Bachelor thesis
Computing Science

Radboud University

Evaluating the practicality of using blockchain technology in different use cases in the healthcare sector

Author:
Mischa van Reede
s 4557816

First supervisor/assessor:
dr. ir. Erik Poll
erikpoll@cs.ru.nl

Second superviso/assessorr:
drs. ing. Tommy Koens
tkoens@cs.ru.nl

June 24, 2020

Abstract

In the past decade blockchain technology went from a seemingly unknown technology to being a technology praised by many companies and start-ups that are now eager to use it. These companies and start-ups often claim that the need for using blockchain technology in their use-case is necessary without much substantiation, or that the use of other types of data-storage techonologies do not offer the same benefits. Decision schemes have been proposed in the academic literature that determine whether or not the use of blockchain technology is justified or if non-blockchain-based solutions are preferred. This thesis will use such a decision scheme and apply this to two use cases that make use of blockchain technology in the healthcare sector. The first use case that is evaluated, is the Estonian e-Health initiative. The Estonian e-Health initiative uses a blockchain-based Keyless Signature Infrastructure to ensure the integrity of the medical data of Estonian citizens. The second use case that is evaluated is the EmrShare framework. EmrShare is a blockchain-based approach that facilitates cross-organisation sharing of electronic medical records. By evaluating these use cases we determine whether or not these projects can benefit from blockchain technology or if an alternative data storage technology offers a more sensible solution.

Contents

Chapter 1

Introduction

In 2008 Satoshi Nakamoto introduced a Peer-to-peer electronic cash system called Bitcoin [44]. Bitcoin is a decentralised digital currency, which means it eliminates the need for a central authority in charge of verifying transactions. A decentralised digital currency, also known as a cryptocurrency, relies upon a technology called blockchain technology to facilitate peer-to-peer transactions. Although the general thought is that blockchain technology was birthed with the introduction of Bitcoin, a paper from 1991 called "How to Time-Stamp a Digital Document" [50] laid the groundwork by proposing a way to time-stamp digital documents in such a way that the time-stamps could not be altered. However, the launch of Bitcoin was the first real-world application of blockchain technology.

Blockchain technology offers a way to store information in a decentralised manner. A blockchain is a chain of blocks which contain information and are cryptographically linked together. The blocks in the Bitcoin blockchain contain information about transactions, making the entire Bitcoin blockchain a ledger of sorts. In the case of the proposed blockchain solution in the paper "How to Time-Stamp a Digital Document" [50] the blocks would contain digital time-stamps connected to information of digital documents.

There is no set way that dictates which information can be stored in a blockchain. Many companies and startups have ambitious goals of applying this technology to solve societal problems or to re-design current solutions. The reason for using blockchain technology in many use cases is often not necessarily based on a technical need for this technology, but on economic incentives, philosophical beliefs, and networking effects [36].

Consulting agencies and the scientific community have made efforts to propose decision schemes that determine if a blockchain based solution is justified for a particular project. A critical analysis of 30 existing schemes by Koens & Poll [35] has shown that these schemes lead to contradicting results or are biased towards the use of blockchain technology as they do not consider alternatives. Koens & Poll propose a new improved scheme, which

is unbiased to the use of blockchain technology as it considers alternatives, which they argue is more useful in practice.

This research will use the decision scheme proposed by Koens & Poll to evaluate existing blockchain-based initiatives within the healthcare sector. In particular, we will evaluate the following main research question:

> Is the use of blockchain technology for specific use cases in the healthcare sector justified?

In order to answer the main research questions we look at the following sub-questions:

- Which blockchain-based use cases from the healthcare sector are we going to evaluate?
- What kind of service or solution do the use cases offer?
- To what extent do the use cases use blockchain technology?
- What is the result of the evaluation against the decision scheme of Koens & Poll for those specific cases?

The first use case that we will evaluate, is the Estonian e-Health initiative. The Estonian e-Health initiative uses a blockchain-based Keyless Signature Infrastructure to ensure the integrity of the medical data of Estonian citizens. The second use case that we will evaluate is the EmrShare framework. The EmrShare framework is a blockchain-based approach that facilitates cross-organisation sharing of electronic medical records. By evaluating these use cases we determine whether or not these projects can benefit from blockchain technology or if an alternative data storage technology offers a more sensible solution. Applying the decision scheme to these use cases result in a scientific argument whether or not the usage of blockchain technology is justified or if using an alternative data storage technology is a more sensible approach in those use cases.

Personal Motivation

The motivation for writing this thesis mainly stems from a personal interest in blockchain technology. During my study of Computer Science at the Radboud university, I have realised that the information technology (IT) industry is growing faster than ever. The developments and growth of blockchain technology, being a relatively new area and field of study in IT, is no exception. Many have made the argument that blockchain technology is a revolutionary and disruptive technology [34, 51, 37, 41].

With the introduction of a supposedly revolutionary technology such as blockchain, it is easy to see why many projects are eager to implement it.

The rising popularity of Bitcoin and the subsequent rise of its monetary value has also attracted investors willing to invest in new blockchain-based initiatives hoping to make a good return on investment.

These developments have lead to an industry wide interest in the technology, which also raises the question of the reasons and justification behind the adoption of blockchain technology in many use cases. This research hopes to create an understanding of when the use of blockchain technology is justified.

Readers guide

This thesis is structured in the following manner. Chapter 2 contains preliminary information about blockchain technology (2.1) and the decision scheme used in this research (2.2). In chapter 3 a selection of healthcare use cases is made. This is done by stating the criterion for selecting a use case (3.1), providing a selection of use cases (3.2) and providing an overview of the selected use cases (3.3). In chapter 4 two of the selected use cases are evaluated, the remaining use cases were not evaluated due to fact that the gathering of information on the first use case took longer than expected. The necessary information for the evaluation is given in the corresponding sections in which the use cases are being evaluated (4.1 & 4.2). Chapter 5 touches on related works of literature and chapter 6 mentions some opportunities for future research. In chapter 7 we present the conclusion of this research.

Chapter 2

Preliminaries

This chapter will contain the necessary background information that is needed to understand this thesis. Section 2.1 will explain the concept of blockchain technology, as well as certain properties of a blockchain that are relevant for the evaluation of use cases in chapter 4. In section 2.2 we will look at a decision scheme that determines which database storage technology is appropriate for a given use case. This will allow us to evaluate the use of blockchain technology in several use cases that are presented in chapter 3.

2.1 Blockchain Technology

Blockchain is the technology in which a blockchain is used to store data. Even though a novel version of this technology had been proposed in 1991 by Scott et al. [50], the introduction of Bitcoin [44] in 2008 accelerated the public interest in this technology. Since then companies and scholars have tried to leverage the properties of a blockchain to solve particular use cases.

Numerous studies, such as [29, 57, 58, 45, 49], have provided in depth explanations of the concept of blockchain technology. In this section we'll give a short overview of the main concepts of this technology relevant for this research.

We notice that the terminology and definitions surrounding blockchain technology is not used consistently between different sources. In this research we make an effort to follow the terminology as defined and used by Koens & Poll [35], for the simple reason that this work attempts to apply the decision scheme proposed in that article.

2.1.1 Blockchain

In essence, a blockchain can be thought of as a distributed database of transactions, records or digital events bundled into so-called blocks linked

together creating a chain of data [29]. This link is usually created by including a hash value from the previous block in the newly created block(s), as shown in figure 2.1. However, other blockchain schemes exist in which the link between blocks is created as a result of creating a Merkle tree [20] in which (new) blocks are added as leaf nodes to the tree [23]. Note that in this way, not the data is stored on the blockchain, but a hash value of the block contents.

In a traditional blockchain (example figure 2.1) each block, with the exception of the genesis block, has a reference towards their parent block. Because of the decentralised nature of blockchain, the network has to come to an agreement how and which new blocks are added to the blockchain. How this is done is dictated by a consensus mechanism, examples of consensus mechanisms are: Proof of Work, Proof of Stake, Proof of Authority, Practical byzantine fault tolerance, Delegated proof of stake, Ripple or Tendermint [57, 49]. By creating a linked structure of blocks and having a sound consensus mechanism in place to add new blocks, the network builds trust in the integrity of the data stored on the blockchain.

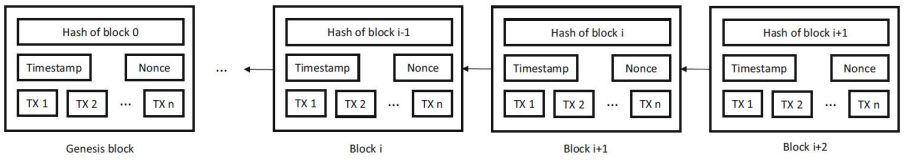

Figure 2.1: A basic example of a blockchain. [45]

2.1.2 Permissioned vs. Permissionless Blockchain

A difference can be made between permissioned and permissionless blockchains. The *permissioned* and *permissionless* keywords refer to the type of validators in the network (i.e. the users or nodes that are able to write to the blockchain). Permissionless blockchains are blockchains in which everyone can propose a new state of the ledger. This can be seen in, for example, Bitcoin where everyone can run the proof of work consensus algorithm to propose a new state of the Bitcoin blockchain [44, 29]. Another example of a permissionless blockchain is Ethereum, which uses a proof of stake algorithm where everyone can stake funds to validate transactions and receive a reward for doing so [25]. Permissioned blockchains are blockchain networks in which specific set of users or nodes are assigned to propose new ledger states. Examples of such a blockchain can be seen in Hyperledger Fabric or R3 Corda [17, 5, 55].

2.1.3 Public vs. Private Blockchains

Another distinction can be made between public and private blockchains. The *public* and *private* keywords refer to the restrictions, or lack thereof, in place for new participants to join the network and read information on the ledger. In a public blockchain network everyone has the ability to join the network and access the information on the blockchain. In a private blockchain only known users can access the network, this is usually done though authentication.

2.2 Decision scheme

2.2.1 What blockchain alternative do you need?

As a reaction to the rising need to determine if blockchain technology should be used Koens & Poll analysed 30 schemes [35]. Their analysis showed that some of those schemes lead to contradicting conclusions on which, or if, to use blockchain technology, when compared with each other. Additionally, they argue that most of the schemes are biased towards using blockchain technology, because the end-states of many schemes only mention blockchain-based solutions while excluding other data storage technologies. This has led to Koens & Poll proposing a new, unbiased decision scheme, shown in figure 2.2.

Figure 2.2 is made up of a number of binary-question that one needs to answer in the context of a given use case. These questions are numbered from 1 to 9 and can be found in the diamond shapes squares. One would start in the top-left of the scheme with the first question and end up in a certain end-state. In total there are eight possible end-states, which are represented by roman numerals inside squares on the right. These end-states represent the appropriate data storage technology that should be used for the use case in question.

With regards to the advice resulting from this decision scheme, we see that the end states recommend the use of specific types of data storage technologies. However, it is important to note that implementations of database technologies exist on a spectrum rather than in specific categories. Each use case is different and therefore the data storage needs of each use case vary.

Questions in the decision scheme [35]

As we can see in figure 2.2, the decision scheme contains a total of nine questions. These questions refer to the needed functionality and technical properties of a use case that is being evaluated. Because some words in the scheme (figure 2.2) are abbreviated we will list the question, in full, below:

- 1. Need to store state?

