it is the fastest and best algorithm that can be easily adopted and maintained".*

- Sin Kuang Lo: *"The cheapest one is the Proof of Authority, no electricity, no stake of coins. You are hiring someone, a trusted party to do the work for you, doctors will be playing the role".*

- Guy Newing: *"A certain centralisation of power is needed in order to implement a blockchain solution for the healthcare system".*

## Step Five: "Results"

Step Five presents the 'Narration of meaning'. It elaborates on the data collected from the research after data saturation was reached. Data saturation is defined as "the stage when any additional data collected provides few, if any, new insights"[76]. The narration of meaning aims to picture the story data want to tell and to translate the last into insights to answer the research questions. The qualitative data collected, have been subsequently coded and analysed, to gain clear insights on which blockchain solution is the most appropriate after the multicriteria analysis and why.

As evident from Table 5.6, a private permissioned blockchain is the most preferred solution according to all the experts interviewed. This type of network was ranked the best in:

- *Innovation readiness:*

To which extent, different types of blockchain can support the future integration and exploitation of innovative technologies such as AI, IoT, Virtual Reality and, Big Data. A permissioned private Ethereum Blockchain is "a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralised applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions"[77]. Through the creation of decentralised apps (Dapp), Ethereum blockchain would provide a solid integration with Artificial Intelligence and, consequently, a more appropriate tool to make use of medical Big Data. This argument is supported by many experts at Cambridge and Stanford University. Developers, within these two universities, are working together on 'doc.ai', a platform built on Ethereum that makes use of Artificial Intelligence to learn from the cumulative information gathered about patients to customise itself accordingly to the situation.

- *Integration Readiness:*

The degree to which medical data and EMR or EHR of patients already collected by doctors and care providers can be integrated into a blockchain solution. Permissioned Private blockchains are preferred. Most of the experts suggested that such a blockchain solution should be built in Hyperledger Fabric 1.0 or Ethereum. Both the platforms aim to develop specific blockchains for enterprises, helping, for example, the healthcare industry to realise its full potential. Permissioned blockchains efficiently answer to different needs of different participants in the network that can act independently. Old medical data saved off-chain in external databases will be collected with the help of smart contracts. Smart contracts will function as data pointers that access medical records across multiple databases, furthermore a single common interface will enable patients to view and share the medical data they want when needed. To conclude, the enabling factor that encourages the use of a private permissioned blockchain for better integration readiness is, again, the use of smart contracts.

- *Authentication Control:*

The degree to which extent different types of blockchain can better use authentication control to provide data security, privacy and integrity. One of the main problems of blockchain that yet need to be solved is the "Identity verification". This means ensuring individuals that claim identities in the network are the rightful owners of these identities. In a private permissioned network with a Public Key Infrastructure (PKI), a certificate authority will be able to handle the identity verification. According to experts, this could be done face to face or through a tight online control to make sure that the person accessing the data is actually whom he claims to be. Besides identity verification, C.A. will handle certificates and authorisations for the trusted digital entities (nodes) in the network. The "C.A. will issue and manage certificates needed for the trusted digital identities to implement strong authentication, digital signatures, and data encryption"[78]. Moreover, using a private permissioned blockchain alongside asymmetric encryption to create a PKI, will be fully GDPR compliant, patients' medical data will never be revealed to the owners of the medical blockchain, providing data security and privacy. (The public keys are used to identify individuals, while the private key will function as the security signature)

- *Network Control:*

A private-permissioned blockchain provides the most effective network control since nodes have first to request access and secondly only selected nodes are able to participate in the consensus algorithm. Network control within this blockchain includes designating different permissions, put restrictions, control nodes activity and managing the different level of access for each node in the network. The owners of the network (the certificate authorities in case poA is being used, or delegates in case D-PoS is being used) will be empowered to manage these permissions and access. The security of these networks is directly linked to the capacity of guaranteeing the network impenetrability among non-authorized individuals. A public blockchain is not considered (even though MedRec, as explained in Chapter 3, makes use of it) since does not implement access control. Public blockchains are designed for public consumption and not for enterprise applications, like private ones.

- *Smart Contracts:*

Smart contracts role will be critical to automatically execute updates to the shared ledgers and helping users managing transactions between them. General complexity, frauds, abuses and claims process will be enhanced to support every patient-provider health agreement, and to remove every intermediary from this sensitive process. This feature will improve efficiency and reduce costs in the medical ecosystem. Smart contracts, according to experts, work the best in a private permissioned blockchain like Ethereum since the platform allows developers to code the smart contracts they need, and since the coding and structuring of these smart contracts necessitate of legal support from experts within these private platforms. They need to define with extreme precision the conditions and modalities that control the activation of predetermined actions.

As evident from Table 5.7, different consensus algorithms have different benefits. The research evaluated through experts interviews

- *Network Speed:*

According to experts, Proof of Authority provides the higher speed in term of transaction validation per second; indeed it can handle thousands of transactions per second. It is a centralised method, this means authorities, or a consortium, have the responsibility of reaching consensus to validate medical transaction on the blockchain. Even though decentralisation is one of the keywords for blockchain and PoA is the less decentralised algorithm, it has the lowest power consumption and the fastest speed for transactions verification. The second best option after PoA is the Delegated Proof of Stake. D-PoS is preferred to the normal PoS since it promotes collaboration between the witnesses, speeding up in this way the transactions. Finally, PoW is the last preferred algorithm due to its speed. Indeed it takes on average 7 minutes to mine a block on Bitcoin blockchain.

- *Consumption Costs:*

Proof of Work is not sustainable in the long run due to the high electricity consumption costs. The entire Bitcoin network now consumes more energy than Austria or Chile.

Moreover, miners owning modern equipment find more accessible to find the correct nonce while other miners strive more due to their not suitable equipment. With a scale economy, this problem can only worsen. The less

computation power and power consumption required by PoA makes it faster and more efficient.
"PoW is currently very widespread, but its cryptography solving system isn't very environmentally friendly as it consumes a lot of energy. PoS requires less energy, but both are still too wasteful for IoT applications"[79] Is evident that both PoW and PoS are not adequate. Moreover, they have low compatibility with IoT devices due to the computing power these devices would need, while PoA can be easier implemented on IoT devices.

- *Adoption Easiness:*

Regarding adoption easiness some support PoA, others D-PoS. By comparing the consensus algorithms analysed in the research, a few problems regarding the adoption easiness appeared. For PoW the main hurdle would be the hardware and computing power needed to validate transactions across the network. For PoS, according to some experts, the main problem would be the incentive in minting blocks of transactions. Indeed, introducing a medical coin in the healthcare ecosystem will raise complexity, and eventually, it will intensify competitiveness. However, this is still a hot topic among experts. An example of a company building a blockchain solution based on D-PoS is Medicalchain. "Medicalchain is built using a dual blockchain structure. The first blockchain controls access to health records and is built using Hyperledger Fabric. The second blockchain is powered by an ERC20 token on Ethereum and underlies all the applications and services for our platform" (W.Paper) It is a private permissioned network. Medical tokens like MedTokens will be used to incentivise individuals like care providers to continue acting as a node and to maintain the network. Indeed Proof of Stake depends on the incentives offered. Moreover, it solves the problem of inequality between miners, and the 51% attack. Using a stake will make extremely difficult for an attacker to gain posses of 51% of the stakes to achieve a double spending attack.

