UiA University of Agder

A User-centered system with blockchain in the Norwegian healthcare: From a security and privacy perspective

SINDRE GJELSTEN
SNORRE BIRGER TUNGE

SUPERVISORS
Jaziar Radianti
Paolo Spagnoletti

University of Agder, 2020
Faculty of Social Science
Department of Information Systems

Master

Preface

This master thesis was written in connection with the master course IS-507 from Faculty of Social Sciences at the University of Agder. The thesis was written between January and June 2021.

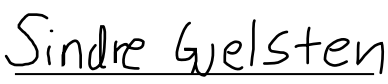
The IS-507 course offers the possibility to work with a specific subject of choice or specific task from a company in the cybersecurity sector. After conducting the research and writing the thesis, we have gained a better understanding of applying theoretical knowledge to a specific problem. In addition, we learned to develop a design study and evaluate our own design based on prior research. The purpose of this thesis is to propose a more user-centric healthcare system in the Norwegian IT domain.

We want to extend a big thank you to our supervisors: Jaziar Radianti and Paolo Spagnoletti from the Institute of Information System at the University of Agder. Their guidance and expertise have been very valuable, and the continuous feedback was unprecedented.

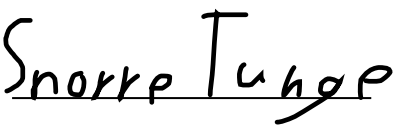
We would also like to thank everyone who participated in interviews, which gave us much needed information and data for the thesis. The data we collected, supplemented with other sources, resulted in a more holistic thesis.

Kristiansand, 3rd of June 2021.

Sindre Gjelsten



Snorre Birger Tunge



Abstract

With the current Covid-19 pandemic roaming the world, the IT attacks on the healthcare sector has increased five folds from 2019 to 2020. The Norwegian healthcare system is divided into different regions with their own systems respectfully. This fragmentation causes great communication issues between systems and exposes the transmitted data for attacks. To better combat this situation and improve upon the fragmented healthcare systems, a restructure is needed. In this thesis we explore the possibility of using blockchain technology as the foundation of a system that unifies the systems in the Norwegian healthcare sector. We adopt a Design Science Research approach to propose a blockchain-based architecture to solve the problem. Interviews with IT professionals in the Norwegian healthcare sector gave us their opinion about implementing blockchain and how the current systems are structured. Scalability was a common issue that different papers cited. There were multiple proposed solutions for this issue, but none seem practical for implementation today. It continues to be a difficulty and is one of the biggest reasons why we see hesitation in parts of the relevant sectors. Of course, blockchain has its upsides as well. Improved security and privacy with immutable ledgers make the system better suited for an increasingly exposed IT sector. It also provides a stronger availability since the same information is distributed between different nodes which take away the single failure point of regular database systems. The result from our evaluation of our proposed system is that it provides great user experience, increased security and privacy and better availability. Unfortunately, the benefits in these areas compared to the current systems are rather slim. Blockchain also introduces some performance penalty for smaller systems and scalability issues when the system becomes too large (with reference to storage and processing power). The conclusion is that a blockchain based healthcare system is better, but the amount of money and effort required to restructure the current system is too high and the demand for increased security is still too low. A more unified version of the current system could see good results, even without using blockchain.

Table of content

List of Figures

List of Tables

List of Abbreviations

ACL	Access Control List
AES	Advanced Encryption Standard
APT	Advanced Persistent Threat
BUC	Blockchain User Centric
CA	Certification Authority
CDA	Clinical Document Architecture
DBMS	Database management system
DDoS	Distributed Denial-of-Service
DSR	Design Science Research
DLT	Distributed Ledger Technology
DNS	Domain Name System
EBSI	European Blockchain Service Infrastructure
ECC	Elliptic Curve Cryptography
EEA	European Economic Area
E.g.	Exempli gratia (For example)
EHR	Electronic Health Record
EU	European Union
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation
GP	General Practitioner
IoT	Internet of Things
IPFS	Interplanetary file systems
IT	Information Technology
IV	Initialization Vector

MHMD	My health My data
MITM	Man-in-the-Middle
NFC	Near-Field Communication
OECD	Organization for Economic Co-operation and Development
P2P	Peer-to-peer
PBFT	Practical Byzantine Fault Tolerance
PI	Personal Information
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PoA	Proof-of-Activity
PoET	Proof-of-Elapsed-Time
PoS	Proof-of-Stake
PoW	Proof-of-Work
PPPoS	Permissionless Pure Proof-of-Stake
RNB	Random Number Generator
RHF	Regionalt Helseforetak
SLR	Systematic Literature Review
SSL	Secure Sockets Layer
TRL	Technology Readiness Level
UCD	User-Centered Design
UI	User Interface
UX	User Experience
WHO	The World Health Organization

1 Introduction

1.1 Research Background

With the Covid-19 pandemic currently (2021) roaming the world, the importance of healthcare is at an all-time high. Cyber criminals use this opportunity for their own gains. The World Health Organization (WHO) reported that there is a 5-fold increase in cyber-attacks during the spring of 2020 compared to 2019 (WHO, 2020) This shows the ruthless mindset cyber criminals have by preying on the weak during a pandemic. Kaspersky also reported a need for more reliable healthcare infrastructure (Namestnikova, 2020), not only to coordinate between hospitals, but also for facilitating medical research. As researchers worked hard to find a vaccine for the Covid-19 virus, cyber criminals went a different route by trying to steal such information from other vaccine companies. Ransomware has typically been the biggest threat to the healthcare sector but has now become more targeted. Namestnikova reported that certain known hacker groups chose to not pursue medical organizations with ransomware (Namestnikova, 2020, para. 4). Not everyone has the same mindset. In a report from unit 42 (Paloalto Networks, 2021, para. 5-6), healthcare facilities were the most targeted sector for ransomware in 2020. The reasoning was that “these types of organizations knowing that they couldn't afford to lose access to critical data as they sought to conduct research into COVID-19 and help patients afflicted with the virus” (Whitney, 2021b, para. 3). In addition, the increase in ransom paid was up by 171% in 2020 compared to 2019.

In Norway, as with other countries, the IT infrastructure of the healthcare sector is the backbone for its operations. However, some systems in the Norwegian healthcare sector are lagging behind (Øyvann, 2018) when it comes to certain aspects such as user-centered systems, security, and unifying the different systems into fewer, more manageable systems. User-centered is inspired from “User-centered design” (UCD) (Spagnoletti & Tarantino, 2013). This is a design which focuses on “involve users throughout the design process[...], to create highly usable and accessible products for them” (Interaction-design, Unknown, para. 1). In this thesis the term “User-centered” will mean to design a system which not only gives the user more control over their data, but also improves usability, accessibility and interoperability. For this thesis patients are considered the users. Currently in Norway there is a small amount of data that is available for the user. The purpose of Helsenorge’s website is to “give patients or relatives a better and easier way to deal with healthcare services, and help them better their understanding, make the patient’s role more important, and improve the patient’s health” (Helsenorge, 2020, para. 6). The terms of use on Helsenorge’s website (Helsenorge, 2018, p. 2) gives information regarding what data users have access to, and what they can do with that data. This data includes the following:

- Social security number
- What consent the user has given

- Information the user has provided
- Log In times, and what services has been accessed
- General information, such as name, age, sex, etc.
- Who the user's general practitioner is

In Norway, healthcare is provided by the Norwegian Government. The healthcare system started as a single entity but has now expanded to four regions. Each of the four systems are isolated from each other, to give the individual regions more control. The problem occurs when doctors need to exchange journals between hospitals and local offices. This sounds like an easy process, but due to security and privacy concerns it is quite a time consuming and complex process. Each journal must be exported out from one system and then imported into the desired system. We can view this as the difference between international mail shipping and domestic. With international shipping, you must go through customs and extra controls because it crosses borders and different mailing systems. The systems in use by the healthcare service need to endure pressure, not only in a capacity manner, but also when it comes to security.

This thesis will use Norway as a case when looking at the possibility of unifying the systems in the Norwegian healthcare sector, and the benefits and downsides of using blockchain technology to achieve this.

Blockchain will be a focal point in this thesis and will be used as the desired technology in the proposed system. It is a hot topic today within cybersecurity research. Blockchain is a promising "new" (2008) technology which was initially developed to achieve decentralization while maintaining privacy and security in the cryptocurrency domain. It has now spread into other domains such as the healthcare system where it helps with improving security and privacy issues with its immutable ledgers. Blockchain also has practically 100% uptime which is a requirement for healthcare facilities. In the US, Big Pharma[1] is experimenting with blockchain in their supply chains. Their reasoning is "competitors can collaborate on a shared platform without sharing sensitive information" (McCauley, 2020, para. 6). This allows them to trace the provenance of supplies, verify their status, and reduce friction throughout the supply chain. Mainly there are two blockchain technologies which are used in such applications. These are the **Ethereum** blockchain and the **Hyperledger** blockchain. Recently a new blockchain technology called **Algorand** has emerged.

Previous research has sought to improve both the security in Electronic Health Record (EHR) with blockchain technology and improving the user interaction (ownership) of the data. The problem is that these have been conducted in an isolated manner and their solutions are not displayed as a holistic system. This sparks the idea for a complete overhaul design of the infrastructure in the healthcare system. At the core

[1] Big Pharma means a collective of pharmaceutical companies.

are the values of user centricity, more complementary EHR, improved security and a more streamlined system for every healthcare provider.