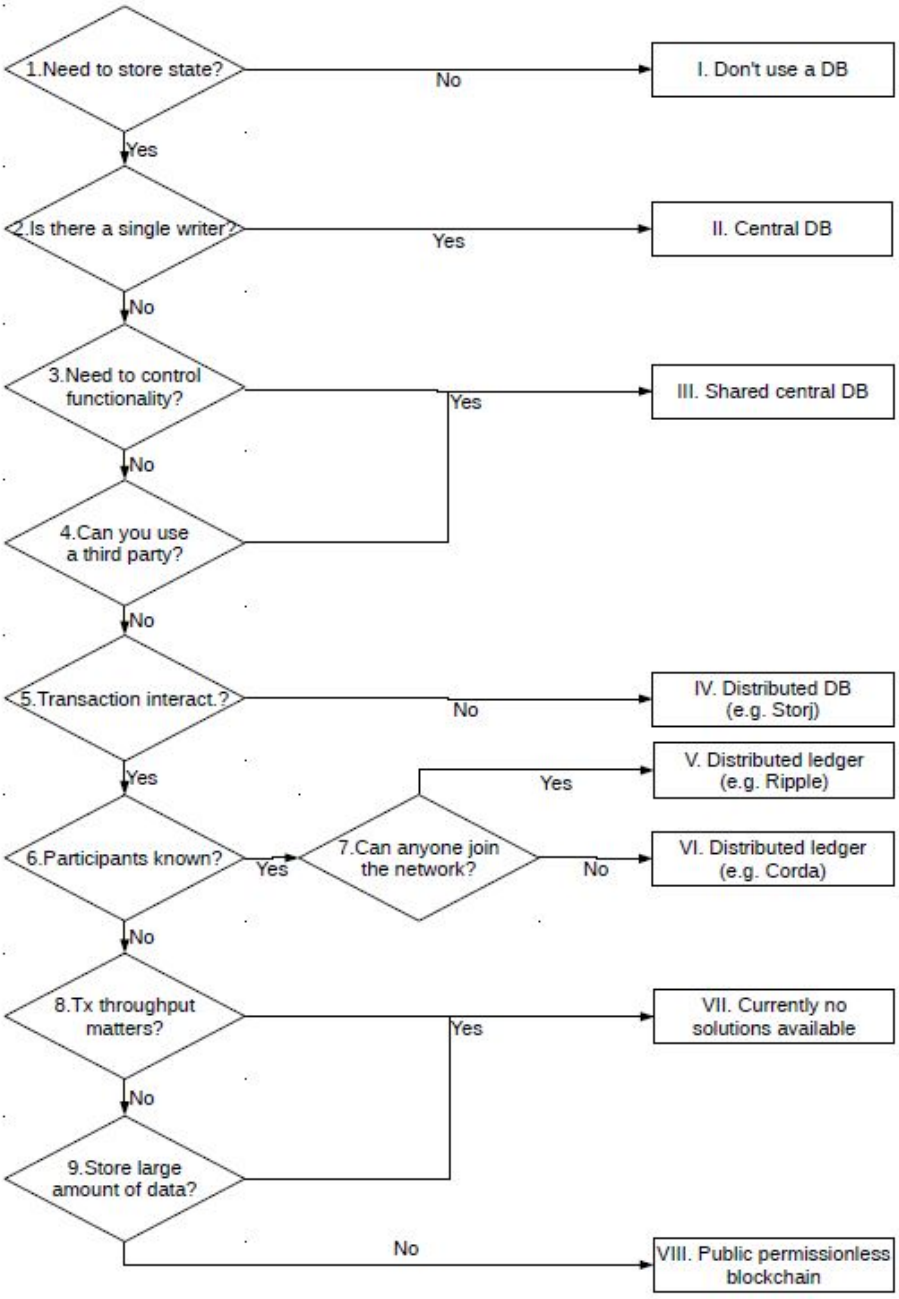

Figure 2.2: Decision scheme created by Koens & Poll to determine which data storage technology is applicable for a given use case. [35]

- 2. Is there a single writer?
- 3. Need to control functionality?
- 4. Can you use a third party?
- 5. Transaction interaction?
- 6. Participants known?
- 7. Can anyone join the network?
- 8. Transaction throughput matters?
- 9. Store large amount of data?

Even after writing out the abbreviated words, the questions are still concisely worded. Therefore we will elaborate on each of the questions and describe its meaning in the following paragraphs. Note that for a given use case, one does not have to evaluate each question in the scheme, as it is possible to arrive in an end-state from every question except for question 5.

Need to store state? (1) This is the first question encountered in this scheme. Each evaluation start by asking this question. The aim of this question is to obtain information about the need to store a state of the system. The state of a system refers to information or data captured by the system at a specific time[1]. Therefore this question evaluates to ***yes***, if and only if there is any need to store information in the system. If this is not the case, and the answer is ***no***, then we arrive in end-state ***I***. Answering this question with ***yes*** leads to question 2.

Is there a single writer? (2) This question is reached if there is a need to store state. Asking the question *"Is there a single writer?"* obtains information about the number of users/entities that can update the state of the system. If there is a single user or entity that can update the system (question is answered with ***no***), then we arrive in end-state ***II***. However, if multiple users or entities can update the state of the system (question is answered with ***yes***), then we are led to question 3.

Need to control functionality? (3) Having reached this question, we've established that there is a need to store states (1) and that multiple users or entities need to be able to propose new states (2). Koens & Poll define the meaning of 'controlling database functionality' as follows:

[1] https://whatis.techtarget.com/definition/stateless [Online; accessed 23. Mar. 2020]

> "Controlling database functionality may include setting the rules on how database permissions are set (such as create, store, delete), how the data is stored in the database (a relational database or an object oriented database), or how the database can be queried (e.g. ServerSQL, or MySQL)." [35, p. 10]

Note that they mention that these rules are being set and maintained by a specific party in the system, which is trusted by all users of the system. If there is a need for these kind of rules to be set and we trust a specific party in the system to do so, we answer this question with ***yes***, which means we arrive in end-state ***III***. Otherwise we are led to question 4.

Can you use a third party? (4) This question asks if there is a third party available that offers a comparable service that the use case in question offers. Most of the time this also comes down to trusting a third party in their sincerity. Note that Koens & Poll state that further research is needed surrounding the "important" concept of trust. Apart from this question trust is not taken into account in the decision scheme.

If there is a third party available that is trusted and offers the same service, one could use that service from the third party. This means we answer this question with ***yes*** and are led to end-state ***III***. If no third party is offering the same service or there are trust issues with using the third party, then we answer this question with ***no*** and are led to question 5.

Transaction interaction? (5) Koens & Poll use the following definition of transaction interaction. Koens & Poll use the term transaction interaction to describe the degree of coherence between transactions. In the case of Bitcoin this means that a valid transaction can only originate from a bitcoin address with a non-zero balance. That is, the balance of the bitcoin address was increased by a previous transaction [35].

The term 'transaction' leads us to believe we are performing a financial action in which a form of value is transferred between users. This need not be the case as a transaction can also refer to the exchange of data ownership between participants (users). If there is a need for the interdependent interaction of data in the system, we would answer this question with ***yes***. This would lead us to question 6. In the case that there is no need for the interdependent interaction of data, then the answer is ***no***, and we arrive in end-state ***IV***.

Participants known? (6) This question concerns the users of the system, which are called the participants. If the participants are known entities, whose identity can be validated, for example through using a certificate authority [35], then we should answer this question with ***yes***. In which case

we are led to question 7. If participants of the system are not known, then we move on to question 8.

Can anyone join the network? (7) If the system does not restrict access to itself for new users, and thus allows anyone to join the network, then this question should be answered with ***yes***. In which case we arrive at end-state ***V***. If however, there are certain rules in place that restrict access to the system for new users, then we arrive at end-state ***VI***.

Transaction throughput matters? (8) It is worth noting that from this question onward Koens & Poll state that a public blockchain may provide a solution. However, they also state that blockchain technology still has scalability issues [35].

> "Currently, blockchain is limited in processing a large number (a ball park figure is greater than 2000 transactions per second) of transactions (8). and is not fit for storing large amounts (e.g. Tera-bytes) of transactional data (9). Although current research in scalability has shown significant improvements ... there are currently no real life implementations on a global scale." [35, p. 11]

Therefore, if the system is required to handle a throughput of more than 2000 transactions per seconds, we should answer this question with ***yes***. This will lead us to end-state ***VII***. In the other case that low transaction throughput can be guaranteed, we should answer this question with ***no***, in which case we are led to question 9.

Store large amount of data? (9) As we can see from the quote in paragraph "**Transaction throughput matters? (8)**" in 2.2.1, blockchain is not yet suited for storing large amounts of data. So if the if a use case (eventually) requires the storage of Tera-bytes of data on the blockchain, we should answer this question with ***yes***. Having answered the question with ***yes*** leads us to the end-state ***VII.***. However, if the there is no need for the eventual storage of Tera-bytes of information, then we should answer this question with ***no***, in which case we are led to end-state ***VIII***.

End-states in the decision scheme [35]

Figure 2.2.1 contains a total of eight end-states in which one could end up when evaluating a use case. The end-state one would arrive in corresponds with the data storage technique that is most fitting for a particular use case that is being evaluated. Below is a list of all the possible end-states:

- I. Do not use a Database

- II. Central Database
- III. Shared central Database
- IV. Distributed Database (e.g. Storj [53])
- V. Distributed ledger (e.g. Ripple [6])
- VI. Distributed ledger (e.g. Corda [5])
- VII. Currently no solutions available
- VIII Public permissionless blockchain

The paragraphs below will elaborate on the each possible end-state.

Do not use a Database (I) Having reached this end-state the conclusion is that there is no need to store any state of the system. Therefore the advice is not to use a database.

Central Database (II) Because, in this end-state, the conclusion is that there is only a single writer that needs to alter the state of the system the advice is to use a central database. This could be local on-disk data storage that is only available to the system that needs to interact with the data.

Shared central Database (III) This end-state can be reached from two different questions (3 and 4). There is either a need to control access rights of multiple users to the data in the system, or there is the option to use a third party which offers the wanted functionality. In both cases a shared central database (e.g. ServerSQL, MySQL or third party hosted alternatives) should provide the needed functionality.

Distributed Database (e.g. Storj[53]) (IV) If we have reached this enc-state, the advice is to use a distributed database. A distributed database is defined as " A database that is not entirely stored at a single physical location, but rather is dispersed over a network of interconnected computers."[1]. Koens & Poll suggest to use a cloud-storage network such as StorJ in this case [35, 53].

Distributed ledger (e.g. Ripple[6]) (V) This end-state suggests one should use a distributed ledger. Ripple is suggested as being a viable solution in this case. [6]

Distributed ledger (e.g. Corda[5]) (VI) This end-state also suggest one should use a distributed ledger. However, in this case there is a need for a kind of access control because not anyone can join the network. Koens & Poll suggest to use a technology such as Corda [35, 5].

Currently no solutions available (VII) As can be read in the quote in paragraph **Transaction throughput matters?** in 2.2.1, despite the current research on scalability of blockchain, Koens & Poll suggest there are currently no justifiable solutions available to implement for a use case that ends up in this end-state.

Public permissionless blockchain (VIII) Koens & Poll argue that a public permissionless blockchain is the only viable blockchain solution one should consider. 2.2.1 Having reached this end-state, the use of such a blockchain solution is justified. In any other case, blockchain should not be used and other alternatives, such as the ones outlined above, are more applicable.

Chapter 3

Selecting use cases

In this chapter we will explore the current state of blockchain based initiatives in the healthcare sector. During this exploration we will make a selection of interesting cases, which we will analyse further in chapter 4. The criteria on which we make our selection will be discussed in section 3.1. After having discussed these criteria we will take a look at a collection of use cases from which we make our selection in section 3.2. In section 3.3 we will present seven use cases in the order in which we intend to evaluate them in chapter 4.