- *Transaction Fees:*

Regarding exploiting transaction fees to maintain the network, is not yet clear which consensus algorithm is the best to apply. MedRec solution proposes PoW, in this network researchers receive aggregated medical data as a bounty, reward for mining transactions and adding them to the chain. However, the speed of PoW influences the scalability and, consequently, the adoption of this consensus algorithm. Regarding D-PoS and PoS, here the miners earn fees associated with the transactions contained in the block, these fees incentivise miners to maintain the blockchain. The last solution taken into account is to build a blockchain with PoA without any token or reward. It is a consensus algorithm built for private permissioned networks in which incentives are not necessary to run the blockchain since a central authority. A trusted party will take this responsibility.

## Answering the Research Questions

The main research question had been answered through the following three subquestions:

*(1)* ***Which are the essential properties, for a healthcare blockchain solution, that should be considered in a multicriteria evaluation of blockchain technology, like different networks type and consensus algorithms?***

A blockchain solution for the healthcare systems should provide scalability, interoperability, and efficient medical data management. These three attributes gain strength through a blockchain solution able to improve the properties listed in Table 5.5a and 5.5b. Such a solution would create a more patient-centered system and, consequently, enhance population health management, medical research, patient engagement and, healthcare quality as illustrated in Fig 5.1. These results have been obtained by comparing three factors. First, the healthcare system's major problems emerged from the literature review and their overall impact on healthcare system's interoperability, scalability, and medical data management, Table 5.1. Second, the impact of the proposed solutions analysed, so the benefits that a blockchain solution could bring to the healthcare system, Table 5.2. Third, blockchain experts' opinion collected with the scoping interviews listed in Table 4.1. These opinions helped the comparison of healthcare system's problems with blockchain's benefits and, helped the construction of Table 5.5a and 5.5b. Figure 5.2 depicts a summary of the research's results, the essential properties that need to be considered in a multicriteria evaluation of a blockchain solution are encircled by the red line.

*(2)* ***Should a blockchain solution for the healthcare system be implemented on a public or private, and permissioned or permissionless network? Which are the different benefits and limitations of these types of networks when applied to the healthcare system?***

Such a solution should be realised by creating a private permissioned blockchain on Ethereum or Hyperledger Fabric 1.0. Most of the experts interviewed have suggested these two platforms due to their properties, and due to their related healthcare projects like Hyperledger Healthcare Working Group (HLHC Working Group), and Healthureum. The main advantages of a private permissioned blockchain compared to the other types of network have been identified with experts interviews, and are listed below:

- Ethereum blockchain and Hyperledger support the use of Smart Contracts, Artificial Intelligence, Internet of Things, Dapp and Big Data. These features have a positive impact on two of the properties listed in Table 5.5b, 'Innovation Readiness' and 'Smart Contracts Adoption'. The lasts impact on a system's interoperability and scalability as shown in Fig 5.2.
- A private permissioned blockchain provides better 'Integration Readiness', and 'Authentication Control', two of the properties that enhance 'Health Data Management' in Table 5.5a. Besides, such a blockchain, implemented on platforms like Ethereum and Hyperledger, supports ad-hoc solutions for enterprises and businesses different components can be individually modified

without affecting any other part of the system that will be still capable of executing operations regarding health data management.

- It guarantees more 'Network Control' compared to public blockchains and permissionless networks in which anyone can participate and take part in the consensus algorithm. Network control, as explained in Table 5.5a, enhances interoperability by reducing frauds, abuses. This control can be better carried out with a private permissioned network in which different hospitals, insurance companies and government entities are the nodes in control of who can access the network and who can participate in the information validation.

*(3)* ***Which consensus mechanism fit best in such a blockchain solution in the healthcare system, Proof of Work, Proof of Stake, Delegated Proof of Stake, or Proof of Authority? Which are the different benefits and limitations of PoW, PoA, D-Pos and PoS when applied to the healthcare system?***

Experts' opinions, on which consensus algorithm fits the best for such a blockchain solution, diverge. On average, Proof of Authority and Delegated Proof of Stake are preferred due to the characteristics listed below:

- Higher network speed. Thousands of transactions per second
- Incredibly lower energy consumption cost to validate transactions and add them to the blockchain, compared to PoW.
- Higher adoption easiness when compared to PoW. This is due to the lower or non-existent competition, and to the less computational power needed, in terms of necessary hardware and software.
- Regarding transaction fees, with D-PoS and PoS algorithm there is the need for tokenisation to elect validators and delegates. Tokens and fees are needed to run and maintain the network. With PoA there is no need for tokenisation, nodes in control are elected through a different process.

All the four features mentioned above impact the 'Scalability' of a blockchain solution to healthcare system's problems, Table 5.5b.

To conclude, from the interviews was clear the absence of 'the most suitable algorithm'. Instead, every algorithm has different benefits and limitations. Based on these limitations, the results of the interviews revealed that both D-PoS and PoA fit for a blockchain solution in the healthcare since they allow scalability, interoperability, cost savings and efficient patient data management. The final choice depends on the desired degree of decentralisation. D-PoS suits better when there is a strong need for decentralisation and tokenisation, in a system characterised by low trust in actors. It resolves consensus problems in a fair and democratic way. PoA suits better in a system which allows a certain degree of power centralisation. It sacrifices centralisation in favour of network control and security.

Table 5.8 illustrates the aspects in which PoA, PoS, and D-PoS differ and how they have been ranked by the experts.

| | Network Control and Security | Decentralisation |
|---|---|---|
| 1° | Proof of Authority | Delegated Proof of Stake |
| 2° | Delegated Proof of Stake | Proof of Stake |
| 3° | Proof of Stake | Proof of Authority |

Table 5.8: Final comparison of PoA, D-PoS and PoS. Source: Author

(1) ***Which type of blockchain and consensus algorithm meets and fulfils the essential criteria for a blockchain solution to be applied to the healthcare system?***

- The type of blockchain that meets and that fulfils the most these essential criteria is a *Private and Permissioned Blockchain.*
- The consensus algorithm that meets and fulfils the most these essential criteria are *Proof of authority and Delegated Proof of Stake.*