While previous research has looked at using blockchain technology in many ways, there are those who are skeptical about implementing the technology. Being critical and asking questions regarding the validity and necessity of using blockchain is important. Therefore, it will be important to gather information about and discussing if implementing a newer technology in blockchain is something worth pursuing or not.

The scope of this thesis is limited to the systems in Norwegian Healthcare and their current state. In addition, it will look at a new, proposed design which focuses on a more user-centered approach to improve aspects in usability, placing ownership of the data in the users' hands, utilizing blockchain technology to improve security, privacy, ease of use of EHR in the healthcare domain and looking at the validity of blockchain technology in the Norwegian healthcare sector.

1.2 Research Goals

Based on the current Norwegian healthcare status described in the introduction we wish to present research goals instead of research questions. The goal is to investigate the impact of utilizing blockchain in the Norwegian healthcare sector. In addition, we want to design a system which increases the user experience and gives the user more control over their own data. To achieve these research goals, we employ a Design Science Research approach. The potential opportunities which blockchain can provide to such a system are many. Immutable ledger and strong encryption help to improve security and privacy and it can help with uptime since the blocks are stored at different servers (nodes) at the same time. With all the security issues which could arise and the current escalations of cyberattacks, it seems to be a good time to investigate new technologies which can improve in these areas. To yield greater benefit to the current Norwegian Healthcare system which is currently divided into four parts and require special export-import protocol to share data between regions, a complete system design for the entire healthcare sector will be proposed. One last thing regarding a user-centric system and third-party applications. This is a lacking area in the current system. Based on these lacking areas, we have arrived at some specific research goals:

RG1 What are the opportunities and hindrances of blockchain in the Norwegian healthcare system regarding security, privacy, and performance?

RG2 How could a user-centered system be designed in relation to third-party applications and privacy?

1.3 Thesis Structure

The thesis has the following structure: chapter 2 contains related work with security issues, background theory in blockchain, Encryption Key generation, AES and prior research findings. Chapter 3 describes the methodology and background used for the design science research, interviews and SLR. The SLR section displays how relevant studies were gathered and how the number of papers were narrowed down based on certain criteria. Chapter 4 presents the proposal of a user-centered system with all the relevant features and solutions. Chapter 5 evaluates the proposed systems from a theoretical and descriptive standpoint. Chapter 6 discusses the evaluation of the system, the current situation of healthcare and pandemic, the necessity for such a system, the contributions and limitations of this thesis. The chapter also tries to answer the research goals asked in chapter 2. Finally in chapter 7, a conclusion is presented regarding the system and its future.

2 Related works

This part of the thesis will present the relevant theory to the user-centered system to give a better understanding of the technology and the terms used in the thesis. The topics that will be touched on are security, blockchain, smart contracts, public key infrastructure, advanced encryption standard and prior research data in the related topics.

2.1 Privacy and security mechanisms

The theoretical background sub-chapters provide relevant background information about the technologies which will be utilized in the proposed system. The sub-chapter also covers common security issues which are relevant to such a system.

2.1.1 Security issues

With the increased cause for concern regarding cyberattacks, this section will introduce some typical attack methods. These methods are specific for communication between two systems or entities. “Data in transit describes data that is sent over a network (cellular, Wi-Fi, or other networks) or is located in the RAM” (Mullen, 2017). One can say if data is being moved from one place to another, it is considered data in transit. During transit, the data is exposed to malicious actors. Below are some well-known techniques:

- Man-in-the-Middle (MITM) attack
- MITM SSL attack
- Domain Name System (DNS) spoofing attack
- Baseband Attack

All these attacks have one thing in common; their objective is to retrieve the data that is being transmitted. Therefore, it is important to understand that security involving data in transit is crucial. The healthcare sector could benefit from better interconnection between systems It can be beneficial for conveniences and possible time critical tasks and communication. But the more data that is being transmitted, the bigger the risk is for it to get intercepted. In the current system data must be exported and imported between systems. This exposes it to the dangers of the above-mentioned attacks. But with a unified system utilizing strong security measures (such as blockchain), the data can be shared in a safer manner.

According to Sardi, Rizzi, Sorano, and Guerrieri (2020, p. 8), there is poor attention in the scientific community to cyber risks in health facilities (except from the United States). Current medical IT infrastructure is aging and with the increase in interoperability demand, one needs to look at new options.

Blockchain has been in the wind lately with its benefits regarding security and privacy. This makes it seem like blockchain is a good investment, because improvement in these areas is one of the focal points for a system managing data of high importance and privacy. But as with everything, there are drawbacks. These drawbacks will be discussed later in the thesis, but to understand how blockchain works, we must dive a little deeper into the technology.

2.1.2 Blockchain

Blockchain was popularized with Bitcoin by Satoshi Nakamoto in 2008 (Nakamoto, 2008). The technology is a form of distributed ledger technology (DLT) with a list of records stored in a giant 'database'. These databases are formed by multiple connected devices (Memon et al., 2018, para. 1). Each entry in the ledger is called a 'block'. The block is composed of messages and transactions which are linked and timestamped with cryptographic hashes (Nakamoto, 2008, p. 2). Each block needs consensus from the other members of the blockchain to be approved and added to the blockchain. As seen in figure 1, blockchain uses a SHA-256 algorithm and an initialization vector (IV) to encrypt block 1. The next block will be encrypted with a hash value from the output of block one. (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016, p. 10). This continues and creates a chain. The benefit of the chain is if any information is altered in one of the blocks, the following blocks will be rendered useless as the hash values no longer match. It will make it easy to discover if anyone has manipulated the data.

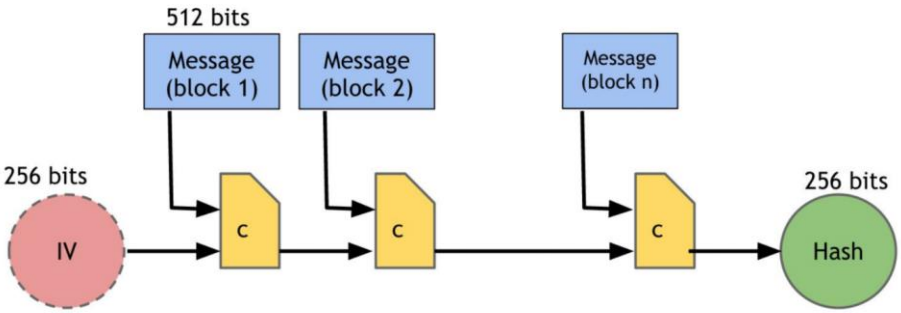


Figure 1: SHA-256 Hash function (Narayanan et al., 2016, p. 10).

In figure 2 we can see the chain in a bigger perspective. This shows that the previous hash is used in the next block and it continues to create a chain. Also note that a block contains a header and a data partition.

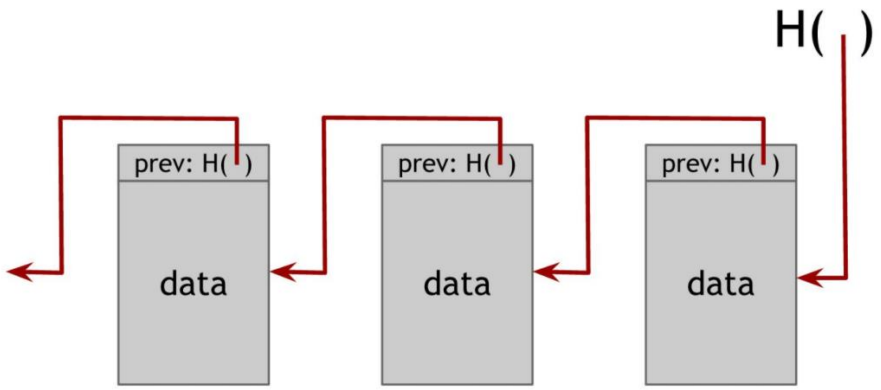


Figure 2: Blockchain (Narayanan et al., 2016, p. 11).

Blockchain can also utilize a technique known as Merkle Tree (Qureshi, 2019). In this technique, blocks are paired up to form a data structure of two hash pointers, one pointer to each block. The pointers then split up and point to two new pairs of blocks (of two blocks). Looking at it, we can see it resembles a tree where the blocks are leaves and it continues up the branches until it reaches the root (master block). Figure 3 illustrates the concept of Merkle tree. This increases the efficiency of blockchain storage.