3.1 Criterion for selecting use cases

Before we can start with the evaluation of use cases, we first have to select a sub-set of the current blockchain based initiatives. In this research we do not have the time and/or resources to do a large literature study where we evaluate a large portion of the current proposals to use blockchain in healthcare. And since there are many blockchain-in-healthcare frameworks that have been proposed, but only a few that have been implemented or piloted [28], it is sensible to start our selection with the ones that are being implemented. Therefore, our criteria for selecting a use-case will be that the use-case is being implemented or piloted in some way. We believe that basing our selection on this criteria will lead to more substantial results after having evaluated the use cases. Because of the fact that the use cases are "*in-use*", as to say, the results might challenge the reasons for using blockchain in those particular use cases.

3.2 Collection of use cases

Since blockchain technology has been popularised by the introduction of Bitcoin, research has been ongoing to extend its applications to non-financial

use cases. It is expected that blockchain will have significant impacts in the healtcare sector. [16]

To obtain a collection of use cases we use the work of Chukwu and Garg ([28]), who provide an overview of current state of blockchain-in-healthcare research. Chukwu and Garg reviewed a total of 143 research articles and classified them in three categories.

- Framework Proposal
- Prototype
- Pilot or Implementation

Of those 143 articles, 57 percent of them (i.e. 82 of all 143) were classified as being a *Framework Proposal*. The remaining articles were subjected to further evaluation. *Prototypes, Pilots and Implementations* accounted for the remaining 61 of the reviewed articles, with only 7 of those articles falling under the categorisation of *Pilot or Implementation*. The initiatives categorised under *Prototypes, Pilots and Implementations* were evaluated on the following properties.

1. System architecture
2. Blockchain platform
3. Storage schemes
4. Standards or ontologies analysis
5. Privacy and security analysis
6. Blockchain type and consensus mechanism
7. Performance analysis
8. Cost analysis

With their analysis of these properties Chukwu and Garg identified three impediments withholding the implementation of blockchain in healthcare. Namely, poor scalability, low general performance and high cost generally hindered the implementation of the blockchain use cases from the analysed literature. It might be interesting to see if these three impediments; scalability, performance and cost, apply to to the chosen use cases outlined in section 3.3.

Interesting use cases

Following the criterion from section 3.1, namely that a use case is being implemented or piloted, we find that there are seven publication mentioned by Chukwu and Garg that are of interest to us. These publication discuss use cases that are classified as **Implementations or Pilots** and thus are in line with our criteria. In the following section (3.3) we will discuss these use cases in more depth. Even though these cases are all classified as implementations or pilots, we will see that there is a big difference in the degree of realisation of the use cases.

3.3 Use cases

In this section we will elaborate on the seven use cases we have identified as interesting. We start of by discussing the *e-Health* initiative implemented by the Estonian government in 3.3.1. Afterwards, in section 3.3.2, we will discuss *EmrShare*, a framework for managing and sharing medical data across organisations. Section 3.3.3 will discuss the BAQALC project, an abbreviation for *Blockchain Applied FASTQ and FASTA Lossless Compression*. Section 3.3.4 will describe the *Modum.io* initiative. Section 3.3.5 will discuss *OmniPHR*, a blockchain-based personal health record implementation. In section 3.3.6 we will discuss an initiative that uses blockchain for health information exchange and the persistent monitoring of clinical trials. Finally, in section 3.3.7, we will discuss a blockchain-based framework that helps with the screening for dyslexia in children.

3.3.1 e-Health Foundation in Estonia

Heston ([34]) provides us with a short case study in which he acknowledges the fact that the e-Health Foundation of the Estonian government uses blockchain technology to ensure the integrity of healthcare records of its citizens. Namely, by using a blockchain-based initiatives called Keyless Signature Infrastructure (KSI) Blockchain developed by the company Guardtime. Currently the KSI Blockchain is fully implemented within the e-Health foundation. Compared to the other use cases from this section, the implementation of blockchain in the *e-Health* initiative is being done on the largest scale. Later in section 4.1 we will evaluate this use-case and see if the usage of this type of blockchain is justified. Necessary information needed for this evaluation will also be given in 4.1.

3.3.2 EmrShare

As explained by Xiao et al. ([56]), developments in information and storage technologies have lead to a change in the way we use and interact with

digital documents. One sector that has undergone many changes in the storage of (digital) documents is the healthcare sector. Patient records and medical records have been largely digitised, allowing these electronic medical records (ERMs) to be shared between organisations. However, these ERMs often contain sensitive personal information. And as a result the sharing of these EMRs comes with privacy concerns, strict legal regulations and trust issues. These factors lead to the sharing of EMRs to be a time-consuming affair in a sector in which time is often of the essence. Xiao et al. proposed a blockchain based initiative called EMRShare in which a permissioned blockchain is used "to resolve the trust concern existing in EMRs sharing practice among different participants like patients, clinicians and researchers, and other relevant parties such as insurance agents and government, to make medical data sharing and access secure, inefficient, transparent, immutable, traceable, and auditable." [56, p. 1].

This use case is currently classified in the Implementation or Pilot phase by Chukwu and Garg. We could not find any information of current implementations of this framework. The article by Xiao et al. state that only small scale performance analysis has been conducted on a simulation hosted on Amazon Web Services (AWS [1]). Therefore it would have made more sense if this use case was classified as a prototype by Chukwu and Garg.

3.3.3 BAQALC

Developments in high-throughput DNA sequencing technology have lead to a major reduction in the cost of genome sequencing. This resulted in "revolutionary advances" within the genetics industry [38, 52]. However, even after reducing the cost and time it takes to perform DNA sequencing, the management of the large amount of data involved is still being considered as an issue. Next Generation Sequencing allows for the parallel processing of DNA data, but the storage of the generated data is still regarded as an issue [26]. As a result Lee et al. have proposed a Blockchain Applied FASTQ and FASTA Lossless compression (BAQALC) algorithm, a lossless compression algorithm which allows for the storing and transmission of large amounts of DNA sequence data [38]. In their proposal they state that this solution is currently being tested on a small scale and therefore this use case is in the pilot phase.

3.3.4 Modum.io

Within the medical industry there are strict rules and regulations surrounding the transport of medical products. Factors such as temperature and humidity need to be kept in check to ensure the quality of the transported medical goods. Modum.io is a startup presented by Bocek et al. in which

[1] https://aws.amazon.com/

blockchain technology is used in combination with IoT (Internet of Things) sensor devices to ensure data integrity and provide public information of transportation data in supply-chains [22]. Modum.io was initially presented as a solution for pharmaceutical supply-chains, but has broadened the scope since its release to provide other supply chain solutions for sensitive goods. Modum.io is currently in the implementation phase providing supply chain solutions to various sectors.

3.3.5 OmniPHR

At the current point in time healthcare data of patients is often scattered over multiple organisations within the healthcare sector. There are multiple standards in place for healthcare records, with some of them being patented by healthcare providers. Electronic Health Records (EHRs) and Personal Health Records (PHRs) are usually stored in the database of the healthcare providers, which combined with the fact that their data is scattered over multiple organisations, leads to patients not being able to easily access and control their data. This also leads to inefficiencies in communication of healthcare data between organisations. Roehrs et al. aims to solve these issues in their proposed OmniPHR model, a distributed solution for maintaining and accessing PHRs [48]. The author states that future work needs to go into evaluating security and integrity of OmniPHR and the integration into other systems. From this we condlude that OmniPHR is in its early stages of being tested and therefore in its pilot phase. Superficially it seems that OmniPHR and EmrShare (section 3.3.2) are similair use cases. However, OmniPHR aims to create a model that obtains healthcare data from various sources and bundles them together to be presented to its users, where as EmrShare is a framework that facilitates the sharing of healthcare data.

3.3.6 Health Information Exchange and Persistent Monitoring for Clinical Trials

Zhuang et al. explored the application of smart contracts in the context of health information exchange and for monitoring clinical trials [60]. They created a proof-of-concept with smart contracts on the Ethereum blockchain and state that their implementation uses a private blockchain. For now it seems that this project is not being used or implemented on any significant scale as the authors only have presented a minimal viable product that is based on blockchain. Additional research has improved this minimal viable product and tested it in a simulation process [59]. However, no statements have been made about further implementations. This leads us to believe that this use case is currently in the pilot phase.

3.3.7 Blockchain-based screening framework for children with dyslexia

Rahman et al. proposed a framework for testing and identifying dyslexia with the use of a mobile multimedia Internet of Things environment [47]. They use blockchain technology in their framework for the storing and sharing of test results. The future work of this article included proposed tests in different hospitals in the UK and Saudi Arabia indicating that this use case is in its pilot phase.

Chapter 4

Evaluation of use-cases

4.1 Use Case: e-Estonia [34]

4.1.1 e-Estonia

Estonia prizes itself on being "the world's most advanced digital society" [7]. They have taken the lead as a nation on the digitisation of many of their government services. For instance every citizen of Estonia has a digital identity that allows them to file taxes, view their medical records and even vote online. Their e-governance strategy has lead to 99 percent of state services to be accessible as e-Services online. Through a GovTech partnership with the company Guardtime the government uses Keyless Signature Infrastructure (KSI) for independent verification of integrity of government processes [12]. The Keyless Signature Infrastructure uses a blockchain to record the history of generated signatures. These signatures can then be used to verify the integrity of digital data. One e-Service in which the KSI blockchain is used, is the e-Health service. This service is offered by the e-Health foundation, which is tasked with preserving the privacy of the users as well as ensuring the security and integrity of the user's medical data. We will see that the type of blockchain being used in this use case most resembles a private permissioned blockchain.

4.1.2 KSI Blockchain

Information of the KSI blockchain useful for the evaluation of the use case

The Keyless Signature Infrastructure is a means to provide digital signatures. More information on the Keyless Signature Infrastructure is given in the following paragraphs of this section (4.1.2). Below we summarise a few points that are used in the evaluation of the e-Health use case in 4.1.4.

- The Keyless Signature Infrastructure can be used to create digital sig-

natures. To obtain a signature on digital data, a hash value of this data is send to one of the aggregation servers of Guardtime. Each second Guardtime aggregates the hashes and creates unique signatures for each received hash. These signatures are used to verify the integrity of user data. Signature data is recorded on the KSI blockchain which allows signatures to be verified independently or by using the KSI Application programming interface (API). Records of this blockchain are periodically published by Guardtime in widespread media channels.

- The Keyless Signature Infrastructure is able to create up to 10^{12} signatures per seconds. This allows KSI to be applicable for use cases that require the creation of large amounts of signatures on a specific time.

- The KSI blockchain is identified as being a private permissioned blockchain. This is because the KSI service is being offered by the company Guardtime. Guardtime requires users to authenticate in order to use the KSI blockchain. The aggregation servers owned by Guardtime are the nodes that are eligible to propose new states of the KSI blockchain.

An explanation of the Keyless Signature Infrastructure

This section will contain some background information regarding the mechanism behind the Keyless Signature Infrastructure. Not all of the information given in this section is necessary for answering the questions in 4.1.4, but rather to give a more complete picture of the e-Health use case. Essential information regarding the evaluation will be summarised in the previous paragraph of this section (4.1.2).