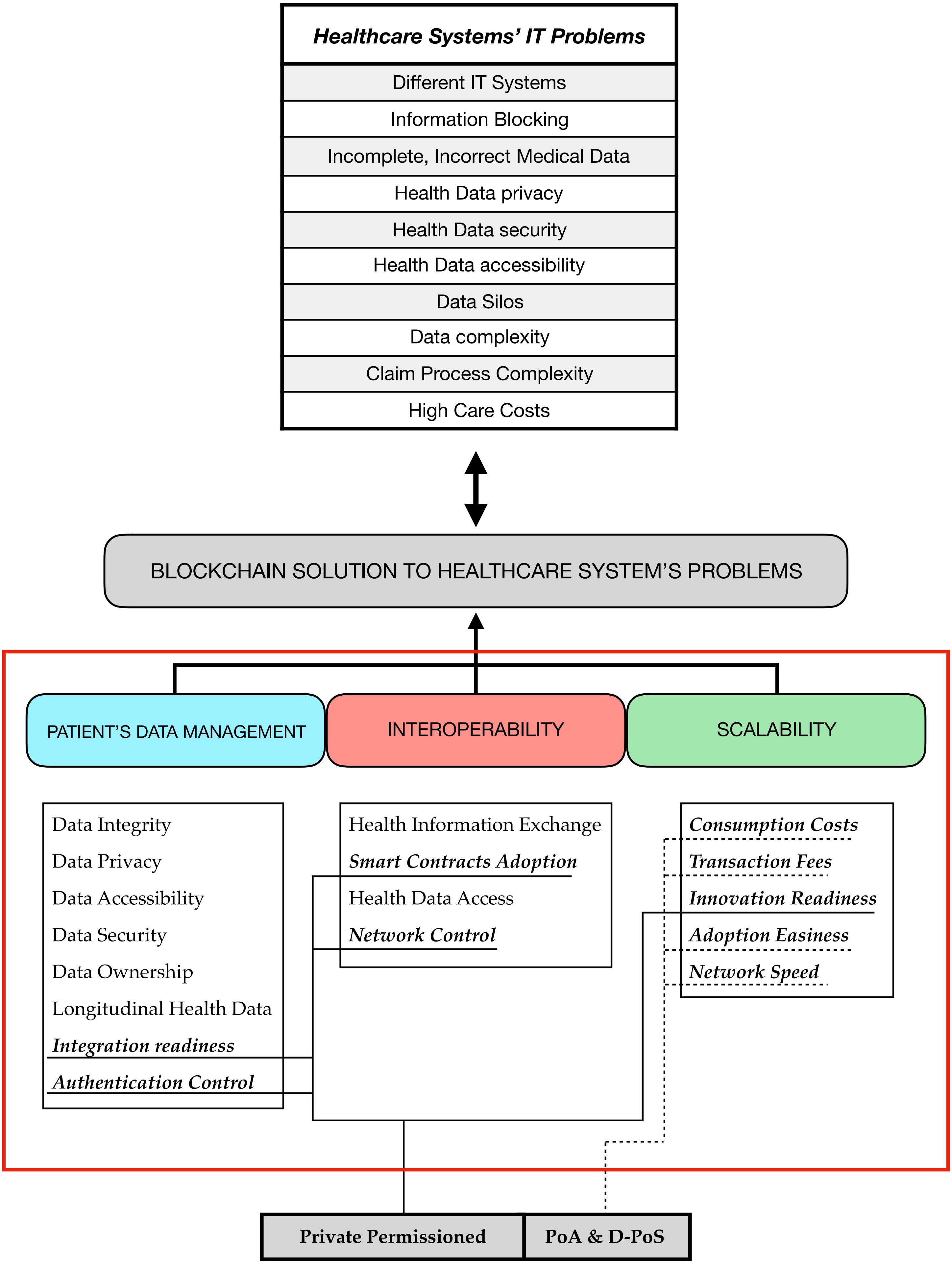



Figure 5.2: Research's results summary. Source: Author

Chapter 6

# Discussion and Conclusion

## Introduction

Chapter 6 recapitulates and elaborates on the finding laid out in 'Chapter Five'. First, in the 'Blockchain Solution' paragraph is described a basic infrastructure of a blockchain solution including the stakeholders involved, and the main hurdles. Second, in the 'Discussion' paragraph, the future steps to adopt a blockchain solution for the healthcare system are explained. Subsequently, reflections and limitations met during the research are presented to assess the quality of the final results. The 'Future Work' section aims to explain where the results found can lead further researchers, which could be the future steps and which questions will they raise. Finally, the 'Conclusion Chapter' recapitulates the entire research and the major findings.

## Blockchain Solution

The following paragraphs propose and describe a hypothetical blockchain solution based on insights and information collected interviewing experts.

### Solution Architecture

According to the experts interviewed, a private and permissioned blockchain network, that uses PoA or D-PoS as consensus mechanisms, meets and satisfies the essential criteria for an IT solution to be implemented in the healthcare system. Such a blockchain technology, when compared to other types of blockchains, provides superior Interoperability, Scalability, and Health Data Management.

Again according to the experts interviewed, such a solution should be implemented using Hyper-Ledger Fabric. "Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, IoT, supply chain, manufacturing and technology. Hyperledger's goal is to help organizations build industry-specific applications, platforms, and hardware using blockchain for better overall interoperability"[80].

Figure 6.1 and 6.2 depicts a basic infrastructure of this hypothetical solution, first to upload medical data and, second, to retrieve medical data. This blockchain solution will make use of three smart contracts. These contracts will automate the movements of patients' medical information across the health IT infrastructure, ensuring transparency, security and total control over the data. The three smart contracts are described below:

- Gate Smart Contract (GSC) with the duty of checking that the Identification and Endorsement Phase have been successfully completed. In case these two phases are both validated by health providers and patients, they will move the transaction to the Validation Phase. The aim of this contract is to automate the process of checking, grouping and prioritising medical transaction that will be later added to the blockchain.
- Patient-Provider Smart Contract (PPR). It saves the Patient-Health Provider relationships. These relationships include pointers to the local database where medical data have been saved, the stewardship and the access of the medical data. Pointers are always associated with access permissions, and this provides data security, confidentiality and a more transparent process in which the patient has now total control over his medical data.
- Summary Contract (SC). This smart contract lists all the PPR relationship of a patient, or a provider, to represent all the old and current engagements of the nodes participating in the network. The aim of this smart contracts is to keep track of every Patient-Provider relationship and to notify the users of any update in the PPR list.