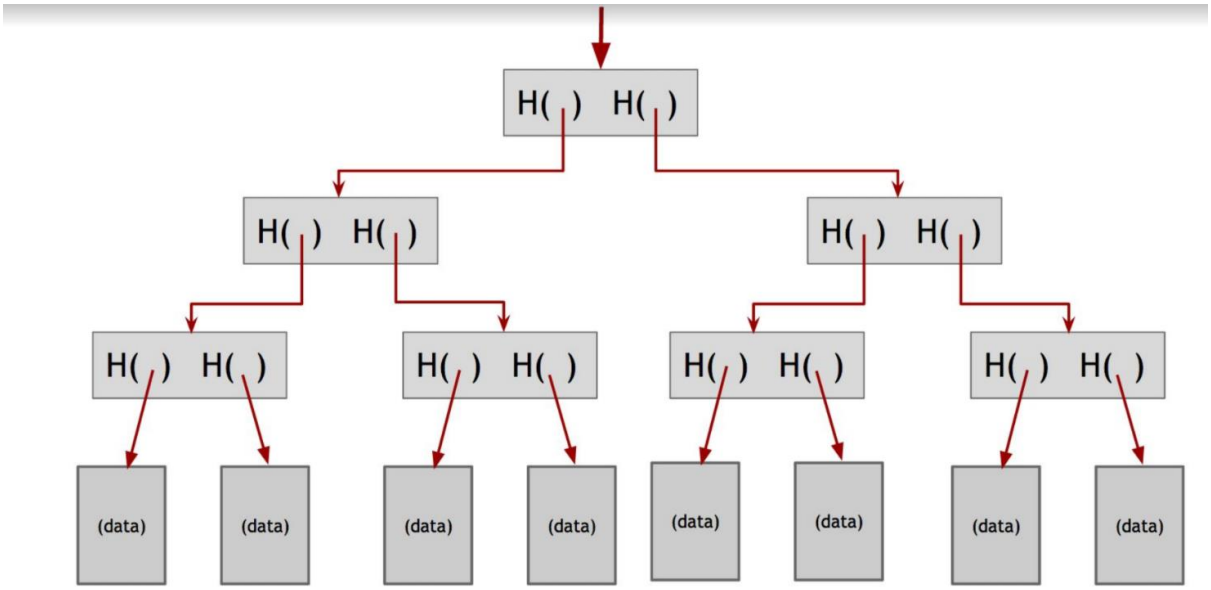


Figure 3: Merkle tree (Narayanan et al., 2016, p. 13).

Blockchain can often be categorized by its type. This is based on how the network members reach consensus and validate transactions or what platform they run on. If it is classified by type, a blockchain network can be public, private or a consortium. Each has their own benefits and drawbacks.

Public Blockchain is the most common one, because it is used for cryptocurrency and the Ethereum blockchain. Public blockchain allows anyone to join the network. It also often utilizes Proof-of-Work (commonly known as mining). The mining causes the users to feel incentivized to improve the system. Smart Contracts are also an important

feature as it solves the issue of trust between two parties by guaranteeing the deliverance of an item.

Private Blockchain is a restrictive blockchain which operates on a closed network (Sharma, Unknown, para. 8). This type of network would be centralized because only one entity controls it. Typical use would be internal within an organization. Hyperledger Fabric is an example of a private blockchain.

Consortium Blockchain is a hybrid of public and private blockchain. It is an invite only blockchain, but it has several in-charge entities. The different entities have therefore the possibility to agree together on what information is accepted on to the blockchain. This is done through a consensus mechanism. Typically, the consensus mechanism is different from public blockchains, since the required trust is lower and a faster performing, lower power consuming consensus mechanism is preferred. Consortium Blockchain helps keep the decentralization alive by having multiple entities deciding together but is not as decentralized as a public blockchain.

Table 1: Advantages and Disadvantages of Blockchain Classification

Public		**Private**		**Consortium**	
Pros	Cons	Pros	Cons	Pros	Cons
-Trustable & transparent. -No intermediaries -Secured	-Scalability issues -Poor transaction speed -Consume a lot of energy	-Higher transaction speed -Very scalable	-Less Secure compared to public blockchains -less decentralized -Hard to achieve trust	-Suited for organizational collaboration -Good scalability and security -More efficient compared to Public -Better customizability and control over resources	-Less transparent -Least anonymous compared to other blockchains

Table 1: Advantages and Disadvantages of Blockchain Classification

Blockchain can also be classified by how the members of the network reach consensus. There are many different categories, but all of them fall under two categories; proof-based and vote based. In figure 4 one can see a number of different consensus algorithms (Chukwu & Garg, 2020, p. 3).

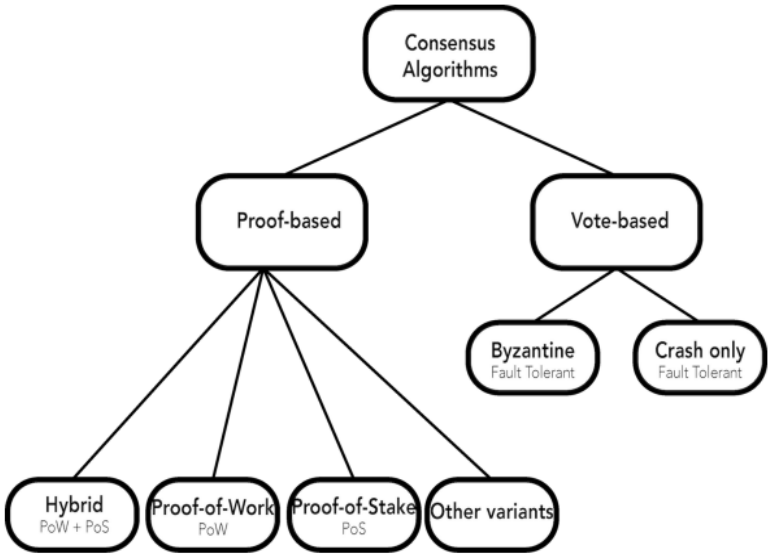


Figure 4: Blockchain consensus algorithms (Chukwu & Garg, 2020, p. 3).

Proof-of-Work (PoW) is the most common consensus mechanism. It is a method which is very labor intensive, but very easy to verify. The mechanism works by having a puzzle which each node tries to solve. This puzzle is connected to the previous block and a node provides a string. When combining these two strings together and hashing them the goal is to come up with a new hash string. In bitcoin the new string is required to have 40 zeros in the beginning of the hash. It means that miners have to try different solutions with the two strings until they find the correct one which starts with 40 zeros. This gives the puzzle 2^{40} different possibilities (Ramzan, 2013, timestamp 6 min). When a node finds the correct hash, it will be incentivized. The new hash will be used in the next block on the blockchain, and the process starts again. Because this consensus mechanism is labor intensive, it is not good for performance, scalability, or power consumption, but is good for when the nodes do not trust each other.

Proof-of-Stake (PoS) uses a different approach to "mining". Instead of having homogenous mining power between all nodes, PoS gives more power the bigger stake in the currency someone owns. It makes it more proportional when it comes to mining pools (which are very common with PoW) and PoS requires less power consumption compared to PoW (Frankenfield, 2021, para. 7). PoS can also suffer from a *nothing-at-stake* problem. This is where nodes validate multiple conflicting copies of the blockchain since there is minimal cost of doing it. There is also a small chance of missing rewards by validating a block on the wrong chain. This issue will cause a "double spending" problem (Saleh, 2020, p. 28). It is possible to mitigate these issues and PoS is considered more secure than PoW from miners who attack the network. Because the miners themselves own a stake in the network, they would attack themselves. PoS sees very little use, but the Ethereum blockchain has started to experiment with it and its popularity continues to increase.

Proof-of-Authority (PoA) works with having validator nodes which are authorized by the network. These validator nodes approve which blocks are accepted to the blockchain and which are rejected (Vorotnikov, 2015). This helps with removing any need for mining, but it decreases the decentralization. It also improves performance, scalability and power consumption compared to PoW. The danger of this is if the nodes are controlled by one entity. This entity controls what is accepted on the blockchain. If all validator nodes are controlled by different entities, the decentralization is increased as no single entity controls all the nodes. The upsides of performance, scalability and power consumption is still present. This consensus mechanism is best suited for a private blockchain network.

Proof-Of-Elapsed-Time (PoET) uses a lottery system to hand out mining rights. It uses randomly generated elapsed time to decide which node wins the mining lottery. PoET runs on a permissioned network, which obligates the nodes to identify themselves and be verified before joining. The consensus mechanism causes an enhancement in transparency by ensuring lottery results are verifiable by external participants (Frankenfield, 2020, para. 1). PoET works by having each node in the network wait for a random chosen time period. The first node to complete the designated waiting time wins the next block. During the wait, each node is put to sleep to save power. The one who wakes up first wins the lottery and commits a new block to the blockchain. After that, it broadcasts the necessary information to the other nodes and the process starts over again (Frankenfield, 2020, para. 4).

Practical Byzantine Fault Tolerance (pBFT) is a bit different as it is a vote-based consensus mechanism. It works with 5 steps (Medium, 2019, para. 4): First the user sends a transaction to the primary. In the next step the primary produces a proposal containing the transactions and forwards it to the nodes. When the nodes receive the proposal, the backups will verify it. If this is successful, they will broadcast the message to all other nodes. If the verification fails, the backups do nothing. This was the first round of voting. When ⅔ of the prepared messages are received, the nodes will broadcast a commit message. This is the second round of voting. After this, the block has been approved to the chain and is visible for everyone in the network. The whole step process can be seen in figure 5.