The Keyless Signature Infrastructure, or KSI, is a proprietary digital signature scheme developed by Guardtime [23, 13]. The signature scheme uses a hash tree (Merkle tree [20]) to enable the verification of integrity of digital data. Each second Guardtime collects the hashes of data sent by the users of the KSI, these hashes are then aggregated into a hash tree called the *Global Aggregation Tree* with at the top of the tree the *Global Root Hash Value*. During this time a signature token is sent back to the user that proves that the data existed at the time it was received and that the data was sent by a that specific user (or send through a specific access point) [23]. This process is illustrated in figure 4.1. After the construction of the *Global Aggregation Tree* the *Global Root Hash Value* is added to the *Calendar Blockchain*, which introduces a blockchain structure in the KSI. The *Calendar Blockchain* is in essence another Merkle tree to which the *Global Root Hash Value* from each aggregation tree is added.

Using the received signature token, which contains a series of hash-values, the user is able to verify the integrity of a digital file which hash-value has previously been submitted to the KSI blockchain. Guardtime states that

the theoretical maximum of signatures per second that the KSI is able to process is $2^{50} \approx 10^{15}$, as the depth of the hash-tree is fixed at 50 [23]. However, e-Estonia states that KSI can process 10^{12} signatures per second, which is probably a result of the data processing overhead [8].

The aggregation of hash trees as well as the creation and verification of signatures is performed by four layers of geographically dispersed clusters of servers. These servers are provided by Guardtime which makes the KSI blockchain a permissioned blockchain. And as the identification of the user is required for the user to be using the KSI blockchain service, we deduce that the KSI blockchain is seen as a private blockchain. Therefore we state that the KSI blockchain is a private permissioned blockchain. Note that this classifications are not explicitly given as such by Guardtime. They simply state that the *Calendar Blockchain* consists of another hash tree which links the blocks (*Global Root Hash Values*) together. The root of this (meta) hash tree is published periodically in widespread media allowing for the independent verification of signatures as well to allow users to verify existing signatures even if Guardtime ceases to exist.

It is worthy to note that compared to other permissioned private ledgers such as Corda [5] or Ripple [6], the KSI blockchain does not offer the same functionality. For instance, Corda and Ripple are able to facilitate the transfer of ownership of digital assets between users. KSI on the other hand is a framework that creates signatures that verify integrity of digital data. Despite the differences in functionality, if we follow the definitions from section 2.1.1, we see that the KSI blockchain is placed inside the category of a private permissioned blockchain.

KSI signature security claims

We have seen that KSI signatures can be used to verify the integrity of digital data. This is done by relying on the security of hash-functions. In the documentation of the KSI Java SDK from Guardtime's Github page we find that KSI supports multiple hashing algorithms [3, 33]. Table 4.1 lists the supported algorithms and the corresponding security strengths of these algorithms. As KSI signatures aim to provide verifiable integrity of data files, these data files need to be accessible and stored alongside the signatures of these files. With access to the files stored, the integrity of these files can be guaranteed up to the security level defined under the 2nd preimage security strength in table 4.1, as this denotes the effort needed to find the same hash value from a different data input.

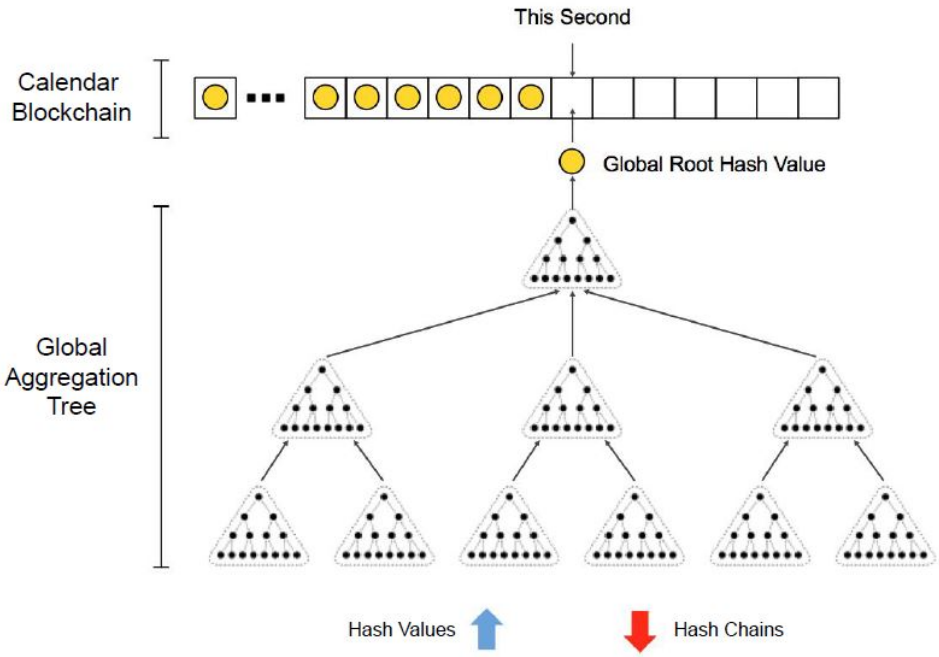

Figure 4.1: An illustration of the KSI blockchain. [40]

Comparing Keyless Signature Infrastructure to Public Key Infrastructure signatures

In 4.1.2 we have seen that KSI is able to provide digital signatures that can be used to verify the integrity of the signed data. Another way to ensure the integrity claim of digital data is through the use of public key infrastructure (PKI) signatures. In this sub-section we will provide a brief overview in the differences between KSI and PKI signatures.

To start the comparison we make an effort to define the trusted computing base (TCB) of both the Keyless Signature Infrastructure and Public Key Infrastructure is these systems were used for creating signatures on medical data in the e-Health use case. In both KSI and PKI it is inevitable that the signers of the data (i.e. the doctors and organisations) are trusted to be sincere and are able to manage their credentials. In the KSI framework credentials are used to authenticate to Guardtime, signers are active in an organisational network from which the signer is able to make a connection to Guardtime to request and verify signatures. To verify the KSI signatures, an organization can do this independently using the published records of Guardtime or by communicating with the KSI access point. By communicating with the KSI access point we must trust the communication channels between Guardtime and the organization. By using PKI to create signatures we see that credentials are used in a different way. Credentials for PKI sig-

Hashing Algorithm	Security strength in bits		
	Collision	Preimage	2nd Preimage
RIPEMD_160	80	160	160
SHA2_256	128	256	256
SHA2_384	192	384	384
SHA2_512	256	512	512
SHA3_224	112	224	224
SHA3_256	128	256	256
SHA3_384	192	384	384
SHA3_512	256	512	512
SM3	128	256	256

Table 4.1: Overview of the security strength of the supported hashing algorithms for signatures in Guardtime's Keyless Signature Infrastructure. [33, 46, 30]

natures are in the form of a public and private key pair which are owned by the signer and allow the signer to sign data offline. Verification of PKI signatuers is done by using the public key of the signer. A certificate issued by a Certificate Authority (CA) is used to confirm that a public key belongs to a specific signer (i.e. doctor or organisation). By using PKI signatuers we have to trust the Certificate Authority as well as the certificate that is used in the signature.

The main difference between KSI and PKI signatures is that KSI derives its integrity claims by relying on the security of one-way hash functions (e.g. SHA-256), while PKI's integrity claims rely on public key cryptography (e.g. RSA or ECC). PKI signatures also require additional data to be added within the signatures such as verification of identity of the signer, a certificate confirming the identity from a Certificate Authority (CA), time-stamping data as well as other information that ensures the validity of the signers keys to prevent revocation problems and prove the keys are valid at the signing time [24]. Compared to PKI signatures, the KSI signatures seem to be less complex, only consisting of a hash-value appended with user identification coupled with the necessary hash-values of parent nodes to calculate the global root hash value. PKI signatures are valid as long as the certificate from the CA is deemed to be valid, KSI signatures on the other hand are valid indefinitely. Another difference we see is that KSI signatures are said to be "Quantum-immune" as opposed to PKI signatures, as cryptographic hash functions are resistant to quantum computational attacks [24].

For an organisation to create valid signatures using KSI, that organi-

sation needs to authenticate itself to Guardtime, so in order to falsify a signature, an attacker needs have access these credentials and the network of the organisation providing the signature, as the signature can only be created online with a connection to Guardtime. However the damages of a breach in an organisation are limited. Signatures of other organisations and users remain valid and depending on the digital infrastructure of the organisation the time of entry of an attacker can be seen through the use of access logs, whose integrity can also be verified with KSI, withholding the attacker from erasing its tracks. By taking this approach the aim is not to stop an attacker from entering, but rather to pinpoint the fact that a breach has happened and acting accordingly. This would allow the signature created before the time of entry to still be valid.

PKI on the other hand suffers from more catastrophic damages in a breach. In the case that an organisation is breached that organisation would have to revoke all of its signatures as the validity of these signatures cannot be guaranteed anymore. If there is a breach in the CA providing certificates to a particular organisation used in their signatures and an attacker is able to create false certificates, then this leads to the forced revocation of all signatures of all organisation that use certificates of that CA.

In KSI we see that trust is placed in the organisation to manage their own credential. Compare this to PKI were trust is not only placed in the organisation to manage their keys, but also in the security and validity of CA certificates and we see that within KSI a lower degree of trust is required. KSI has the other added value of the indefinite validity of signatures as well as being resistant to quantum computational attacks.

4.1.3 The usage of KSI Blockchain by Estonia's e-Health Foundation

One of the responsibilities of Estonia's e-Health foundation is facilitating the communication of sensitive medical data between hospitals and medical centres. This sensitive medical data includes data such as medical records of patients, digital prescriptions and access logs. This data gets send from the hospitals and medical centres to the e-Health foundation, which then uses the Keyless Signature Infrastructure to ensure data integrity [9]. As explained in previous paragraph, this is done by sending a hash value of the data to the KSI access point of Gaurdtime and receiving a signature. This signature can be used to verify the integrity, time of existence and author of the data.

Identifying more specifics on the technicalities of how KSI is implemented by the e-Health foundation remains a challenge. Information from the ICT department of the e-Health Foundation, the Health and Welfare Information Systems Centre of Estonia, could not be used as is was written in the Estonian language [15]. We therefore rely on the information provided by

Guardtime regarding the implementation of the KSI blockchain.

4.1.4 Evaluation against decision diagram of Koens & Poll [35]

In this section we will evaluate the e-Health use case, mentioned in 3.3.1, against the different questions in the decision diagram (figure 2.2) outlined in section 2.2.1. As we have identified in section 4.1.2, the KSI blockchain used in the the e-Health initiative can be considered a private permissioned blockchain. Following the definitions of Koens & Poll, a private permissioned blockchain resembles a distributed ledger. By answering the questions below we will see if we end up in an end-state that corresponds with a distributed ledger technology. Note that it is important to state the point of view from which we approach the following questions. Although it is possible to evaluate the need to use blockchain technology in the Keyless Signature Infrastructure, we will not be taking this approach. In fact, we will be approaching the questions from the point of view of the e-Health foundation, which as we identified, uses distributed ledger technology to ensure the integrity of medical data (section 4.1.2). The users in this system are the healthcare providers who are affiliated with the e-Health foundation in order to ensure the integrity of their data.

- 1. **Need to store state?** Yes.

  Because of the fact that healthcare records need to be updated and these updates need to be verified, the state of the e-Health system of Estonia needs to be stored. Therefore we can answer this question with ***yes***. Because we have answered this question with ***yes***, we move on to the second question.

- 2. **Is there a single writer?** No.

  No, there are multiple writers in the e-Health system. These writers take the form of organisations authorised to access and update medical records and prescription data. Therefore they propose state to the medical data in question. Having answered this question with ***no***, leads us to move on to the third question.

- 3. **Need to control functionality?** No.