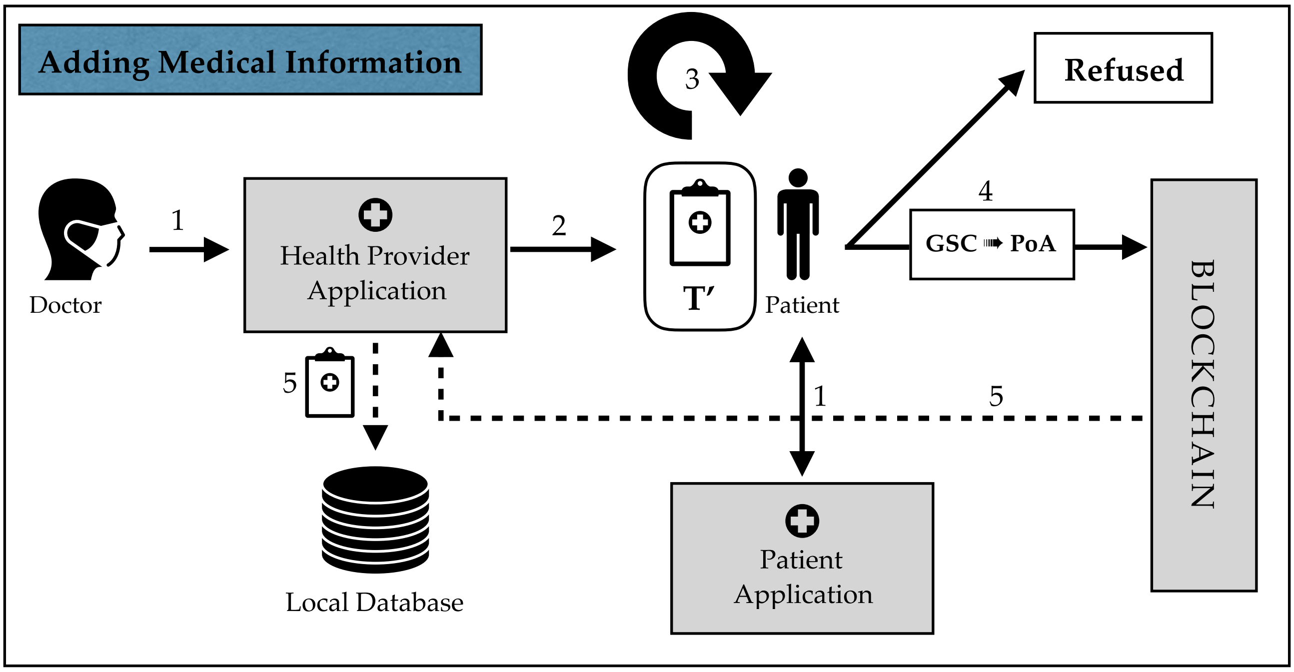



Figure 6.1: Blockchain Solution Infrastructure Data Upload. Source: Author

1. *Identification Phase.* The doctors and the patients enter their relative applications with their Private Keys to be identified by the system.
2. The doctor endorses and sends the medical document and the relative transaction to the patient. The relative transaction corresponds to a unique ID of the medical data. This ID will include, in the form of digits, information about the hospital, date, and care provided.
3. *Endorsement Phase.* The patient checks whether the data in the medical document sent during Phase 2, are correct or not. In case they are correct, the patient also endorses the transaction (T′). In case they are not correct, the transaction gets refused and sent back to the health provider by the patient.
4. *Validation Phase.* Endorsed transactions, from both doctors and patients, will go through the validation phase. In this phase, medical data will be hashed and added to the private blockchain with PoA. If this hash matches the hash of the medical data saved in the local database the medical data can be trusted. In this way, is possible to verify the authenticity of the off-chain medical data.

5. Once the transaction is added on the blockchain, the doctor will be notified in the health provider application and, the medical data will be saved off-chain on the local database.

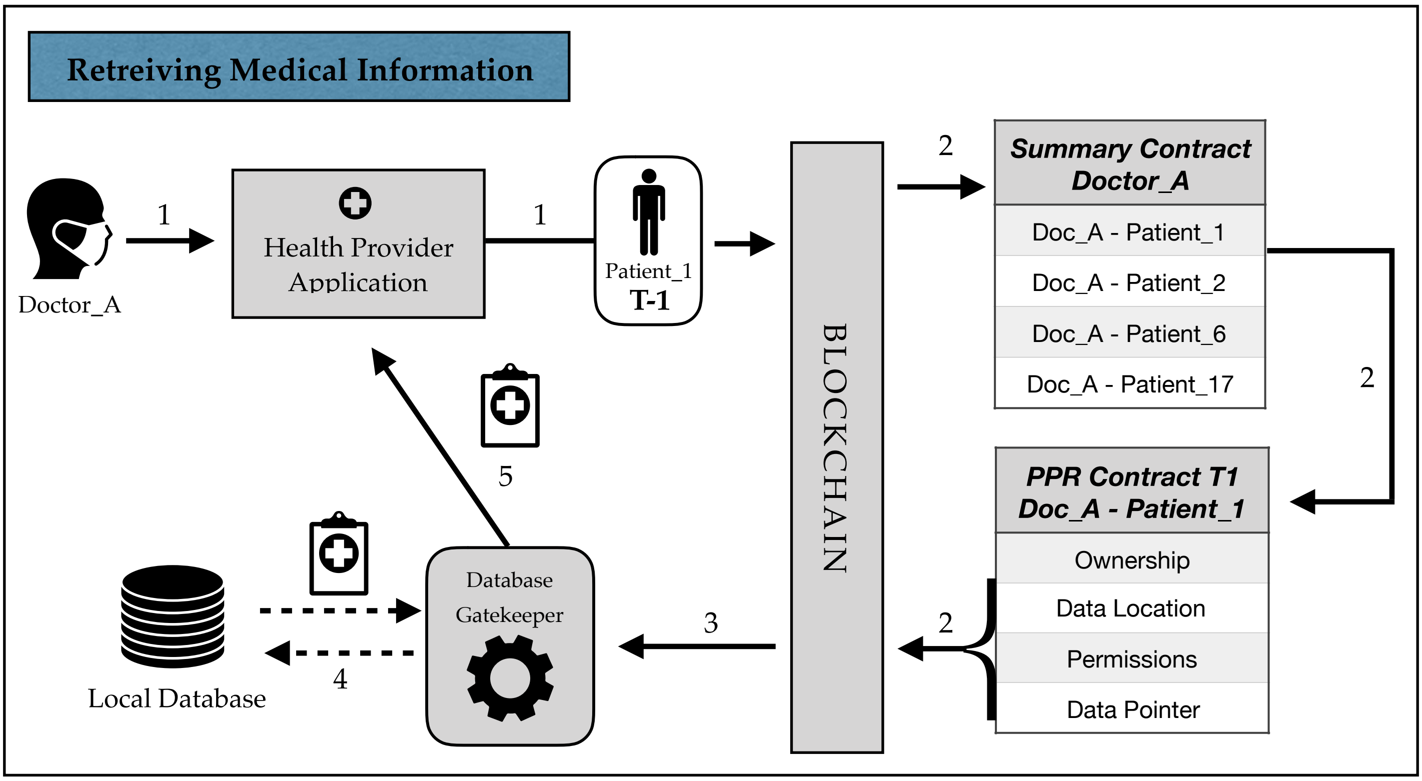



Figure 6.2: Blockchain Solution Infrastructure Data Retreiving. Source: Author

1. Identification Phase: Doctors enter the application with a Private Key and query the medical data T-1 of Patient_1. T-1 refers to one of the multiple transactions that Doctor_A had with Patient_1.
2. The Summary Smart Contract on the blockchain checks whether Doc_A has or not records with Patient_1. If so, the PPR contract investigates to which degree Doctor_A can access the patient's medical data.
3. After the two Smart Contracts verify whether Doctor_A can access Patient_1 or not, and to which degree Doc_A can access, view and modify patient_1 medical data, a request is sent to the Database Gatekeeper. This request uses the data pointer contained in the PPR contract which indicates in which local database medical data is stored and, through which gatekeeper they can be retrieved. The request contains Doctor_A digital signature and, information about the data that need to be retrieved.