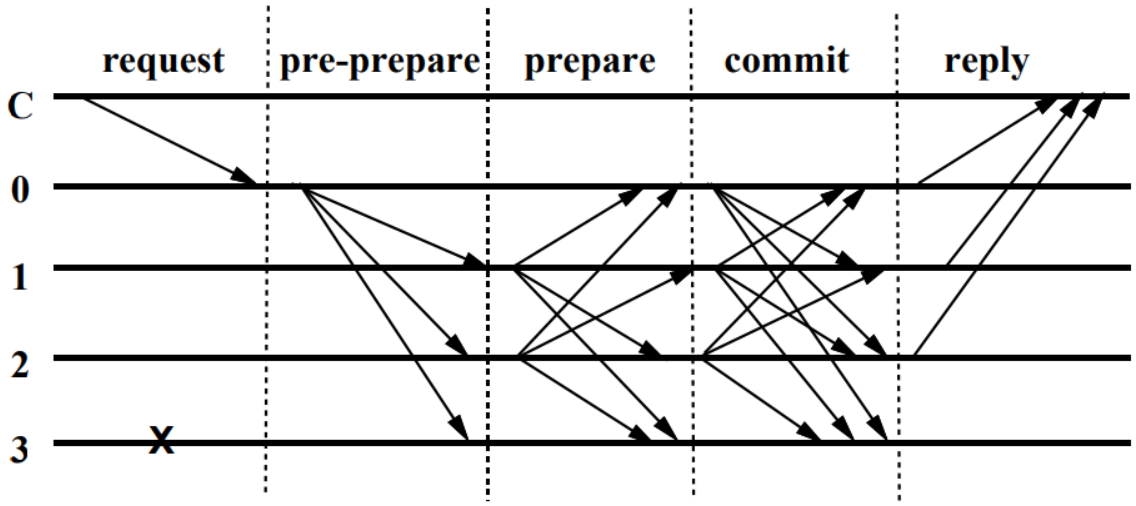


Figure 5: pBFT steps. 0 = primary, 1 = backup 1, 2 = backup 2, 3 = backup 3. These are considered nodes (Miguel Castro, 1999, p. 5)

pBFT has a ⅓ fault tolerance and 2 rounds of voting. It makes it quite secure within a trusted network. It also is very fast compared to a proof-based consensus mechanism. A major downside with pBFT is the number of messages which gets stored from the voting process (Sheffield, 2018, para. 2).

Table 2: Comparing advantages and Disadvantages of Blockchain Consensus Models

	PoW	PoS	PoA	PoET	pBFT
Pros	-No need for trust -Everyone can help -Random	-More proportional (own more = bigger chance to mine next block) -Regarded more secure than PoW	-Highly scalable -Less power consumption (compared to PoW) -Faster	-Smaller power consumption -Random (partly decentralized)	-Fast -Vote based -Trustable -Small power consumption -Decentralized
Cons	-Slow -High power consumption -Incentives are required -Low scalability	-Exposed to *nothing-at-stake* -Requires incentives	-More centralized	-Not particularly fast -Permissioned network	Exponentially increasing message count
Suited network	Public Network	Public Network	Private network	Permissioned network	Consortium network

Table 2: Comparing advantages and Disadvantages of Blockchain Consensus Models

Blockchain also has some unique privacy related features. One of these features is **homomorphic encryption** which allows for analyzing encrypted data. In essence it means that only the intended people can view the data, while for everyone else the data appears obscured. This can be beneficial for the healthcare sector and for privacy because the Personal Identifiable Information (PII) is not exposed using this encryption, but data can still be used (Marr, 2019, para. 3). **Zero-Knowledge proof** is an authentication mechanism which confirms a secret without providing the key or password (Hackernoon, 2020, para. 1). The title explains the concept with zero knowledge of information being exchanged, but the proof shows that both parties know the secret. A good reason to use this mechanism is, for example, when trust has not been established between two parties, but a proof is needed that both parties know specific information. This is possible using zero-knowledge proof. **Interplanetary file system** (IPFS) is a file sharing system which is used to store and share large files more effectively. This is one of the core experiences of blockchain because it is an algorithm to share and retrieve data from the nodes. It tries to get the information from the closest nodes instead of the furthest away ones (IPFS, Unknown, para. 4).

The next section explains some different blockchain technologies which are currently being used by different entities (mostly cryptocurrency).

Hyperledger fabric (IBM) is primarily a public blockchain, but it also offers private blockchains which can interact with the public blockchain if needed. The private blockchain will offer privacy for the data which is stored there. Hyperledger is not an open, permissionless system, but it is a scalable and secure platform which supports private transactions and confidential contracts (Hyperledger, Unknown, p. 1). The Hyperledger fabric is intended for developers and enterprises to utilize their blockchain framework. Because the blockchain is modular, it is often fast to get started and it satisfies a broad range of industry use cases (Hyperledger, Unknown, p. 1). Hyperledger operates on a permissioned voting-based consensus mechanism. Since the environment is partially trusted (permissioned network), they utilize this higher performing lottery-based consensus (Kumar, 2018, para. 6).
Ethereum is primarily a public cryptocurrency and operates as such, but they offer developers to utilize their technology to create their own Ethereum blockchain network. Ethereum has built in utilization of IPFS, which helps with larger files. A problem with Ethereum is their vast storage use. Their current system is at 350GB, which means that each node has to store 350GB of data (Ethereum, 2021, para. 2). Every user must store the 350GB of data as they represent a node each. If healthcare is added on such a technology, the storage demand can be astronomical. A private version based of the Ethereum blockchain is called Storj DCS (Decentralized Cloud Storage) (Storj-DCS, Unknown). Storj DCS encrypts all data uploaded to the blockchain by default. It is then split into 80 pieces and distributed across over thousand nodes in over 100 different countries. The good part of this system is that it only requires 29 nodes to rebuild your file. This means that a big outage of multiple nodes will not affect the network (Storj-DCS, Unknown, para. 4).

Algorand is a cryptocurrency that uses a consensus mechanism called Permissionless Pure Proof-of-Stake (PPPoS), which allows for around 1000 transactions per second. In comparison, Bitcoin manages 5 transactions per second and Ethereum manages 15-30 (Phillips, 2021, para. 8-11). With how lacking a lot of blockchain technologies are when it comes to scalability, the ability to process many transactions per second makes Algorand appealing. The main focus of the technology is in regard to the financial sector, but it could also be useful in the healthcare sector, where handling information regarding a lot of people over a short amount of time could be very beneficial. Algorand offers a public permissionless and decentralized blockchain. Anyone can join, generate blocks and read every block (Algorand, Unknown, para. 1). Since public blockchain is not always the best suited regarding sensitive information, Algorand has developed something called “co-chain”. This is a private permissioned blockchain which provides rigorous controls which organizations typically look for (Micali, 2020, para. 3-5). It can still interact with the public Algorand blockchain as a part of a layering system. Anything in layer 1 is public and can be interacted with, but layer 2 is private. The co chain is “totally independent from the public chain, shields its transactions from all outsiders, chooses its own validators, and runs its own Algorand consensus algorithm”(Micali, 2020, para. 3).

2.1.3 Smart contracts

Smart contracts enable the possibility to use scripts (self-executing code) on the blockchain network. This facilitates the negotiation, verification, execution and enforcement of contracts without the need for a third-party verification (Chukwu & Garg, 2020, p. 3).

Using smart contracts makes the exchange between two parties, automatic. It is possible to use conditions that need to be met, and once they are met the result of the agreed upon contract will take place. IBM presents four benefits of using smart contracts.

1. Speed, efficiency and accuracy
2. Trust and transparency
3. Security
4. Savings

Speed, efficiency and accuracy:
Smart contracts allow for automation of the signature process of contracts, which will make the entire process much faster compared to having a third-party look through the contract and sign off on it.

Trust and transparency:
Some of the properties of a blockchain creates a lot of trust when it comes to smart contracts. This claim of trust is supported further by removing the need for a third-party to be involved in the process.

Security:
“Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.” (IBM, Unknown, para. 3)

Savings:
Because smart contracts take away the need for a third-party to handle the contracts, and because they allow for the possibility of automation, the cost of approving these contracts can, and will in most cases, reduce the overall cost of contracts (IBM, Unknown, para. 3).

An example of how smart contracts can improve a system is voting in an election. With the immutable property of blockchain, it makes it difficult to alter the contents of the blocks. In an election, votes which are stored in the blockchain, will remain anonymous to the public, but each user has a unique ID. The smart contracts would be an automated and secure way of handling each individual vote.

2.1.4 Public Key Infrastructure

Encryption is vital to keep data hidden from others. As the proposed system in this thesis will be “invite only”, all the members can view the data on the blockchain there. Even though they might not be able to connect who it belongs to. To help increase privacy, encryption for off-chain storage of certain sensitive data will be used. This information can be shared with medical personnel, but the user will manage the keys to view the data.

Public Key cryptography uses a pair of keys to encrypt and decrypt content. The pair consists of a private key and a public key. These keys are mathematically related. They work by allowing data to be encrypted using the public key, and then decrypted the data using the private key. A simplified example of this would work can be seen below from Microsoft:

1. “Both Bob and Alice have their own key pairs. They have kept their private keys securely to themselves and have sent their public keys directly to each other.
2. Bob uses Alice's public key to encrypt the message and sends it to her.
3. Alice uses her private key to decrypt the message” (Microsoft, 2018, para. 1).