  While it is true that certain users in the e-Health system have permission to request and verify a KSI signature of to the e-Health records, these sets of actions and rules set by the e-Health system and do not need to be changed. Each healthcare provider can perform these actions, there are no discrepancies between the actions and rules set for each of the users. New users are subjected to the same rules as existing users indicating that these rules do not need to be changed. Therefore

we answer this question with ***no***. Because of that answer we move on to the fourth question.

- 4. **Can you use a third party?** Yes & No.

  We see that this question can be answered with both ***yes*** and ***no***. The main factor that determines whether we answer this question with yes or no is the trust implications of using a particular third party. However, we cannot make any statement on the e-Health foundation's stance on the preferred degree of trust in third parties. We will see that we cannot use a different third party other than Guardtime that provides the same functionality for the e-Health system without introducing a more centralised approach of trusting that party.

  Currently, the e-Health foundation uses the third party Guardtime though a partnership. So in that sense we should answer this question with ***yes***. However, answering this question with yes leads us to the end-state in which a shared central database is advised. Guardtime does not take this data storage approach as it introduces a single point of failure. This is not desired by the e-Health foundation. The e-Health foundation emphasises the the need for verifiable integrity and mitigation of internal threats to medical data [9]. The KSI framework is used, not as a security tool to prevent attackers gaining access to e-Health communication systems, but to make attacks visible by signing medical data and access logs. From this we see that if we were to use another third party, that third party would need to offer this functionality of assuring the integrity transparency of data changes in the e-Health system.

  In theory one could place trust in another third party or another government service to provide the service of verifying the integrity of the medical data in the e-Health records. However, this would simply shift the trust from the Guardtime to the other party or multiple parties. For instance, as we have seen in 4.1.2, if another party is used to provide digital signatures which uses a Public Key Infrastructure signature implementation, trust is not only being shifted towards that party in general, but also to their ability to properly manage keys as well as to the certificate authority providing certificates for the signatures.

  The need for trusting a third party to verify data integrity is eliminated by using an implementation of the KSI blockchain, as this verification can either be done through communication with Guardtime or by verifying the KSI signatures independently. In this system we see that Guardtime still plays a central role in the verification process. However, given that the users of the KSI infrastructure can also independently verify the generated KSI signatures, the trust in Guardtime

is less prominent compared to the required trust in other alternative third parties.

As of now there seems to be no third party, besides Guardtime, that both eliminates the trust placement in an audit service and that is able to verify the integrity of data while at the same time allowing for independent verification.

For this reason we choose to not give a hard yes or no answer and evaluate the remaining questions since there is no centralised third party alternative that offers the same functionality and benefits of the KSI framework.

- 5. **Transaction interaction?** Yes.

  As explained in section 2.2.1, transaction interaction does not necessarily refer to a financial action but to the interdependent interaction of data in the system or service. Within the e-Health system this property is not as evident as, for example, in Bitcoin, where the validity of a transaction directly depends on past transactions. However, there is a case to be made for the interdependence of medical files and access logs. The system is required to allow updating the state of these files. Where the integrity of a particular version or after a state update of these files needs to be verifiable to guarantee the file history. By using KSI, the validity of these signature depends on the validity of not only the previous signatures of that particular file, but on every signature from the past. This particular property provides undeniable proof of integrity, which is ultimately needed for the e-Health use case. Therefore we see that 'transaction interaction' is needed in this use case and we answer this question with ***yes***. Because we have answered this question with ***yes***, we move on to the sixth question.

- 6. **Participants known?** Yes.

  In the e-Health system we can identify two types of participants. The organisations using the service and the citizens of Estonia whose medical data is being stored and communicated between the organisations. The organisation connected to the e-Health system are known to the e-Health foundation. The Estonian citizens use the e-Health service to access and view their medical data though the state portal [10] and rely on the integrity of the data that can be viewed in there. Only registered citizens can access the state portal and since the e-Health service is a service offered by the government, we conclude that these citizens are known and identifiable in the system. Because all participants of the e-Health system are known we answer this question with ***yes*** and move on to the seventh question.

- 7. **Can anyone join the network?** No.

The e-Health Foundation does not just allow everyone to join the network. Medical organisations obviously have to follow strict rules and regulations to become part of the e-Health infrastructure and process medical data of Estonian citizens. The other type of participants, the Estonian citizens, need to be registered Estonians to access data through the e-Health service in the state portal as the state portal is accessed with the use of their personal ID card. Therefore we conclude that this question can be answered with ***no***. Having answered the question with ***no*** we are lead to end-state ***VI.*** in the decision scheme.

- 8. **Transaction throughput matters?** N/A

  Not applicable as this question is not reached in the decision scheme.

- 9. **Store large amount of data?** N/A

  Not applicable as this question is not reached in the decision scheme.

During the evaluation we found that providing a binary answer to question 4 and question 5 was not as straight forward as it was for the other questions. Question 4 asks if there is a third party that can be used for this use case, even though this might be possible, and each solution might have its pros and cons, the e-Health service praises the fact that they use KSI and its benefits [8]. We therefore evaluated question 4 by keeping in mind the benefits that KSI offers and came to the conclusion these benefits are not offered by any other (centralised) third party. Question 5 asks if there is a need for transaction interaction. We see that this question is not as applicable in a healthcare use case compared to a financial use case, however the validity of a signature of a file at a given moment relies on the fact that all preceding signatures are also valid. Taking into account that later versions of a file are only valid if the history of that file can be proven, we can view the series of state updates to this particular file as transactions in the e-Health system.

Resulting end-state

As a result of answering question 7 with a ***no*** we are led to end-state *VI. Distributed ledger (e.g. Corda).* The advice is to use a distributed ledger technology such as Corda [5]. Corda started out as permissioned blockchain solution for the financial industry, but has since grown into an open source permissioned blockchain platform that can be applied to companies in multiple sectors. On the surface Corda seems to offer more functionality than the current KSI blockchain implementation in the e-Health service, however the question remains whether or not this added functionality is needed in this particular use case. The e-Health service mainly uses KSI to ensure integrity of data, where as Corda is more suited for the handling and executing

financial transactions and data transfers by making use of smart contracts. Interestingly, in an interview with Guardtime's General Manager of Financial Services it is mentioned that Guardtime is currently using Corda to develop new business solutions [2]. Coming back to the Estonian e-Health use case, the KSI blockchain implementation does seem to be a good fit according to the results of the decision scheme. This is confirmed by this resulting end-state we arrive in as we identified KSI to be a distributed ledger in 4.1.2.

4.1.5 Evaluation of 3 major impediments; poor scalability, low general performance and high costs

Whilst obtaining the the collection of use cases to evaluate mentioned in 3.3 from the work of Chukwu and Garg in section 3.2, we saw that there are currently 3 impediments limiting the implementation of most blockchain based initiatives [28]. Namely, poor scalability, low general performance and high cost. Chukwu and Garg concluded that these barriers that limit implementation generally apply to blockchain solutions in healthcare, however they do not state how these impediments relate to this use case in particular. In section 4.1.2, we saw that the KSI blockchain is scalable to handle 10^{12} signatures per second. Since this volume is magnitudes greater than what traditional blockchains can handle, this provides a counter-argument against the scalability impediment. Additional analysis of the performance and cost of the Keyless signature infrastructure has shown that the network response time is nearly 50% shorter, as well as a 20% reduction in the cost of data storage compared to conventional blockchain technology [43]. Therefore, we conclude that the three impediments do not hinder this specific use case.

4.2 Use Case: EmrShare [56]

4.2.1 EmrShare

EmrShare is a blockchain based framework, proposed by Xiao et al., which facilitates the sharing and management of Electronic Medical Records (EMRs) [56]. Statements given in this section are drawn from the work of Xiao et al. [56].

In the healthcare sector patients' medical data is often scattered across multiple organisations, which leads to the need for EMRs to be shared between medical institutions. Given that these EMRs contain personal medical data, the sharing of these EMRs requires careful surveillance and is subjected to strict regulations. As a result the sharing of EMRs across organisations introduces "excessive" administrational costs.

The purpose of the EmrShare framework is to unify the sharing and management of EMRs across multiple organisations. This would lead to more

efficient sharing procedures between organisations such as medical centres, research institutes and government institutions.

The EmrShare framework uses an "*Off-chain Secure Data Management*" and "*On-chain Document and Data Tracing*" approach for storing data. The actual medical data is stored *Off-chain*, as storing it on a blockchain is too expensive. Xiao et al. proposes two ways to facilitate this *Off-chain* storage. Either a single organisation, such as a government agency, is tasked with providing the storage facilities for hosting the medical data. Or the medical data will be kept at the healthcare institutions as it currently is. The data stored on the blockchain (*On-chain*) consist of data requests and request approvals. In both cases of the *off-chain* storage, the data stored *on-chain* will contain a uniform resource identifier (URI) that points to the medical data stored *off-chain* as well as encrypted credentials to access this data. Figure 4.2 contains an illustration of the flow of information in the EmrShare framwork.

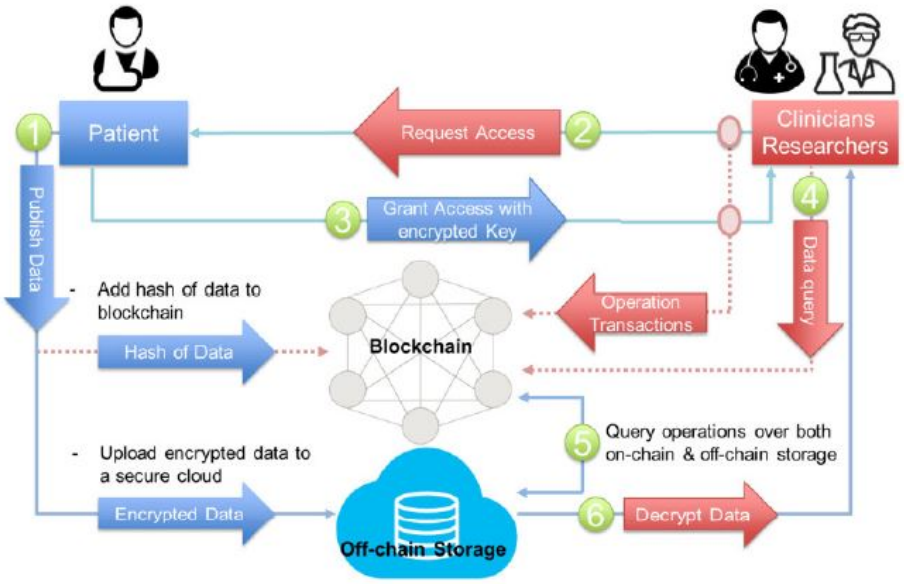

Figure 4.2: An illustration of the flow of information in the EmrShare framework. The successive actions are numbered 1 through 6. [56]

4.2.2 The use of blockchain in EmrShare

In this section we elaborate more on the way blockchain is used in the EmrShare framework. As we have stated in 4.2.1, a blockchain is used to establish and record sharing agreements between two parties. The EmrShare blockchain-based framework ([56]) is build using Hyperledger Fabric ([17]).

Hyperledger Fabric is a framework in which private permissioned blockchain solutions can be created. For this reason Xiao et al. classify EmrShare as a private permissioned blockchain. Following from the definitions in 2.1.2, we see that this classification of a private permissioned blockchain is correct.

To allow for the verification of the integrity of the medical data stored *Off-chain*, a hash value of data is uploaded to the blockchain. Besides that other information such as; the location of stored medical data, patient and doctor ID, file permissions and degree of anonymity are stored on the blockchain. Figure 4.3 shows an overview of the stored data on the blockchain. It also illustrates the data flow between *On-chain* and *Off-chain* storage.