4. Such a request, governed by the permissions stored by the PPR on the blockchain, is off-chain and gives access to local databases. The database Gatekeeper, by elaborating the request, collects the desired medical data from the local database.
5. Medical data are sent to Doctor_A's application interface, ready to be accessed and used. The patients will be then notified by the system if any new data is added to their medical record as explained in Figure 6.1.

## Solution's Stakeholders & Hurdles

The following paragraph takes into account who and how such a blockchain solution to the healthcare system affects. First, stakeholders are identified and defined. Second, the main hurdles to implementing such a solution are highlighted and associated with the stakeholders that are mostly involved. Stakeholders and hurdles have been identified assuming that the blockchain solution will be implemented on a national scale in a developed country.

- Patients. They include all the citizens of a country. This category is the amplest and, it contains health care providers, policymakers, researchers and industry representatives. They are directly affected by any change in how the national healthcare plan is operationalised and, they are the force driving healthcare system's changes. Understanding better patients' needs and creating a solution that fits these needs, is a necessary step to shift toward a more patient-centered healthcare system.

- Providers. There are multiple types of healthcare providers like physicians dentists, nurses, surgeons, paramedics, nutritionists, pharmacists and many more. They deploy the national health care plan by practically delivering care to patients across all the country. Providers offer care in public and private structures. These include hospitals, medical centres, clinics, practitioners offices, research centres, pharmacies. In this fragmented structure, patients' medical data are saved off-line in local databases. This fragmentation, the division between public and private health providers and different IT systems, result in difficult interoperability among health providers and in a lower quality of care.

- Policymakers. These can also be defined as ministries of health; they are official government offices which operate with the resources allocated to the healthcare system. Their duty is to provide a health plan for the entire population, and health economic policies based on the data they collect from patients and providers. They are responsible for who receives care services and, how these are deployed as well as checking the quality, the costs, and the innovation of these services to plan population health management ahead.

- Researchers. They operate close to medical institutions and structures using aggregated medical data to conduct studies to investigate human diseases. Higher interoperability between care providers, and better medical data management will positively affect the outcomes of their research.

- Industry Representatives. This category of stakeholders includes salespeople employed by companies that produce medical devices like health-IT vendors. These corporations play an essential role in the healthcare system's quality and, they have to respect the regulations set by governments and policymakers. Nevertheless, due to their private essence, they always aim to maximise their profit, paying less and less attention to the real needs of patients and providers.

Each group of stakeholders has different duties in relation to others. Providers and Industry Representative need to align with the policy set by the policymakers. Policymakers create policies based on the data they collect from researchers and care providers. Figure 6.3 roughly depicts the major connections between healthcare stakeholders.

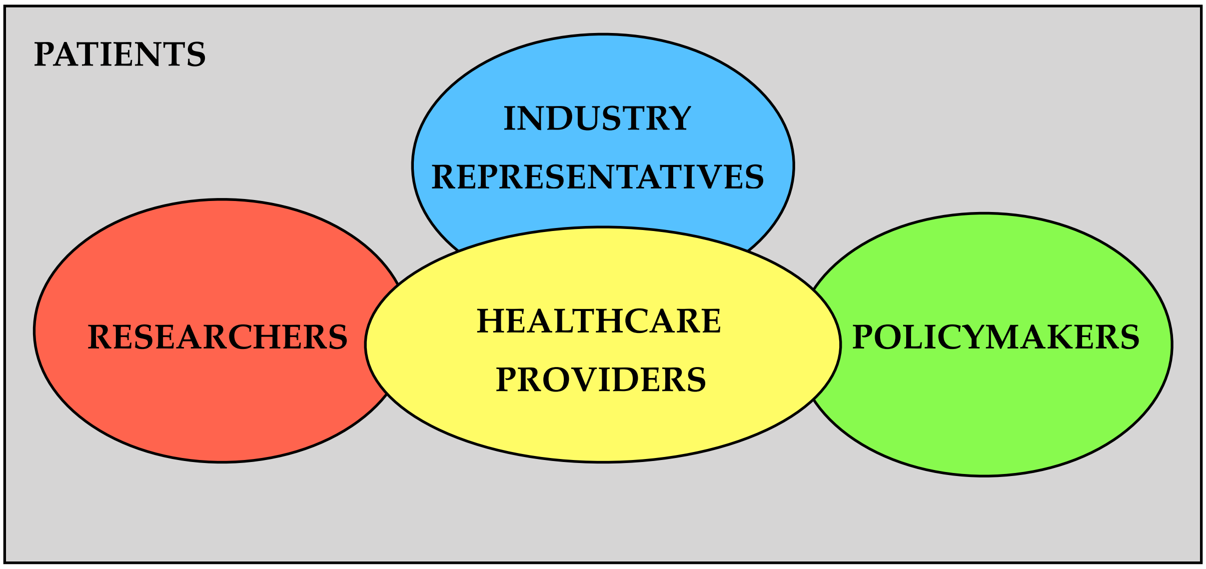



Figure 6.3: Major Stakeholders Healthcare System. Source: Author

The major hurdles that have been identified are listed below. Is necessary to overcome these barriers before such a solution could be adopted and, could effectively provide the benefits mentioned in Chapter 5 of the research.

- Financial challenges. These include, for example, set-up, adoption and maintenance costs. More specifically, costs include personnel training and assistance, the formation and continuation of national consortiums, IT solution deployment and upgrades, databases renovation, new hardwares, the coding of the smart contracts with Hyperledger Fabric platform and many more.
- Adoption time. The time required to use such a blockchain application efficiently may discourage its adoption for healthcare providers and patients. Even though a blockchain solution can be built upon the existing IT infrastructure and, can use the existing local databases, the time required for an entire nation to implement and to adapt to such a change will be one of the major hurdles to surpass.

- Consortium creation. Both PoA and D-PoS will need the creation of multiple consortiums with different rights and authorities. These consortiums will have the responsibility of validating medical transactions and adding them to the blockchain. They will be in charge of the stewardship of the private blockchain network by controlling the access and the rights of all the nodes. Different consortiums will need to create and enforce data regulations, medical data standards and guidelines for health providers, patients and, industry representatives. As mentioned before, different stakeholders have different goals and purposes. Aligning all of them and, maintaining a reliable collaboration is an important barrier that needs to be passed.
- Social barriers. These barriers regard the problems that can arise within medical teams and within a group of people working in the healthcare environment. These problems, especially in such a high-stress environment, affect the correct implementation and use of a new IT solution like the one proposed in the research. Examples are the shortage and resistance of internal resources needed to lead the change initiative, scepticisms and hesitancy to invest time, energies, and money among health providers and stakeholders.