This simplified example shows an obvious concern which Bob must have about the public key he used to encrypt the message. The concern is that Bob cannot with certainty know that the key he used to encrypt, actually belonged to Alice. It is possible that the key got substituted by a 3rd party, who monitored the communication between Bob and Alice. This is where Public Key Infrastructure (PKI) comes in. The PKI consists of software and hardware elements which are signed by a trusted third party. This helps in maintaining integrity and ownership of a public key. These trusted parties are called a *certification authority* (CA) and they accomplish this by giving out signed binary certificates that confirm the identity of the users. It also binds the identity to the public key, so it takes all doubt out of the equation. CA manages to sign the certificate by using its own private key. Then it sends the corresponding public key to all parties in a self-signed CA certificate. The previous example has will look more like this with the CA involved:

1. “Assume that the CA has issued a signed digital certificate that contains its public key. The CA self-signs this certificate by using the private key that corresponds to the public key in the certificate.
2. Alice and Bob agree to use the CA to verify their identities.
3. Alice requests a public key certificate from the CA.
4. The CA verifies her identity, computes a hash of the content that will make up her certificate, signs the hash using the private key which corresponds to the public key in the published CA certificate. The CA then creates a new certificate by concatenating the certificate content and the signed hash. The new certificate is then made publicly available.
5. Bob retrieves the certificate, decrypts the signed hash by using the public key of the CA, computes a new hash of the certificate content and compares the two hashes. If the hashes match, the signature is verified and Bob can assume that the public key in the certificate does indeed belong to Alice.
6. Bob uses Alice’s verified public key to encrypt a message to her.
7. Alice uses her private key to decrypt the message from Bob.” (Microsoft, 2018, para. 3)

This process enables Bob to verify that the public key was not tampered with or substituted with another key. The CA hashes the content, signs the hash with their own private key and includes the encrypted hash in the certificate. Then Bob can verify the content by decrypting the hash with the public key and comparing the two hashes (one from the CA and one he made from the content). Bob can be very confident that the content has not been altered with if the hashes match (Microsoft, 2018, para. 4).

2.1.5 Advanced Encryption Standard

Advanced Encryption Standard (AES) is an encryption method developed by two Belgian cryptographers; Vincent Rijmen and Joan Daemen (Lake, 2020, para. 11). It takes blocks of 128-bits and divides these bits into a four-by-four columns, where each cell is a byte (ComputerPhile, 2019). In the example below, “Love Blockchain“ is used, where each letter and the spaces are a byte long.

L		C	A
O	B	K	I
V	L	C	N
E	O	H	

After the four-by-four grid has been made, it goes through 5 steps which are repeated dependent on the key size. For a 128-bit key, the whole process is repeated 10 times. AES also has the option of 192-bit key and 256-bit. These perform 12 and 14 rounds respectively. The steps are shown in figure 6, but they consist of:

1. Add Round Key
2. Substitute Bytes
3. Shift Rows
4. Mix Columns
5. Add Round key

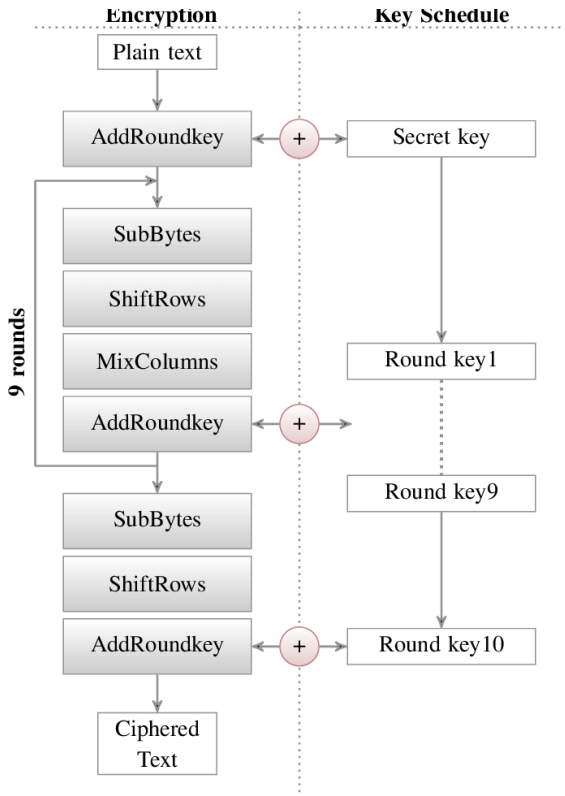


Figure 6: AES encryption steps (Shahid, Chaumont, & Puech, 2013, p. 5)

In this example, we will use a 128-bit key. The key is expanded using the Rijndael Key Schedule. This algorithm takes the original key and creates multiple unique subkeys of different lengths. The subkey named round key in the diagram.

Step 1: The key is XOR’ed[2] with the plaintext to begin with. It is important to note that AES does not utilize regular XOR (Addition and Subtraction), but also Multiplication

[2] XOR is a digital logic port. It will output TRUE (1) if the number of inputs are odd. (E.g 0 and 1 = 1 while 0 and 0 = 0)

and division. It also uses the Galois Finite field to scramble data easily and effectively (Benvenuto, 2012, p. 2).

Step 2: All the bytes are substituted with another byte from a lookup table. The only two rules are: no byte is substituted with the same byte (E.g., 1010 is not replaced by 1010) and there are no opposite replacements (E.g., 1010 is not replaced by 0101). Since this step utilizes a lookup table, it is swiftly executed.

Step 3: Shifting rows is not scrambling of the rows, but to byte shift row 2, 3 and 4. Row 1 remains unchanged, while the bytes in row 2 are shifted 1 step to the left. Row 3 will shift 2 steps to the left and lastly row 4 will shift 3 steps to the left. Figure 7 displays the different shifts.

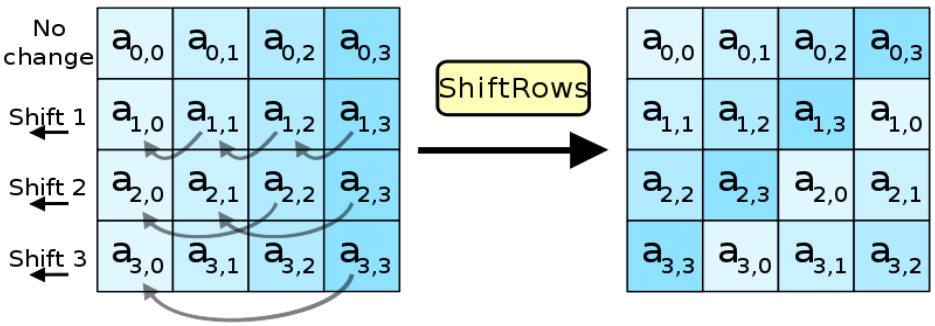


Figure 7: Shifting row step in AES encryption (Hafez & Mokhtar, 2010, p. 406)

Step 4: The mixing columns is a linear transformation where the columns are multiplicated with a matrix. The Matrix is a predefined matrix which is always the same. It can be seen in the middle of figure 8. A_0 to A_3 represents the different rows.

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Figure 8: AES shifting columns step (Random Wits, 2012)

Since it is a linear transformation, there is an inverse. The inverse matrix, M^{-1}, is =

$$\begin{matrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{matrix}$$

In the tenth round, the mixing columns step will not be applied as it has little to no impact on obscuration, but it has a cost of performance.

Step 5: A new round key (subkey) is added to be used as the new key for the next process.

After 10 rounds of this process, the output will be a well encrypted message, which also can be decrypted with the same key. AES is considered a random permutation algorithm.

The following part of this chapter elaborates on the research results from the Systematic Literature Review (SLR) that was conducted. The results from the SLR will be presented in three main categories: Security focused papers, performance and scalability focused papers and user centric papers. After the three paragraphs, a table comparing all the 12 papers is included to better display the differences. In the end, a summary of the research results is presented, and a paragraph that highlights the limitations of the studies and introduces why the proposed systems could bridge the gaps and contribute to the literature.

2.2 Related work concerning blockchain and healthcare

A Systematic Literature Review was conducted to understand how other researchers have studied the blockchain and healthcare. The methods used to conduct the SLR are described in Section 3. The topic of blockchain and healthcare is growing in the research literature. However, no real-world experiment outside isolated testing has been conducted. This substantiates how new and unexplored this research area is. The findings will help create a better understanding of the current state and which solutions are available.

Blockchain-based privacy and security solutions

Azaria, Ekblaw, Vieira, and Lippman (2016) introduces a new way for users to access their medical data. Their system is built upon the Ethereum network and provides good interoperability in the healthcare domain. Even though the system is on a private network, Proof of Work was still the opted method for consensus. Unfortunately, no regards to privacy, decentralization or scalability were considered (But was mentioned to be for further research). They have been an inspiration for others to build a EHR system based on blockchain technology.

Huang, Zhu, Xiao, Sun, and Huang (2020) continue with presenting a design where performance and privacy are the core values. All the data which is generated will be encrypted with Public Key Generation (PKG) and verified with Zero-Knowledge proof before it is temporarily stored in a semi trusted cloud server. Here the data will wait

upon approval to join the blockchain network. In addition, a consensus mechanism called Practical Byzantine Fault Tolerance (pBFT) is presented. This consensus mechanism is meant for consortium networks (smaller networks) since it has issues with scalability. The scalability issue is due to multiple messages being replicated and when ⅔ of them are received by the next step, they are approved.