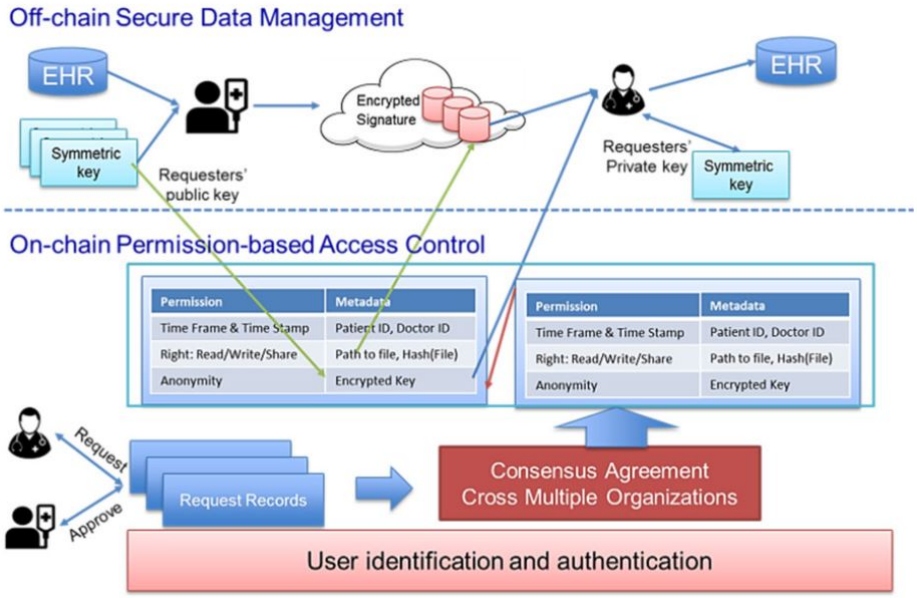

Figure 4.3: An illustration of the data flow between the Off chain Secure Data Management en the On-chain Permissioned-based Access Control of the EmrShare framework. [56]

4.2.3 Alternatives for the EmrShare framework

The authors of EmrShare state that there are current non-blockchain based solutions that facilitate the sharing of electronic patient data between organisations [56]. However, their related work does not mention any non-blockchain based solutions, nor do they mention specific solutions that are currently in place. They compare EmrShare to current practices, but lack proper argumentation and references to sources to back up the claims they make on these current solutions.

In this research we've identified several alternative EMR sharing solutions. The solutions presented in the references we use in this paragraph are not blockchain-based. Azarm-Daigle et al. performed a literature review of current cross-organisational healthcare data sharing solutions and frameworks [18]. The results of Azarm-Daigle et al. show that the reviewed solutions are not cost-efficient, fully automated or truly real time. This indicates that there is a need for a feasible inter-operable health information system shared across healthcare providers. A publication by Li et al. proposes a scalable and secure solution for sharing personal healthcare records [39].

One remark that is made by Xiao et al. is that privacy concerns are present in current alternative EMR sharing solutions [56]. An article by Chen et al. proposes a privacy-preserving framework for healthcare data sharing [27], implementing this framework would counter the argument of Xiao et al. Besides the publication of Chen et al., others have also proposed secure electronic health record sharing frameworks that preserve the privacy of its users [54, 31].

It is not in the scope of this thesis to compare the performances of the mentioned solutions to the EmrShare framework. By providing alternative EMR sharing solutions we show that there are indeed alternative non-blockchain based solutions. These solutions also solve the privacy concerns, mentioned by Xiao et al. [56], present in the current data sharing processes.

4.2.4 Evaluation against decision diagram of Koens & Poll [35]

In this section we will evaluate the EmrShare use case, mentioned in 3.3.2, against the different questions in the decision diagram (figure 2.2) outlined in section 2.2.1. As seen in 4.2.2, the EmrShare framework runs on a private permissioned blockchain. A private permissioned blockchain corresponds with a distributed ledger seen in the end-states of the decision diagram..

To start the evaluation we try to define the exact use case that EmrShare tries to solve. EmrShare is used as a mediation framework in which electronic medical records can be shared between organisations. Participants or users in the EmrShare network are the patients and medical institutions sharing EMRs as seen in figure 4.2. Clinicians and researchers from medical institutions can send a request to a patient to access (parts of) their patient records. The patients can approve or deny the request and the EmrShare framework handles the response.

- 1. **Need to store state?** Yes.

  The EmrShare use case facilitates the sharing of EMRs. The use case must allow for the medical data to be updated as well as information

to be stored on which EMR is shared with which organisation. For this reason we see that the state of the EMRs and all the accompanying sharing information need to be stored. Therefore we answer this question with ***yes*** and move on to the second question.

- 2. **Is there a single writer?** No.

  Multiple organisation need to be able to update medical data inside patients' EMRs. This means that for updating EMRs, multiple writers are required. However, the main objective of this use case is to allow for the sharing of these EMRs between organisations. But even in that case, multiple writers are needed as data sharing requests and the patient responses to these requests need to be recorded and stored. This means that we answer this question with ***no*** and move on to the third question.

- 3. **Need to control functionality?** No.

  At first it may seem that we need to control database functionality in the sense that we need to set restriction for particular users to write to and read from the stored EMRs. However, the sharing of EMRs can be guided in this use case through a set of predefine rules for each type of user (patients and organisations). Xiao et al. state that in this sharing scheme/framework, all participating parties engage in the same unified system. Both patients and organisations are to follow a set of mutually agreed rules and predefined contracts handling the sharing of EMRs. By specifying how each user is able to gain and revoke access to the stored EMRs from the start, the database permissions for these users does not need to be updated and controlled by a single party in the system. Following the definition of this question, we answer this question with ***no*** as there is no single party that needs to update the database functionality for specific users. Having answered this question with ***no***, we move on to the fourth question.

- 4. **Can you use a third party?** Yes.

  This question is perhaps the most interesting question for this use case. The cross-organisational sharing of electronic medical records is already implemented in practice. For example, in the Netherlands the Nictiz organisation is responsible for the digital information exchange in the Dutch healthcare sector [14]. The Nictiz organisation designs country-wide standards, architectures and infrastructures used in cross-organisation health information exchange. They have implemented the AORTA framework that facilitated health information exchange between various types of medical professionals. Another example is seen in the United Kingdom where the National Health Service (NHS) which designs and implements various healthare IT services

that facilitate sharing of medical data. The NHS has implemented the Data Access Request Service (DARS) [4]. DARS is used by clinicians, researchers, and commissioners to obtain healthcare data sets when properly authorised. As we have seen in 4.2.3, there are various other frameworks and solutions that facilitate cross-organisational sharing of medical data. This combined with the mentioned examples shows that the functionality that the EmrShare offers has already been implemented in various ways. Therefore we see that it is possible to use a third party to facilitate cross-organisational medical data sharing. By concluding that we can use a third party for this specific use case, we answer this question with ***yes***. This means we are directed towards end-state ***III.*** in the decision scheme.

- 5. **Transaction interaction?** N/A

  Not applicable as this question is not reached in the decision scheme.

- 6. **Participants known?** N/A

  Not applicable as this question is not reached in the decision scheme.

- 7. **Can anyone join the network?** N/A

  Not applicable as this question is not reached in the decision scheme.

- 8. **Transaction throughput matters?** N/A

  Not applicable as this question is not reached in the decision scheme.

- 9. **Store large amount of data?** N/A

  Not applicable as this question is not reached in the decision scheme.

Resulting end-state

From the evaluation we arrive in end state ***III.***. End-state ***III.*** represents a shared central database. Xiao et al. already mention that a shared central database can be implemented to store the electronic medical records. However, the results of this evaluation show that the information regarding the data sharing process and data sharing agreements should also be stored in a shared central database. In 4.2.3 we mention several alternative frameworks that could facilitate this. Other alternatives are mentioned as examples in the evaluation of the fourth (4.) question in this section (4.2.4). To conclude this evaluation, looking at the current blockchain based solution in EmrShare we see that there exist a better alternative solutions for this particular use case according to the decision scheme of Koens & Poll.

4.2.5 Evaluation of 3 major impediments; poor scalability, low general performance and high costs

Even tough our evaluation in 4.2.4 shows that a blockchain based solution is not suitable for the EmrShare use case, we try to evaluate the framework against the 3 impediments mentioned by Chukwu and Garg. Unfortunately and cost factor has not been addressed in the EmrShare proposal. Therefore we cannot state how the high cost impediment relates to this use case. As we have mentioned in 3.3.2, the performance of the EmrShare framework has been evaluated on a small scale simulation on AWS [1]. Those test results showed that the response time for queries and transactions in the EmrShare framework increased up to 50% when increasing the number of organisation in the simulation from 2 to 4. Given that these results were obtained from small scale tests future research could evaluate how the EmrShare framework performance is affected on a larger scale. Therefore, it is currently unclear how the EmrShare framework deals with the three impediments.

[1] https://aws.amazon.com/

Chapter 5

Related Work

In this research we have evaluated two blockchain-based use cases against a decision scheme proposed by Koens and Poll [35]. The decision scheme of Koens and Poll can be seen in section 2.2 (figure 2.2). This scheme is based on result of an analysis of 30 existing schemes. One scheme that was analysed by Koens and Poll can be seen in the article "Do you Need Blockchain" [55] by Wüst and Gervais. The downside to using the scheme of Wüst and Gervais is that no alternative data storage technologies are considered. Bartoletti et al. conducted a quantitative analysis of 120 social good projects that use blockchain technology [19]. The scheme of Koens and Poll is mentioned as literature that can be used to determine which blockchain architecture is needed. However, despite that statement, Bartolli et al. use the scheme of Wüst and Gervais [55] to conduct the evaluation of the projects. They give no reason why the scheme of Wüst and Gervais is used over the scheme of Koens and Poll.

To the best of our knowledge, there is no literature that applies the decision scheme of Koens and Poll to a particular use case as is done in this research. However, some authors have used the scheme of Koens and Poll to propose new decision models [32, 21].

Farshide et al. introduced a decision model to aid in the choosing of a particular distributed ledger implementation [32]. They have used the decision scheme of Koens and Poll, and several other schemes, to make the argument that there is a "blockchain platform selection problem" and combined the schemes to create their decision model. They have applied their own decision model to three use cases to determine the most appropriate distributed ledger technology to use in each case.

Belotti et al. proposed a "vademecum", or guide, on when or if to use blockchain, which type of blockchain best fits use case requirements, and how to implement various types of blockchain technology [21]. Their article presented a similar decision scheme to the scheme of Koens and Poll. However, they argue that, compared to Koens and Poll's decision schedule,

their schedule not only includes a set of decision points, but also focuses on the decision points where the reader must compromise between highly correlated features such as cost efficiency and performance.

Besides an evaluation of two blockchain-based use cases we have presented the work of Chukwu and Garg that presented an overview of blockchain-based use cases in the healthcare sector [28]. Since the healthcare sector is one of the sectors subjected to strict data-protection regulations (e.g. the GDPR [11]), it is worthy to note that Mulligan et al. state that a blockchain should not be used to store private information or any other data that may be in conflict with either local or global data-protection regulations [42].