# Discussion

## Future Steps to adopt a Blockchain Solution

The research discussed what blockchain technology is and how this disruptive technology could enhance the healthcare system. However, there are some adoption steps that should be taken into consideration before blockchain technology could create a new backbone for the healthcare system. Figure 6.3 depicts the maturity phases that a blockchain solution for the healthcare system should have to go through. At the time of the research, considering the online literature reviewed, blockchain technology is positioned in 'Phase 2'. This phase is characterised by the Proof of Concept (PoC) "it is a demonstration, the purpose of which is to verify that certain concepts or theories have the potential for real-world application. PoC is, therefore, a prototype that is designed to determine feasibility"[81]. Multiple companies and start-up are building prototypes of blockchain solutions. Examples are MedicalChain, IRYO, Patientory, Meidchain, Kinect, Humanscape, Philipps, Hyperledger Healthcare Working Group and many more. All these proposed solutions do not clearly state whether the blockchain should be implemented with a private, public, permissiones or permissionless network and with which consensus algorithm. Phase three, broader adoption. Moving to the third phase requires to scale these solutions for broader adoption. The adoption of a nationwide blockchain solution would require a major cultural shift in how medical documents are handled by doctors, clinicians and patients. Such a solution needs to be adopted on a large scale but, bringing together the numerous healthcare providers will be highly demanding. Resistances can result from private and for-profit healthcare providers that are not willing to adopt an interoperable solution. Moreover, changing such practised medical behaviours across all the healthcare industry will require a great investment in terms of money and time by the local governments. Others obstacles that need to be passed include legal and regulatory constraints and the lack of a common data standard. Surmounting these obstacles requires strict coordination among multiple care providers, collaboration is essential, every refusal in the adoption of blockchain will reduce the utility of the entire system.

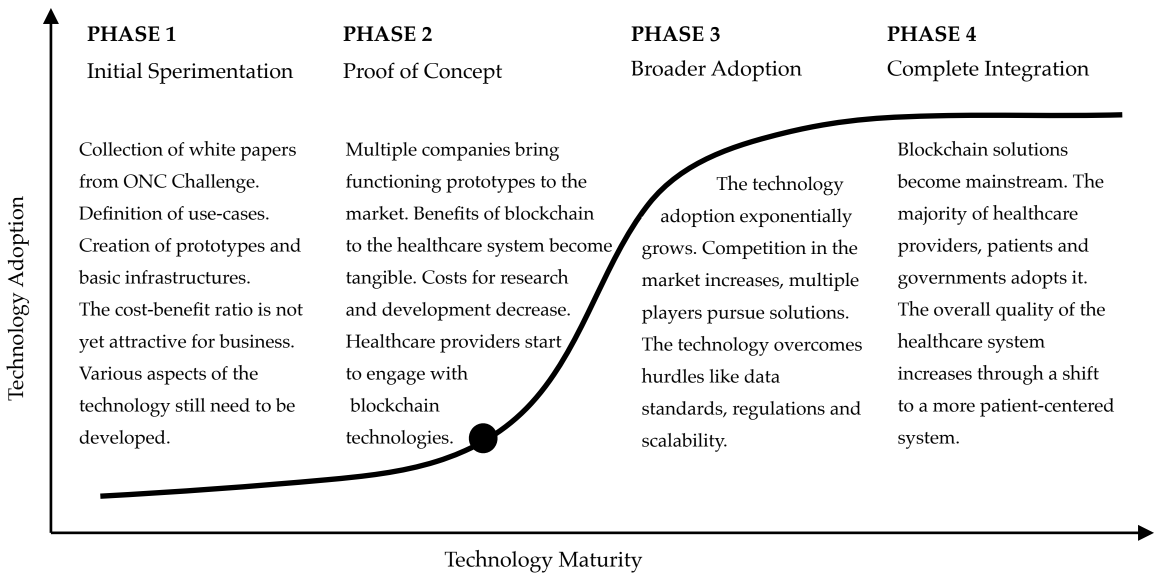



Figure 6.3 Blockchain technology adoption and maturity chart. Image Source: Author

## Limitations

The first problem that impacted the quality of the research was timing. Since blockchain technology is in continuous development, the constant discovery of new literature to review and the timeboxed nature of the research lowered the overall quality of the results. The literature reviewed in the research collects papers that are not older than 2016 apart from Bitcoin: A peer-to-peer electronic cash system. The last papers reviewed are dated September 2018.

The second major problem has been the availability of blockchain experts, which, besides being limited in numbers due to the technology lifetime and complexity, have been difficult to contact and to interview. Furthermore, the chances of interviewing experts face to face with substantial in-depth knowledge and experience about blockchain and the healthcare system were even more limited. Even though this problem affected the collection of qualitative data, the information collected with the interviews were enough to reach data saturation.

A third issue regards the quality of the data collected. The research tried to collect unbiased insights and, to provide an objective flow of reasoning as much as possible. However, due to the exploratory nature of the research, the subjectivity of the experts interviewed influenced data collection. Indeed, experts interpretations and insights are highly dependent on their experience, background, and personal understanding of different features of blockchain technology. The quality of the data collected affects the degree to which results from a similar research mirror this research's results. Interviewing different experts may bring to different results, nevertheless, the research and the interviews aimed to minimise this gap and difference.

Moreover, other problems arose from adapting the findings to the tables and frameworks used in the study. Even though these tables were created with the help of experts, on more than one occasion, it was difficult to asses whether findings would allineate with a particular blockchain aspect or not. This, was in part due to the lack of an explicit agreement on the innovative features of blockchain, since it is a combination of already established technologies.

### Future Work

Even though blockchain solutions are rapidly overcoming problems and maturing, many aspects need to develop further. Blockchain is not fully mature; prototypes have to be experimented to address technical, organisational and economic challenges which research has not adequately addressed yet. Future research on the topic will be influenced by the constant technology evolution and, by the new solutions proposed across the globe. New forms of consensus algorithm, new experts, knowledge and new companies will arise.

In future studies, will be needed to understand to which extent decentralisation can be sacrificed to enhance health data management and transactions speed using Proof of Authority algorithm. Besides this, is needed research about the costs and time of implementing and using such a solution nationwide for specific nations.

To shape a future blockchain solution for the healthcare system is necessary to establish a blockchain framework to coordinate the care provider and receivers, and to establish rules to possibly constitute a consortium to administer these blockchains. In defining these new frameworks with guiding rules, verification and control methods, the guidance of a new professional figure capable of bringing together and finding a synthesis of technologies and regulations is becoming necessary.

## Summary

In the past few years, a new technology caught the interest of societies: the blockchain. This technology has been around since 2008 with the invention of Bitcoin. Societies began to explore different use for this technology, included its applicability to the healthcare system since health institutions suffer from the chronic inability to collect and share data between different platforms and institutions. For these reasons, many blockchain solutions have been proposed to solve the aforementioned problems by governments, health providers and private companies.