MedBlock proposed by Fan, Wang, Ren, Li, and Yang (2018) is a blockchain system which tries to connect different regional hospitals. The blockchain will only contain “breadcrumbs” of data while the regional hospitals will store the medical data. This means that the blockchain is used as an index search and retrieval system for both patients and medical workers across hospitals. Patients are given a private key in an asymmetric encryption system, which is used to sign (encrypt) data before they are stored in the system. In this case, users have no control over who they share information with, but they can sign off on what to send. Unfortunately, this is involuntary. Also, the users are not allowed to input their own data. The design forces users to accept a terms of use contract which implies that the users are forced to accept the terms to use the software.

Chen, Lee, Chang, Choo, and Zhang (2019) introduce an index storing system similar to Medblock. Search indexes are stored on the public blockchain and EHR are stored on a public cloud with encryption. They use previous works from Huang et al. (2020) to achieve a search mechanism without the need for verification. In contrast to Huang et al. (2020), Chen et al. (2019) employs a complex Boolean expression that is used to extract the EHR to construct the index. There is no consideration for user input, access control or encryption. This work only focuses on a search index algorithm with blockchain and EHR on a cloud platform.

Darwish, Yafi, Al Ghamdi, and Almasri (2020) builds a blockchain-based hybrid algorithm to tackle the privacy issues of existing centralized cloud storage methods. The study only focuses on the creation of a security layer before storing data on a cloud service. The hybrid algorithm is a combination of two encryption standards: Elliptic-curve cryptography (ECC) and Advanced Encryption Standard (AES) as well as a key generation using the user's credentials. This is used to encrypt the data with an asymmetric key set generated with the SHA256 hashing technique. All of this is done before storing the data on a regular cloud service to increase security against Man-in-the-middle attacks and help mitigate Distributed Denial of Service (DDoS) attacks on a centralized key management server. In addition, the system checks signatures that are stored to see if any changes are made by malicious actors that have established a foothold in the system. The technique managed to detect 97% of the changes made in the system, which are greater than another system who managed 95% respectfully.

A paper by Mubarakali, Bose, Srinivasan, Elsir, and Elsier (2019) look at the technical aspects of using blockchain technology in a healthcare system. They perform tests with prototypes to get numeric values they compare with other systems. We can understand from the graphs presented, that the algorithm used in the SEHRTB system reduces latency by over two seconds and improves throughput by over 30%. This system uses a proof-of-work concept, which has been shown to be lacking when it

comes to scalability. The last section, future work, mentions the need to evaluate the feasibility of the system, which points in the direction of the system not being ready for a real-life scenario.
Rahmadika and Rhee (2018) proposes a system that uses blockchain technology as the backbone for security measures. The system uses proof-of-work, which we have seen multiple times, comes at a cost of scalability. The paper goes more in-depth regarding security issues, such as an eclipse attack, 51% attack, double spending, and a preimage attack. Keeping these threats in mind, the authors of the paper came up with an idea to effectively collect and manage data from different healthcare actors into a single system. They end their paper with the following quote: “For the future work, the model needs to be evaluated, especially the strategy to prevent several attacks in the P2P[3] network”. This makes it apparent that there are still things that are not clear for the overall system, but especially when it comes to the security aspects.

Performance and scalability of blockchain-based solutions
Not all studies have only focused on a security and privacy. Some investigated the performance side of blockchain in the healthcare sector. Since blockchain in its nature is considered secure and retains privacy, the goal of these papers is to test how the technology scales and the performance impact it has compared to systems that are already in use.
Stamatellis, Papadopoulos, Pitropakis, Katsikas, and Buchanan (2020) presents a system using Hyperledger fabric. It is mainly focused on improving the performance and scalability of current systems, but they also look at how privacy-preserving the system is, and if it follows GDPR regulations. Their system, called PREHEALTH, uses Proof-of-Elapsed-Time, shows similar performance with handling 100 records, as it does with handling 1 000 000 records. This indicates that the scalability of their system is incredible, and the blockchain technology maintains its secure benefits. The Hyperledger Fabric framework helps ensure anonymity, and therefore preserve privacy. The authors argue that their system can be used by both patients and healthcare actors, who want to store healthcare related data.
Toshniwal, Podili, Reddy, and Kataoka (2019) looks at a system that allows patients to have control over their own data. The entire system revolves around using smart contracts to store information about patients. This is done in different ledgers, ranging from general information about hospitals and patients, to sensitive data about patients that only the given patient and the corresponding hospital has access to. As stated in the conclusion “incorporating various multithreading algorithms across the hospital side can help to handle the requests parallelly. This will enable the proposed system to scale well in case of a large-scale network” (Toshniwal et al., 2019, p. 7). From this we can understand that the scalability of the proposed system is lacking, but a benefit of the system is the user-friendly aspect. This is because patients do not need knowledge about how the blockchain technology works, nor do they need advanced

[3] P2P stands for Peer-to-Peer network. It is a network where computers are connected and share information directly between each other without utilizing a centralized server.

hardware. Another benefit mentioned in the paper is that the system offers a secure way of sharing information between patients and the hospitals they wish to share their data with.
Reen, Mohandas, and Venkatesan (2019) attempts to put forward a decentralized system that provides immutability of records. Their tests and simulations show that even with very few records (in comparison to other system's tests) the scalability of the proposed system is an issue. The authors argue that a way to work around this is to not store data on the blockchain, but simply use it to transfer data from a database to patients, and vice versa. To ensure the storage of data is secure and that only certain actors have access to records, the paper suggests the use of a combination of symmetric and asymmetric key cryptography. Some issues that will not be solved with this system are also presented. Some of them are healthcare personnel who have access to data. The possibility of taking pictures of the data or writing it down is present and it would not show up on a blockchain. Because of this, there needs to be certain trust towards the healthcare personnel, and you cannot solely rely on the system. Another example is the use of technology in developing countries. It is mentioned that not everyone has access to devices able to run the necessary applications, or do not have the necessary knowledge to perform the needed tasks.

User-centricity in blockchain-based applications
Bosri, Uzzal, Al Omar, Bhuiyan, and Rahman (2020) proposed a user-centric system which allowed users to monitor the hash values which were stored in the blockchain. These hash values were records of the data transaction and not the data itself. This means that the user could see if a hash were passed through and then confirm that the data was stored. In addition, the user was able to permit which healthcare professional to monitor their data. Primarily the data being collected was from wearable health devices (IoT).
Fatokun, Nag, and Sharma (2021) presented a good Ethereum based EHR exchange system. The system is user-centric as it allows for great user interactions with the system and good interoperability between different systems. The user is given an app to view appointments, their data and grant access to healthcare workers. It also provides a standardized platform for EHR sharing across hospitals by collecting them on the same network instead of utilizing Fast Healthcare Interoperability Resources (FHIR) or Clinical Document Architecture (CDA). The Ethereum network is a consortium and uses Proof of Work. Once a block has been added, the users cannot modify it.

Table 3 displays what is included in the 12 papers used in this literature review. The characteristics of each system are displayed to compare, and taken inspiration from, to the system being proposed in this thesis. From early gathering of data through research, some challenges were found, one of which being performance. Performance was therefore a focal point of the literature review, together with security, privacy, and user-centric aspect.

Table 3: Summary of 12 Reviewed Papers based on some Blockchain Properties

Reference	Storage technology	Public /Private/ Consortium	Access Control	Encryption	User interaction	Performance	Privacy	Consensus mechanism
PREHEALTH (Stamatellis et al., 2020)	HLF	Private	Private	Yes	No	Yes	Yes	PoET
MedRec (Azaria et al., 2016)	Ethereum	Private	PKI	Yes	Yes	No	No	PoW
A blockchain-based scheme for privacy-preserving and secure sharing of medical data (Huang et al., 2020)	NA	NA (But presumed private)	PKG	Yes (Zero knowledge)	No	Yes	Yes	pBFT
MedBlock (Fan et al., 2018)	NA	Na (Public Presumed)	PKG	Yes (asymmetric)	No	Yes	Yes	Hybrid with pBFT
Blockchain based searchable encryption for electronic health record sharing (Chen et al., 2019)	Ethereum and IPFS	NA (Public presumed)	Authentication with tokens	NA (Exemplifies AES)	No	Yes	No	PoW
PACEX (Toshniwal et al., 2019)	Ethereum	Public	PKG	Yes	No	No	Yes	PoS
Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid Algorithm (Darwish et al., 2020)	NA	NA	PKG with SHA256	AES and ECC	No	Yes	Yes	PoW
Decentralized Patient Centric e-Health Record Management System using Blockchain and IPFS (Reen et al., 2019)	Ethereum and IPFS	Public	PKI	Yes	No	Yes	No	PoA
Blockchain technology for providing an architecture model of decentralized personal health information (Rahmadika & Rhee, 2018)	NA	Public	PKI	Yes	No	No	Yes	PoW
SEHRTB (Mubarakali et al., 2019)	NA	Private	PKI	Yes	No	Yes	Yes	PoW
HIDEchain (Bosri et al., 2020)	NA	NA (Private presumed)	Hash matching (SHA256)	Yes	No	Yes	Yes	NA
Towards a Blockchain Assisted Patient Owned System for Eletronic Health Records (Fatokun et al., 2021)	Ethereum	Consortium	PKI (MetaMask)	Yes (ECDSA)	Yes (But no input)	Yes	Yes	PoW
BUC	NA	Private	PKI	Asymmetric	Yes	No	Yes	pBFT

HLF= Hyperledger Fabric, NA = Not announced, IPFS = Interplanetary File System, PKI = Public Key Infrastructure, PKG = Public Key Generator, MetaMask = Cryptokey wallet, AES = Advanced Encryption Standard, ECC = Elliptic Curve Cryptography, ECDSA = Elliptic Curve Digital Signature Algorithm, PoET = Proof of Elapsed Time, PoW = Proof of Work, pBFT = Practical Byzantine Fault Tolerance, PoS = Proof of Stake, PoA = Proof of Authority.