Chapter 6

Future Work

In this research we have used the decision scheme of Koens & Poll (Figure 2.2) to evaluate two blockchain based use cases in the health in the healthcare sector. Within this sector there are strict regulations regarding the storing and handling of personal data as outlined in the General Data Protection Regulation (GDPR) [11]. The GDPR extends to other sectors as well. The GDPR introduces the 'right to be forgotten' stating that an individual has the right to have their personal data removed on request. The decision scheme we have used implicitly takes this into account in the third question (*Need to control functionality?*), but does not link this to compliance with regulations such as the GDPR. Therefore future research could investigate the effect the GDPR and other regulations have on deciding if blockchain technology should be used. Especially in use cases that handle and store personal data. Perhaps this will lead to an extension of the decision scheme that takes the handling of non-transactional and private personal data into account. Another addition that could be put forward by the authors of the decision scheme, is a more nuanced definition of the term *transaction interaction* in the fifth question. It is not entirely clear how to answer this question for non-financial use cases. The authors give an example of transaction interaction between Bitcoin addresses, but do not indicate how this relates to non-financial use cases. Therefore we urge the authors, Koens & Poll, to provide more clarification on how to interpret the term *transaction interaction* and how this question is supposed to be answered for non-financial use cases.

As was already mentioned by Koens & Poll, additional research could also explore the trust implications of using a third party (question 4), and how the concept of trust affects the recommendation of the particular data storage technologies. During the evaluation of the e-Health and EmrShare use cases we have seen that some third parties offer parts of the service that the use cases are trying to implement. This raises the question when the authors of the decision scheme intended question four (*Can you use a*

third party?) to be answered with ***yes***. Should a single third party provide a comparable service for a given use case or can multiple third parties be used together? Should company owned blockchain-based solutions, such as Guardtime's KSI framework, be considered as third party solutions? To address the latter question Koens & Poll could perhaps modify the fourth question to: *Can you use a centralised third party solution?*. In this way the resulting end-state is more in line with the question if the question is answered with yes.

In the decision scheme in 2.2 the authors mention Ripple as an example for a distributed ledger in end-state ***V.***. Ripple provides a solution as a currency transfer system between banks and other payment providers worldwide. Given that such systems are already in place between these financial organisations, we are left with the question when it is acceptable to use these legacy systems as a 'third party system' or when we should use a decentralised system such as Ripple. We therefore ask the authors of the decision scheme to review the fourth question and clarify when and whether decentralised solutions should be used at all over existing third-party solutions.

As we have stated in 3.1, the main criterion in selecting use cases was to look for use cases that were currently being piloted or implemented. From the collection of use cases used in this research we have obtain use cases from the healthcare sector. Future research could extend this to other sectors to evaluate other use cases that are in the pilot or implementation phase.

In the phase of gathering information for the Estonian use case we saw that collaboration between government and private companies within the healthcare sector are possible. Many developed nations have state run healthcare programs with the exception of the U.S.A where healthcare institutions are mainly privatised. Future research could investigate whether there are other governments or private healthcare institutions that are considering or developing blockchain-based solutions for their practices.

The result of the EmrShare use case evaluation showed that a blockchain-based solution is not suitable for that particular use case. We have seen in section 4.2.3 that there are other frameworks that provide comparable services. It was out of the scope of this research to compare the performance of the mentioned frameworks to the performance of EmrShare. The authors of EmrShare performed a small scale analysis of the performance of the framework but do not state how this relates to the performance of current solutions. Future research could compare the performance of the EmrShare framework to these alternative solutions. Perhaps these comparisons show that the EmrShare framework performs better than existing solutions, in which case a counter argument can be made against the results of the evaluation in this research. However, if it is shown that the EmrShare framework performs worse than existing solutions then it shows that there are no benefits in using the EmrShare framwork over current solutions.

Thus far we have evaluated two out of the seven use cases mentioned in section 3.3. We were not able to evaluate the other remaining use cases in the time available for this research. Future work could look at the remaining use cases and evaluate their implementation of blockchain technology.

Chapter 7

Conclusions

In this research we have identified seven use cases of blockchain technology in healthcare that have been classified as in the implementation or pilot phase. For this we have used the work of Chukwu and Garg [28], which provided an overview of current blockchain projects in healthcare. Of these seven identified use cases, we have evaluated two use cases using the decision scheme proposed by Koens & Poll [35]. We first evaluated the Estonian e-Health initiative in section 4.1, after which we evaluated the EmrShare framework in section 4.2.

Out of the seven use cases, the one that is most advanced is the Estonian e-Health initiative. This e-Health initiative uses KSI blockchain to ensure the integrity of medical data of the citizens of Estonia. Despite this being a state-run initiative together with the private company Guardtime, technical details regarding the implementation of blockchain were hard to find and figuring out how blockchain was used in Estonia's *e-Health* use case took more time than expected. This can be explained by the fact that the KSI blockchain used in this use case is eventually owned by a private company. This hindered the access to information. Most of the information describing the usage of KSI blockchain came from sources associated with the company Guardtime, which provides the KSI service. This was inevitable as other presumably useful sources of information regarding the development of Estonian e-health services were written in their native language [15]. This prolonged search for information on the e-Health use case resulted in the inability to evaluate all seven use cases.

Besides the evaluation of the e-Health use case, we have evaluated the EmrShare use case in a similar manner. EmrShare is a framework that allows for the sharing of electronic medical records (EMRs) between healthcare organisations. Based on the literature we've found, we have seen that the EmrShare framework is currently in the early stages of development of a prototype. Therefore we see that Chukwu and Garg wrongly classified EmrShare in the implementation or pilot category. We based our evaluation

of the EmrShare framework on the information provided in the publication that introduced EmrShare [56].

Even though the e-Health and EmrShare frameworks are both use cases in the healthcare sector, the use case frameworks are used for different purposes. If we compare the evaluation process of describing and evaluating the e-Health and EmrShare use cases, we see that, for the reasons mentioned above, we spent more time on the e-Health use case compared to the EmrShare use case. The descriptions of the remaining five use cases are mostly literature based, this is in line with the description of the EmrShare use case. For this reason we expect that the evaluation process of the remaining use cases will take up less time than the evaluation of the e-Health use case.

Keyless Signature Infrastructure The process of researching the use of blockchain technology in the Estonian e-Health use case allowed us to describe the blockchain-based Keyless Signature Infrastucture (KSI) used in this use case. In the KSI framework the KSI s̈ignaturesd̈iffer from traditional digital signatures in the sense that they are based on cryptographic hash funtions (e.g. SHA-256), where as traditional digital signatures are based on public key infrastructure (PKI). The KSI s̈ignaturesc̈an be used to verify the integrity of signed digital data. Compared to existing PKI signature solutions, KSI offers an alternative signature scheme which does not require a trusted certificate authority (CA) to verify the identity of the signers. In KSI trust is placed in signers to manage their own credentials and to a certain extent the communication channels between the users and Guardtime. Compare this to PKI were trust is not only placed signer's ability to manage their keys, but also in the security and validity of CA certificates and on the surface it seems that KSI requires a lower degree of trust. However, given that Guardtime is the company at the centre of the KSI framework, using the KSI framework also comes with the requirement of trusting the security of Guartime's IT infrastructure. Because it was out of the scope of this thesis to provide an in-depth security analysis or research the trust implications of both frameworks, we see that these topics are opportunities for future research.

Evaluation of the e-Health use case. The Estonian e-Health use case was evaluated against the work of Koens & Poll [35] to determine whether or not the use of the type of blockchain is justified. The use of the KSI blockchain used in this use case most resembles a private permissioned blockchain as participants are required to authenticate to Guardtime to use the service and the nodes/servers that update the state of the blockchain are owned by Guardtime. During the evaluation of this use case providing an answer to the fourth question *Can you use a third party?* was not obvious due to the uniqueness of the KSI service as well as the unavoidable

introduction of trust into services of other parties. By using Guardtime's KSI framework we are using a third party, however this third party is not using a shared central database as suggested by the decision scheme. In the end we decided to answer the fourth question with both yes and no and continue evaluating the other questions as there were no third party alternatives that both eliminated the trust placement in an audit service and allowed for independent verification of data integrity.

Determining whether *transaction interaction* was needed in this use case was also not obvious since the Bitcoin example, given by the decision scheme authors, did not apply to this use case. During the evaluation we have answered this question by asking if there is a need for the interaction of stored data within the system, however as mentioned in chapter 6, future research may provide a more nuanced explanation on how to answer these questions in the decision scheme.

In the end, the results show that indeed a private permissioned blockchain in the form of a distributed ledger is a sensible solution for the Estonian e-Health use case.

The work of Chukwu and Garg identified three impediments; poor scalability, low general performance and high cost, that limit the implementation of blockchain-based solutions in the healthcare sector. The Estonian use case was evaluated against these impediments to see how this implementation handled these factors. Poor scalability did not seem to be relevant for KSI blockchain implementation as this technology is able to handle up to 10^{12} signatures per second. The other impediments, the low general performance and high cost, did not hinder the KSI blockchain implementation, as additional analysis has shown a 50% shorter response time and a cost reduction of 20%.

Evaluation of the EmrShare use case. The EmrShare use case was also evaluated against the decision scheme presented by Koens & Poll [35]. We have seen that the EmrShare framework is a private permissioned build using Hyperledger Fabric [56, 17]. The result of the EmrShare use case evaluation showed that a blockchain-based solution is not suitable for this use case. Currently there exist alternative frameworks, outlined in 4.2.3 & 4.2.4, that (combined together) allow for the same functionality that the EmrShare framework offers, without the use of a blockchain-based data structure. For this reason we see that the decision scheme suggests to use a shared central database as data structure for this particular use case.

We were not able to provide a substantial evaluation of the three impediments mentioned by Chukwu and Garg for this use case. To the best of our knowledge there exist no literature that evaluates the cost, scalability and performance aspects for this particular research, besides the small scale performance test results of the paper that introduces EmrShare. Results

from these small scale tests are mentioned in section 4.2.5. How these results relate to other existing frameworks performances is not mentioned by the authors of EmrShare [56].

Evaluation of the decision scheme of Koens & Poll We have seen that the decision scheme of Koens & Poll is a straightforward approach to determine the appropriate database technology to use in a particular use case. However as pointed out by Belotti et al. in chapter 5 [21], the scheme does not focus in on the decision points (questions) itself and does not allow the user of the scheme to make concessions between features such as trust, functionality, cost efficiency and performance that might be relevant for a particular use case.

In the e-Health evaluation we saw that using a third party is not inherent to using a shared central database as suggested by the decision scheme. Therefore is is yet unclear if third parties that offer a blockchain-based service are meant to be considered during an evaluation of a use case. Perhaps a modification to question four in the form of: *Can you use a centralised third party solution?* is more in line with the resulting end-state if this question can be answered with yes. This remark was mentioned in chapter 6 along with other requests for the authors to clarify some definitions in the decision scheme questions and investigate how regulations such as the GDPR affect the outcome of the decision scheme.

The three impediments mentioned by Chukwu and Garg; cost, scalability and performance, made an implicit appearance in the decision scheme in question 8 (*Transaction throughput matters?*) and question 9 (*Store large amount of data?*).

In the end the decision scheme of Koens & Poll can be used as a practical indication tool that can be used to determine which data storage technology is sensible to use for a particular use case, but struggles with giving concrete advice and clarity on how certain questions should be answered if specific (technical) requirements are given.

Bibliography

[1] Definition of: distributed database, Jun 2007. URL https://www.its.bldrdoc.gov/fs-1037/dir-012/_1750.htm. The Institute for Telecommunication Sciences. [Online; accessed 27. Mar. 2020].

[2] Guardtime on R3 and using Corda, Nov 2018. URL https://www.youtube.com/watch?v=a69uyIPsUI0. Interview with Jamie Steiner, General Manager of Financial services at Guardtime, on the decision to use Corda for their development. [Online; accessed 15. May 2020].