The research collected and analysed all these solutions to gain an overview of the existing knowledge, and on the issues that have been found in the literature review. Online literature revealed a knowledge gap regarding which type of network and consensus algorithm should be adopted in a blockchain solution for the healthcare system. By focusing on this issue, research questions have been carried out, and the focus of the research had been defined. Through multiple interviews with blockchain experts and a methodological analysis of online literature, healthcare system's problems and blockchain benefits have been systematically listed, defined and associated in Chapter 5. The final section of Chapter 5 uses the insights gained during the study to answer the research questions. The findings suggest Interoperability, Scalability and, Health Data Management as the three essential properties that a blockchain solution should provide in order to solve healthcare system's problems. Such a solution, according to the experts interviewed should deploy a Private and Permissioned Network in which the consensus is reached through PoA or D-PoS depending on the desired centralisation level.

Interoperable IT systems promote collaboration. Better collaboration between data providers means, in essence, a greater likelihood of accurate diagnosis, a higher likelihood of opting for effective treatments and, more generally, an increase in the overall capacity of healthcare systems to provide excellent care. Hospitals, payers and other healthcare facilities will share access to their networks without compromising security and integrity.

A scalable system will increase the adoption of such a blockchain solution in the long term. Blockchain potential, like the internet, grows with its adoption; consequently, improvements to the healthcare system will increase with the number of participants in the blockchain network. Scalability will enlarge blockchain's potential use and accommodate future growth to provide better population health management.

Besides interoperability and scalability, health data ownership results is a more patient centred care system in which people mature a broader health responsibility. Ownership associated with control over personal medical data reduces opportunistic practices like information blocking and, lowers the number of medical errors committed every day. The long-term consequences of ownership and control over medical data include an enhancement in medical research. Aggregated medical data will empower researchers and governments to identify care gaps in the population and, to develop new treatments and medicines.

## Conclusion

The future path that blockchain technology will take in the healthcare system remains to be seen. Besides the adoption of a blockchain solution, such improvements will be possible only through a real shift in the behaviour of patients, doctors, and care providers.

To conclude, this research does not promote the adoption of a blockchain solution and, at the same time does not want to discourage it. This research encourages the comprehension of the benefits that different blockchain technologies can bring to the healthcare system.

# *Glossary of Terms and Abbreviations*

EHR: Electronic Health Record

EMR: Electronic Medical Record

PoW: Proof of Work

PoA: Proof of Authority

PoS: Proof of Stake

D-PoS: Delegated Proof of Stake

GPT: General Purpose Technology

DApp: Decentralised applications

PKI: Pulic Key Infrastructure

ONC: Office National Coordinator

C.A.: Certicifate authority

BT: blockchain Type (of network)

CA: Consensus Algorithm

SC: Summary Contract

PPR: Patient Provider Smart Contract

GSC: Gate Smart Contract

# *References*

[1] Forbes: Blockchain In Publishing: Innovation Or Disruption? URL: https://www.forbes.com/sites/forbesproductgroup/2018/05/03/blockchain-in-publishing-innovation-or-disruption/#9d3fbf154569

[2] DeSalvo, T. O. (2015). Connecting Health and Care for the Nation. The Office of the Health Coordinator. URL: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[3] What are emerging technologies? definition and meaning. (n.d.). Retrieved September 2, 2018, from http://www.businessdictionary.com/definition/emerging-technologies.html

[4] Linden, A., & Fenn, J. (2003). Understanding Gartner's hype cycles. *Strategic Analysis Report Nº R-20-1971. Gartner, Inc*. URL: http://www.bus.umich.edu/KresgePublic/Journals/Gartner/research/115200/115274/115274.pdf

[5] https://www.theiet.org/sectors/design-production/resources/horizontal-innovation.cfm?utm_source=redirect-url&utm_medium=website&utm_campaign=innovationpage

[6] Health Care Innovation: Harnessing New Technologies To Benefit Patients, 2nd April 2018 Sanjay Poonen. URL: https://www.forbes.com/sites/forbestechcouncil/2018/04/02/health-care-innovation-harnessing-new-technologies-to-benefit-patients/#56e945b25a88

[7] Van Limburg, M., van Gemert-Pijnen, J. E., Nijland, N., Ossebaard, H. C., Hendrix, R. M., & Seydel, E. R. (2011). Why business modeling is crucial in the development of eHealth technologies. *Journal of medical Internet research*, *13*(4). DOI: 10.2196/jmir.1674

[8] Spil, A. A., & Kijl, B. (2009). E-health Business Models: From pilot project to successful deployment. *IBIMA business review*, *1*, 55-66

[9] Don & Alex Tapscott, authors Blockchain Revolution (2016) URL: https://blockgeeks.com/guides/what-is-blockchain-technology/

[10] Meijer, D. (2017). Consequences of the implementation of blockchain technology (SEPAM Master Thesis), Delft University of Technology, Delft. pp. 6-7

[11] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, *29*(2), 213-38. URL: https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213

[12] Buterin, V. (2017). The meaning of decentralization. Medium. Online at https://medium. com/@ VitalikButerin/themeaning-of-decentralization-a0c92b76a274.

[13] Blockchain Advantage and Disadvantages. Warren Fauvel, Medium 11th August 2017. https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0

[14] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf

[15] Block Header (Cryptocurrency), Investopedia. URL: https://www.investopedia.com/terms/b/block-header-cryptocurrency.asp

[16] How many transactions are included in a block chain? Quora. https://www.quora.com/How-many-transactions-are-included-in-a-block-chain

[17] BitFuri Group, 2015; Buterin, 2014; Walport, 2016 URL: https://bitfury.com/content/downloads/public-vs-private-pt2-1.pdf

[18] What is Cryptoeconomics? The Ultimate Beginners Guide. URL: https://blockgeeks.com/guides/what-is-cryptoeconomics/

[19] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf

[20] Target Hash, Investopedia. URL: https://www.investopedia.com/terms/t/target-hash.asp

[21] Target Hash, Investopedia. URL: https://www.investopedia.com/terms/t/target-hash.asp

[22] Bitcoin's Growing Energy Problem, de Vries, Alex Joule , Volume 2 , Issue 5 , 801 - 805. DOI: https://doi.org/10.1016/j.joule.2018.04.016

[23] Delegated Proof-of-Stake Consensus. URL: https://bitshares.org/technology/delegated-proof-of-stake-consensus/

[24] Proof of Authority: consensus model with Identity at Stake. URL: https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256

[25] Proof of Authority: consensus model with Identity at Stake. URL: https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256

[26] Blockchain: Opportunities for Health Care August 2016, Deloitte. URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf

[27] Iakovidis, I. (1998). Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe. *International journal of medical informatics*, *52*(1-3), 105-115. DOI: https://doi.org/10.1016/S1386-5056(98)00129-4

[28] Karen B. DeSalvo. Connecting Health and Care for the Nation. A Shared Nationwide Interoperability Roadmap. URL: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[29] Topol, L. J. (September 2015). Unpatients, Why patients should own their medical data. *Nature Biotechnology*, 921-924. DOI: 10.1038/nbt.3340