Table 3: Summary of 12 Reviewed Papers based on some Blockchain Properties

Many of the papers in the literature review go over a system designed to improve either security, performance, privacy, or all the above. The security focuses papers presented above only gave a security (blockchain) layer to access a cloud server with the EHR. In essence, what they show is an additional security layer which works as an access management server. This server (based on blockchain) will store keys which the user shares in asymmetric encryption and provide the user with access to a cloud storage of their EHR. The reason most papers have made a security layer instead of storing the EHR in blockchain, is due to the scalability problem. A management system requires less stored data. Stamatellis et al. (2020, pp. 9-11), Toshniwal et al. (2019, p. 6) and Reen et al. (2019, p. 6) showed some promising results regarding performance and scalability which has been a topic of concern regarding blockchain technology. These benefits create additional motivation to design a system based on blockchain.

Papers found in the literature review were not including the use of third-party applications, which provide data like daily nutritional intake, workout information, etc. This shows that there is room for using this information to create a more holistic system.

This thesis aims at designing a Blockchain-based, User-Centered (BUC) system for the healthcare sector in Norway. Not only will the complete system be utilizing blockchain, but it will allow third-party applications the possibility to export data to the users EHR. In addition, the proposed system will have a public basic EHR which is visible to everyone in the consortium. This EHR will contain the basic non-confidential information such as Name, date of birth, height etc. A private EHR is connected which the user can grant viewing access to.

3 Research approach

This chapter presents Design Science Research (DSR) and how it helped frame this thesis. It will also dive deeper into how DSR studies are conducted to give the reader a better understanding of the process of a DSR. Chapter 3.3 and 3.4 will lay the foundation for the related works chapter (2.2) and show how the data was collected. In the end of chapter 3.4. In the end PRISMA[4] chart is presented with the filtration process of the systematic literature review (SLR).

3.1 Research methods

Design Science Research (DSR) will be the approach utilized in this thesis. DSR is based on the need for something new or improving something previous according to Gregor and Hevner (2013, p. 7). The new item is described as an artifact. An artifact can be anything ranging from a new piece of software or algorithm to a new system or framework (Chatterjee, Xiao, Elbanna, & Saker, 2017, p. 1). The only important thing is that it will fall under one of the categories in figure 9 from Gregor and Hevner (2013, p. 7). Invention is perhaps one of the most obvious choices when a new artifact is introduced, but as explained by Hevner it is also one of the rarest ones.

> "True invention is a radical breakthrough--a clear departure from the accepted ways of thinking and doing. Inventions are rare and inventors are rarer still. The invention process can be described as an exploratory search over a complex problem space that requires cognitive skills of curiosity, imagination, creativity, insight and knowledge of multiple realms of inquiry to find a feasible solution."*(Gregor & Hevner, 2013, p. 10)*

Improvement, on the other hand, is a far more common category. It is defined as *"*to create better solutions in the form of more efficient and effective products, processes, services, technologies or ideas. […] The key challenge in this quadrant is to clearly demonstrate that the improved solution genuinely advances on previous knowledge" (Gregor & Hevner, 2013, p. 10).

[4] Prisma chart (also known as PRISMA flow diagram) depicts the flow and information through the SLR[x]

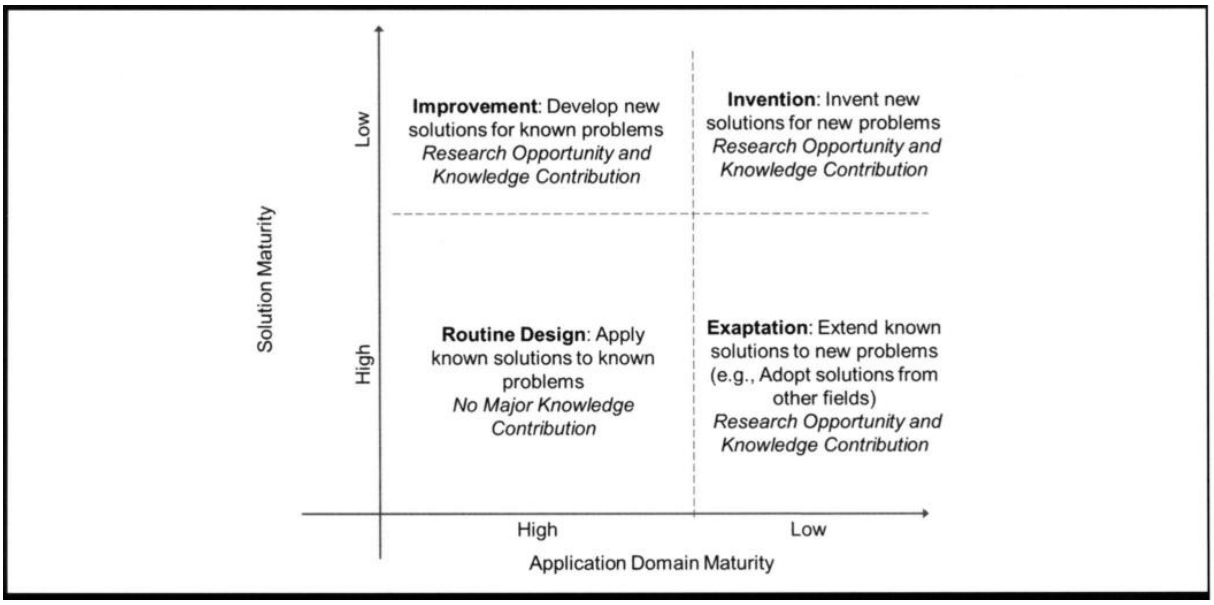


Figure 9: DSR Knowledge contribution Framework (Gregor & Hevner, 2013, p. 10)

In essence, DSR is about creating an artifact which will either improve current systems or create a whole new one. Its aim is to solve problems which either arise from an environment of need or from lacking artifacts currently being used.

Typically, in an improvement DSR, the goal is to gather information and knowledge of the current systems and related work in the field of attention. This step must be performed to ensure a holistic view of the current situation. Both to create a new artifact, and to evaluate the new artifact compared to the current one. Figure 10 is adapted from (Hevner, March, Park, & Ram, 2004, p. 7) which displays the design of the artifact in the middle of the diagram. This thesis evaluates the environment in the beginning of chapter 5 while the knowledge base was presented in chapter 2.

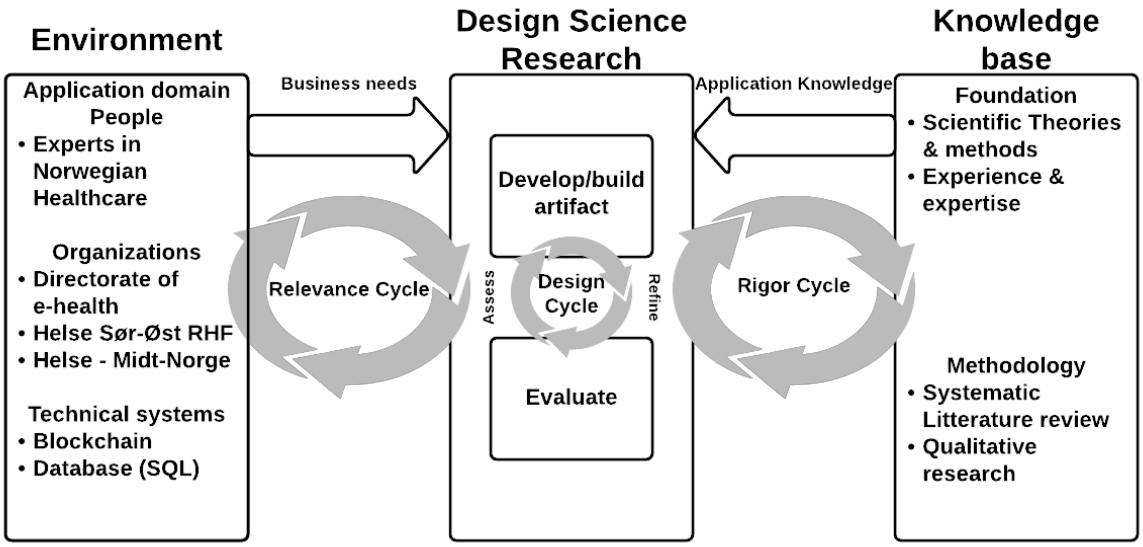


Figure 10: Information Systems research Framework, adapted from Hevner et al. (2004, p. 7)

A later paper from Hevner (2007, pp. 3-6) explains the cycles in figure 10; relevance cycle, design cycle and rigor cycle. The relevance cycle helps feed the design process by providing a need for the new artifact. The rigor cycle gives knowledge and theories about the issue the artifact is trying to solve. Then the last design cycle incorporates these two cycles and provides an artifact based upon them. The artifact will continue to evolve as it is evaluated, tested and new needs or knowledge is provided from the other cycles. The design cycle can be viewed in figure 11 which is taken from Hevner et al. (2004, p. 16).