[3] HashAlgorithm (KSI SDK 4.15.198 API), Oct 2019. URL https://guardtime.github.io/ksi-java-sdk/com/guardtime/ksi/hashing/HashAlgorithm.html. [Online; accessed 24. May 2020].

[4] Data Access Request Service (DARS) - NHS Digital, Jun 2020. URL https://digital.nhs.uk/services/data-access-request-service-dars. Website of NHS: The national health service of the United Kingdom. [Online; accessed 13. Jun. 2020].

[5] Corda | Open Source Blockchain Platform for Business, Mar 2020. URL https://www.corda.net. [Online; accessed 27. Mar. 2020].

[6] Instantly Move Money to All Corners of the World | Ripple, Mar 2020. URL https://ripple.com. [Online; accessed 27. Mar. 2020].

[7] e-Estonia — We have built a digital society and we can show you how, Apr 2020. URL https://e-estonia.com/. [Online; accessed 6. Apr. 2020].

[8] Security and safety — e-Estonia, May 2020. URL https://e-estonia.com/solutions/security-and-safety. [Online; accessed 16. May 2020].

[9] e-Health Records — e-Estonia, May 2020. URL https://e-estonia.com/solutions/healthcare/e-health-record. The Estonian government e-Health website. [Online; accessed 10. May 2020].

[10] Estonian government information portal | Eesti.ee, May 2020. URL https://www.eesti.ee/en. The Estonian state portal website. [Online; accessed 22. May 2020].

[11] General Data Protection Regulation (GDPR) – Official Legal Text, May 2020. URL https://gdpr-info.eu. [Online; accessed 24. May 2020].

[12] eGovernment — Guardtime, Apr 2020. URL https://guardtime.com/solutions/egovernment. [Online; accessed 11. Apr. 2020].

[13] Keyless Signature Infrastructure – Guardtime Federal, May 2020. URL https://www.guardtime-federal.com/ksi. Website of Guardtime containing basic information about KSI. [Online; accessed 10. May 2020].

[14] Nictiz, Jun 2020. URL https://www.nictiz.nl. Website of Nictiz: A Dutch organisation responsible for digital information exchange in the healthcare sector. [Online; accessed 13. Jun. 2020].

[15] May 2020. URL https://www.tehik.ee. Website of TEHIK: As of 01.01.2017 the Health and Welfare Information Systems Centre (TEHIK) is in charge of the development of Estonian e-health services and providing ICT services under the Estonian Ministry of Social Affairs. [Online; accessed 4. May 2020].

[16] Cornelius C. Agbo, Qusay H. Mahmoud, and J. Mikael Eklund. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare*, 7(2):56, Jun 2019. ISSN 2227-9032. doi: 10.3390/healthcare7020056.

[17] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, pages 1–15, 2018.

[18] Mana Azarm-Daigle, Craig Kuziemsky, and Liam Peyton. A Review of Cross Organizational Healthcare Data Sharing. *Procedia Comput. Sci.*, 63:425–432, Jan 2015. ISSN 1877-0509. doi: 10.1016/j.procs.2015.08.363.

[19] Massimo Bartoletti, Tiziana Cimoli, Livio Pompianu, and Sergio Serusi. Blockchain for social good: a quantitative analysis. *Proceedings of the 4th EAI International Conference on Smart Objects and Technologies for Social Good*, pages 37–42, 2020. doi: 10.1145/3284869.3284881.

[20] Georg Becker. Merkle signature schemes, merkle trees and their cryptanalysis. *Ruhr-University Bochum, Tech. Rep*, 2008.

[21] Marianna Belotti, Nikola Božić, Guy Pujolle, and Stefano Secci. A vademecum on blockchain technologies: When, which, and how. *IEEE Communications Surveys & Tutorials*, 21(4):3796–3838, 2019.

[22] Thomas Bocek, Bruno B Rodrigues, Tim Strasser, and Burkhard Stiller. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE symposium on integrated network and service management (IM)*, pages 772–777. IEEE, 2017.

[23] Ahto Buldas, Andres Kroonmaa, and Risto Laanoja. Keyless signatures' infrastructure: How to build global distributed hash-trees. In *Nordic Conference on Secure IT Systems*, pages 313–320. Springer, 2013.

[24] Ahto Buldas, Risto Laanoja, and Ahto Truu. Efficient quantum-immune keyless signatures with identity. *IACR Cryptology ePrint Archive*, 2014:321, 2014.

[25] Vitalik Buterin et al. Ethereum: A next-generation smart contract and decentralized application platform. 2014. URL https://github.com/ethereum/wiki/wiki/White-Paper. [Online; accessed 31. May 2020].

[26] Lei Chen, Xiao-Peng Mei, Chang-Jun Gao, Gui-He Zhang, and Xu-De Sun. Histologic Distribution, Fragment Cloning, and Sequence Analysis of G Protein Couple Receptor 30 in Rat Submaxillary Gland. *Anat. Rec.*, 294(4):706–711, Apr 2011. ISSN 1932-8486. doi: 10.1002/ar.21349.

[27] Lei Chen, Ji-Jiang Yang, Qing Wang, and Yu Niu. A framework for privacy-preserving healthcare data sharing. *2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 341–346, Oct 2012. doi: 10.1109/HealthCom.2012.6379433.

[28] Emeka Chukwu and Lalit Garg. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *IEEE Access*, 8:21196–21214, Jan 2020. ISSN 2169-3536. doi: 10.1109/ACCESS.2020.2969881.

[29] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10):71, 2016.

[30] Morris J. Dworkin. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Jun 2020. URL https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions. [Online; accessed 7. Jun. 2020].

[31] Benjamin Fabian, Tatiana Ermakova, and Philipp Junghanns. Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*, 48:132–150, Mar 2015. ISSN 0306-4379. doi: 10.1016/j.is.2014.05.004.

[32] Siamak Farshidi, Slinger Jansen, Sergio España, and Jacco Verkleij. Decision Support for Blockchain Platform Selection: Three Industry Case Studies. *IEEE Trans. Eng. Manage.*, pages 1–20, Jan 2020. ISSN 1558-0040. doi: 10.1109/TEM.2019.2956897.

[33] guardtime. libksi, May 2020. URL https://github.com/guardtime/libksi/blob/master/src/ksi/hash.c. [Online; accessed 24. May 2020].

[34] Thomas Heston. A case study in blockchain health care innovation. *International Journal of Current Research*, 9:60587–60588, Nov 2017. doi: 10.22541/au.151060471.10755953.

[35] Tommy Koens and Erik Poll. What blockchain alternative do you need? In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pages 113–129. Springer, 2018.

[36] Tommy Koens and Erik Poll. The drivers behind blockchain adoption: The rationality of irrational choices. In *European Conference on Parallel Processing*, pages 535–546. Springer, 2018.

[37] Jong-Hyouk Lee and Marc Pilkington. How the blockchain revolution will reshape the consumer electronics industry [future directions]. *IEEE Consumer Electronics Magazine*, 6(3):19–23, 2017.

[38] Seo-Joon Lee, Gyoun-Yon Cho, Fumiaki Ikeno, and Tae-Ro Lee. Baqalc: blockchain applied lossless efficient transmission of dna sequencing data for next generation medical informatics. *Applied Sciences*, 8(9):1471, 2018.

[39] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Trans. Parallel Distrib. Syst.*, 24(1):131–143, Mar 2012. ISSN 1558-2183. doi: 10.1109/TPDS.2012.97.

[40] I. Löhmus. Ensuring healthcare system integrity with blockchain. *Zenodo*, Sep 2016. URL https://zenodo.org/record/162707. [Online; accessed 24. Apr. 2020].

[41] Matthias Mettler. Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–3, Sep 2016. doi: 10.1109/HealthCom.2016.7749510.

[42] CJ Mulligan, Z Scott, S Warren, and JP Rangaswami. Blockchain beyond the hype. In *World Economic Forum. http://www3. weforum. org/docs/48423_Whether_Blockchain_WP. pdf. Accessed*, volume 2, 2018.

[43] Gayathri Nagasubramanian, Rakesh Kumar Sakthivel, Rizwan Patan, Amir H. Gandomi, Muthuramalingam Sankayya, and Balamurugan Balusamy. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Comput. & Applic.*, 32(3):639–647, Feb 2020. ISSN 1433-3058. doi: 10.1007/s00521-018-3915-1.

[44] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[45] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. *Business & Information Systems Engineering*, 59(3):183–187, 2017.

[46] National Institute Of Standards and Technology. Secure Hash Standard (SHS). *CSRC | NIST*, Aug 2015. doi: 10.6028/NIST.FIPS.180-4.

[47] Md. Abdur Rahman, Elham Hassanain, Md. Mamunur Rashid, Stuart J Barnes, and M. Shamim Hossain. Spatial blockchain-based secure mass screening framework for children with dyslexia. *IEEE Access*, 6:61876–61885, 2018.

[48] Alex Roehrs, Cristiano André Da Costa, and Rodrigo Da Rosa Righi. OmniPHR: A distributed architecture model to integrate personal health records. *J. Biomed. Inf.*, 71:70–81, Jul 2017. ISSN 1532-0464. doi: 10.1016/j.jbi.2017.05.012.

[49] Chinmay Saraf and Siddharth Sabadra. Blockchain platforms: A compendium. In *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, pages 1–6. IEEE, 2018.

[50] W. Scott Stornetta and S. Haber. How to time-stamp a digital document. *Journal of Cryptology*, 3:99–111, 1991.

[51] Don Tapscott and Alex Tapscott. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.* Penguin, 2016.

[52] Erwin L. van Dijk, Hélène Auger, Yan Jaszczyszyn, and Claude Thermes. Ten years of next-generation sequencing technology. *Trends Genet.*, 30(9):418–426, Sep 2014. ISSN 0168-9525. doi: 10.1016/j.tig.2014.07.001.

[53] Shawn Wilkinson, Tome Boshevski, Josh Brandoff, James Prestwich, Gordon Hall, Patrick Gerbes, Philip Hutchins, Chris Pollard, and Vitalik Buterin. Storj: A decentralized cloud storage network framework, Oct 2018. URL https://storj.io/storj.pdf. [Online; accessed 27. Mar. 2020].

[54] Ruoyu Wu, Gail-Joon Ahn, and Hongxin Hu. *Secure sharing of electronic health records in clouds*. IEEE, Oct 2012. ISBN 978-1-4673-2740-4. URL https://ieeexplore.ieee.org/abstract/document/6450972. [Online; accessed 15. Jun. 2020].

[55] Karl Wüst and Arthur Gervais. Do you Need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54, Jun 2018. doi: 10.1109/CVCBT.2018.00011.

[56] Zhe Xiao, Zengxiang Li, Yong Liu, Ling Feng, Weiwen Zhang, Thanarit Lertwuthikarn, and Rick Siow Mong Goh. Emrshare: A cross-organizational medical data sharing and management framework using permissioned blockchain. In *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, pages 998–1003. IEEE, 2018.

[57] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE, 2017.

[58] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4):352–375, 2018.

[59] Yan Zhuang, Lincoln R. Sheets, Zonyin Shae, Yin-Wu Chen, Jeffrey J. P. Tsai, and Chi-Ren Shyu. Applying Blockchain Technology to Enhance Clinical Trial Recruitment. *AMIA Annu. Symp. Proc.*, 2019: 1276, 2019. URL https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7153067.

[60] Yu Zhuang, Lincoln Sheets, Zonyin Shae, Jeffrey JP Tsai, and Chi-Ren Shyu. Applying blockchain technology for health information exchange and persistent monitoring for clinical trials. In *AMIA Annual Symposium Proceedings*, volume 2018, page 1167. American Medical Informatics Association, 2018.