[30] Topol, L. J. (September 2015). Unpatients, Why patients should own their medical data. *Nature Biotechnology*, 921-924. DOI: 10.1038/nbt.3340

[31] Topol, L. J. (September 2015). Unpatients, Why patients should own their medical data. *Nature Biotechnology*, 921-924. DOI: 10.1038/nbt.3340

[32] ADLER-MILSTEIN, J., & PFEIFER, E. (2017). Information Blocking: Is It Occurring and What Policy Strategies Can Address It? *The Milbank Quarterly*, *95*(1), 117–135. http://doi.org/10.1111/1468-0009.12247

[33] Karen B. DeSalvo. Connecting Health and Care for the Nation. A Shared Nationwide Interoperability Roadmap. URL: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[34] Report on Health Information Blocking. April 2015. The Office of the National Coordinator for Health Information Technology (ONC) Department of Health and Human Services. URL: https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf

[35] Karen B. DeSalvo. Connecting Health and Care for the Nation. A Shared Nationwide Interoperability Roadmap. URL: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[36] Karen B. DeSalvo. Connecting Health and Care for the Nation. A Shared Nationwide Interoperability Roadmap. URL: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[37] Karen B. DeSalvo. Connecting Health and Care for the Nation. A Shared Nationwide Interoperability Roadmap. URL: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[38] Karen B. DeSalvo. Connecting Health and Care for the Nation. A Shared Nationwide Interoperability Roadmap. URL: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[39] Shrier, A. A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J. & Hardjono, T. (2016). Blockchain and Health IT: Algorithms, Privacy, and Data. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.
URL: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf

[40] Shrier, A. A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J. & Hardjono, T. (2016). Blockchain and Health IT: Algorithms, Privacy, and Data. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.
URL: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf

[41] Shrier, A. A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J. & Hardjono, T. (2016). Blockchain and Health IT: Algorithms, Privacy, and Data. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.
URL: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf

[42] Shrier, A. A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J. & Hardjono, T. (2016). Blockchain and Health IT: Algorithms, Privacy, and Data. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.
URL: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf

[43] Shrier, A. A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J. & Hardjono, T. (2016). Blockchain and Health IT: Algorithms, Privacy, and Data. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.
URL: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf

[44] Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A., & Accenture, L. L. P. (2016). Blockchain: Securing a New Health Interoperability Experience. URL: https://www.healthit.gov/sites/default/files/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf

[45] Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A., & Accenture, L. L. P. (2016). Blockchain: Securing a New Health Interoperability Experience. URL: https://www.healthit.gov/sites/default/files/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf

[46] Culver, K. (2016). *"Blockchain Technologies: A whitepaper discussing how the claims process can be improved".* In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST. URL: https://www.healthit.gov/sites/default/files/3-47-whitepaperblockchainforclaims_v10.pdf

[47] Institute of Medicine (US) Roundtable on Evidence-Based Medicine; Yong PL, Saunders RS, Olsen LA, editors. The Healthcare Imperative: Lowering Costs and Improving Outcomes: Workshop Series Summary. Washington (DC): National Academies Press (US); 2010. 4, Excess Administrative Costs. Available from: https://www.ncbi.nlm.nih.gov/books/NBK53942/

[48] Culver, K. (2016). *"Blockchain Technologies: A whitepaper discussing how the claims process can be improved".* In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST. URL: https://www.healthit.gov/sites/default/files/3-47-whitepaperblockchainforclaims_v10.pdf

[49] Blockchain: Opportunities for Health Care by RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai. URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf

[50] Blockchain: Opportunities for Health Care by RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai. URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf

[51] Blockchain: The Chain of Trust and its Potential to Transform Healthcare – IBM. URL: https://www.healthit.gov/sites/default/files/8-31-blockchain-ibm_ideation-challenge_aug8.pdf

[52] Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare* (Vol. 1, pp. 1-10). URL: http://www.colleaga.org/sites/default/files/12-55-blockchain-based-approach-final.pdf

[53] Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare* (Vol. 1, pp. 1-10). URL: http://www.colleaga.org/sites/default/files/12-55-blockchain-based-approach-final.pdf

[54] Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare* (Vol. 1, pp. 1-10). URL: http://www.colleaga.org/sites/default/files/12-55-blockchain-based-approach-final.pdf

[55] Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare* (Vol. 1, pp. 1-10). URL: http://www.colleaga.org/sites/default/files/12-55-blockchain-based-approach-final.pdf

[56] Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare* (Vol. 1, pp. 1-10). URL: http://www.colleaga.org/sites/default/files/12-55-blockchain-based-approach-final.pdf

[57] Keyless Signature Infrastructure. Guardtime. URL: https://www.guardtime-federal.com/ksi/

[58] Keyless Signature Infrastructure. Guardtime. URL: https://www.guardtime-federal.com/ksi/

[59] Keyless Signature Infrastructure. Guardtime. URL: https://www.guardtime-federal.com/ksi/

[60] Keyless Signature Infrastructure. Guardtime. URL: https://www.guardtime-federal.com/ksi/

[61] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13). URL: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[62] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13). URL: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[63] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13). URL: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[64] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13). URL: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[65] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13). URL: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[66] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13). URL: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[67] Karen B. DeSalvo. Connecting Health and Care for the Nation. A Shared Nationwide Interoperability Roadmap. URL: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[68] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13). URL: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[69] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13). URL: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[70] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13). URL: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[71] Saunders, M., Lewis, P. & Thornhill, A. (2012) “Research Methods for Business Students” 6th edition, Pearson Education Limited

[72] Myers, M.D. (2008) “Qualitative Research in Business & Management” SAGE Publications

[73] Neuman, W. L. (2003). Social Research Methods: Qualitative and Quantitative Approaches, London: Allyn & Bacon.

[74] Brown, J. D. (1996). *Testing in language programs.* Upper Saddle River, NJ: Prentice Hall Regents.

[75] Saunders,M.,Lewis,P.,andThornhill,A.*ResearchMethodsforBusinessStudents*. Always learning. Financial Times Prentice Hall, 2009. ISBN 9780273716860.

[76] ‘Research Methods for Business Students’ Mark Saunders Philip Lewis, Adrian Thornhill 7th edition

[77] Ethereum White Paper “A next generation smart contract & decentralized application platform” By Vitalik Buterin

[78] Ksiazkiewicz, T. (2018, May 16). How Will Blockchain Affect PKI? Retrieved August 20, 2018, from https://www.cyberarmed.com/how-will-blockchain-affect-pki/

[79] hWhat is Proof-of-Assignment (PoA). (2018, August 17). Retrieved September 2, 2018, from https://captainaltcoin.com/proof-of-assignment-poa/

[80] Hyperledger – Open Source Blockchain Technologies. (n.d.). Retrieved September 20, 2018, from https://www.hyperledger.org/

[81] What is a Proof of Concept (POC)? - Definition from Techopedia. (n.d.). Retrieved October 8, 2018, from https://www.techopedia.com/definition/4066/proof-of-concept-poc