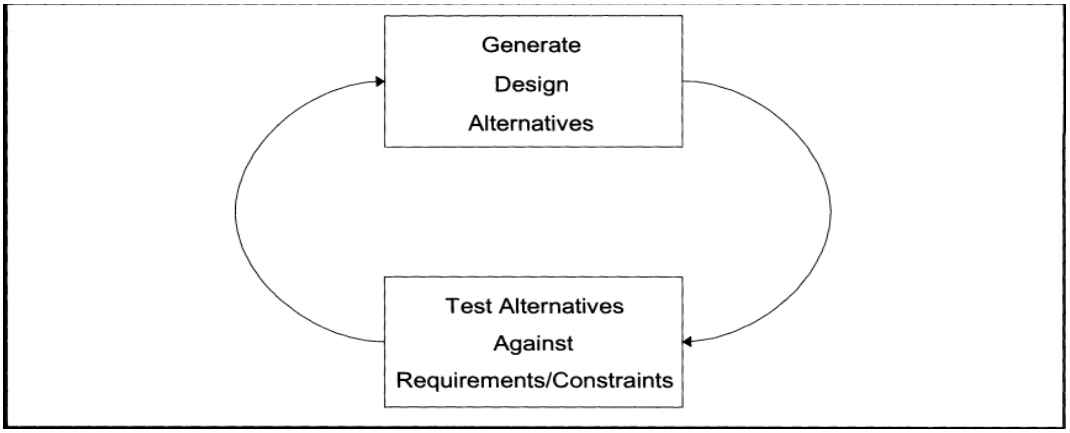


Figure 11: Design cycle for DSR, adapted from Hevner et al. (2004, p. 16)

When it comes to looking at how technology affects the procedures in an organization and how it affects the people in the organization, a qualitative research method is likely to help with getting a better understanding of the implications implementing this new technology could have. The information gathered in the qualitative research will also help with performing a DSR later in the thesis. This is backed up by Creswel, who says that “Often the distinction between qualitative research and quantitative research is framed in terms of using words (qualitative) rather than numbers quantitative)” (Creswell, 2015, p. 32). He then goes on to compare the two different methods and says that “Qualitative research is an approach for exploring and understanding the meaning individuals or groups ascribe to a social or human problem”(Creswell, 2015, p. 32).

> “Qualitative research is an approach for exploring and understanding the meaning individuals or groups ascribe to a social or human problem. The process of research involves emerging questions and procedures, data typically collected in the participant’s setting” (Creswell, 2015, p. 32).

In the event that we want to find out what the users’ needs and requirements are, how satisfied most people are with a technology, how scared they are of implementing new technologies, or the implications that this brings, a qualitative research method can help us find the answers needed.

The following chapters present how the data for the thesis was gathered through conducting interviews and performing a systematic literature review.

3.2 Design Science Research

The goal of this thesis is to design a user-centric system (BUC) and this is regarded as a new artifact. This will be done by using a DSR approach, as this is a good methodology when designing a new system (Hevner et al., 2004, p. 3). It provides a good way to collect previous knowledge about the topics regarding the artifact and displays the clear need for why the new artifact is wanted. To conduct a DSR, inspiration was taken from the 7 guidelines (Hevner et al., 2004, p. 10) outlined in "Design Science in Information Systems Research". Each of these guidelines provide good information on important aspects, and they are all important to follow. Because a typical DSR consists of a need for a new/improved artifact (relevance cycle), previous research (rigor cycle), and design proposal (design cycle), an artifact evaluation with discussion on how the new artifact is contributing to the intended field is required. An overview of the guidelines can be viewed in figure 12 from (Hevner et al., 2004, p. 10).

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Figure 12: Design Science Research Guidelines from Hevner et al. (2004, p. 12)

How data was collected (rigor cycle) is described in chapter 3.3 and 3.4, but the evaluation process will be done quite differently. As this is not a proof-of-work DSR, only a hypothetical artifact will be made. It will only be a proposed and a descriptive evaluation based on three evaluation methods from Hevner et al (2004) will be conducted. These methods include:

- A **case study**, which looks at the artifact from a business environment.
- An **analytic method**, more specifically architectural analysis, optimization, and dynamic evolution. Based on prior proof-of-concept research, the evaluation will display performance metrics from a blockchain system compared to a regular database system.
- An **informed argument**, which will be the main evaluation method. Chapter 5 will present how the system in this thesis differs from other proposed systems in terms of usability, user friendly operations and more power given to a user over their own data.

3.3 Interview

The literature review, as well as the interviews, will be the foundation for the qualitative research done in this thesis. The goal is not to find a definite answer to a hypothesis, but to explore the possibility of a user-centered and blockchain based artifact in the Norwegian healthcare sector. This means that interviews, where going in-depth, is a more attractive option, as together with the SLR, it will give a good overview over what is realistic and what is not.

Following the interviews and literature review, this thesis will use the gathered data to discuss the proposed research goals.

When looking at who to interview for the interviews, the focus was to find people who either know of the blockchain technology, who are working directly with the IT systems in the healthcare sector, or ideally both. IT professionals were the primary interview objects, as thoughts and opinions from people working directly with the systems in question, and people who have knowledge about the technology will likely give the most precise and thorough input. Some questions were prepared, and even sent to the participants before the interview, so that they could process the questions beforehand. Open discussion also played a big role during the interviews, where new ideas, or questions were asked and answered. This allowed for opinions to be shared outside the scope of the questions and presented the opportunity for further questions.

The interviews were conducted in one of two ways. Either a written interview through email or a questionnaire with discussion in a Teams[5] meeting. The questions can be found in appendix A. Teams meetings were chosen for ease of use and due to the covid-19 situation, travel was not recommended. The questionnaire was discussed in

[5] Microsoft Teams

the Teams meetings, but it also added the benefits of follow-up questions and discussions. The duration of the Teams interviews were approximately 60 minutes.
Participants were found by contacting different entities in the Norwegian public health care system. Email was used to reach out and ask participants for interviews. Out of 12 possible interviewees, only 4 responded and accepted to take part in the research. The anonymized list of experts can be found in Table 4.

Table 4: List of experts in the Norwegian Healthcare Sector

ID	Position - Organization
$\lambda 1$	Advisor - Directorate of e-ehealth
$\lambda 2$	Security personnel - Helse Midt-Norge
$\lambda 3$	IT expert - Helse Sør-Øst RHF
$\lambda 4$	Advisor - Directorate of e-health

Table 4: List of experts in the Norwegian Healthcare Sector

$\lambda 1$ and $\lambda 4$ chose to answer the interview protocol by email while $\lambda 2$ and $\lambda 3$ conducted a Teams meeting with us. The Teams meetings sparked great discussions and new perspectives upon the topic of combining blockchain and the Norwegian healthcare sector.

The results of the interview were gathered in individual summaries. These summaries were compared to each other to find differences of opinions and information about the current Norwegian Healthcare system. The results from the interviews will aid in a more holistic view of the current situation in Norwegian Healthcare. Both from a security and infrastructure aspect and a culture aspect. The results are presented in the discussion chapter and utilized throughout the thesis.

3.4 Systematic Literature Review

When looking into a topic or preparing to write a paper, doing research on what is already known will help in understanding a topic better, as well as seeing what research has already been done on that topic. This type of research is often referred to as a literature review. By conducting a SLR, this thesis will access the knowledge database

(Ref figure 10) on blockchain-based healthcare systems as a part of the rigor cycle. Okoli and Schabram (2010) presents the reasons for using literature reviews as the theoretical foundation for primary research and literature reviews for graduate student theses. It is “A Case for Rigor in Literature Reviewing” according to Chitu Okoli (2015). They also mention a third type of literature review, which is stand-alone literature review. The purpose of a stand-alone literature review “is to review the literature in a field, without any primary data (that is, new or original) collected or analyzed” (Okoli & Schabram, 2010, p. 2). Although the stand-alone literature review will usually be part of the two first types of literature reviews, a key difference that distinguishes the review as a stand-alone one is that the data it will not be collected and analyzed. We can support the claims above with a definition from Hart (1998). He defines literature review as “the use of ideas in the literature to justify the particular approach to the topic, the selection of methods, and demonstration that this research contributes something new” (Hart, 1998).

Webster and Watson says that literature reviews “facilitates theory development, closes areas where a plethora of research exists, and uncovers areas where research is needed (Webster & Watson, 2002, p. 13). This means that if a literature review is done right, it will support the research goal by allowing us to see what topics have not been investigated yet.

As part of the literature review, a few databases were selected, and literature from those databases were extracted using specific keyword search terms. The collected literature was filtered down based on criteria that fits the goal of the thesis.

The databases that were used to find the literature were Scopus, Google Scholar, Aisel, and IEEExplore. The following is the string with the search criteria used in the different databases:

> (blockchain AND health* AND design) OR () OR (blockchain AND hospital AND design) OR (blockchain AND phr AND design) OR (blockchain AND ehr AND design) OR (blockchain AND patient AND design) OR (health* AND Norw* AND design) OR (cyber AND risk AND health*)

When searching through different databases for literature, the scope was further narrowed down after the initial search string were used. These steps were to limit the results to only show journal, results between 2015-2021, final publications, and limiting the country of publication to America, Norway, and China. The reason why other counter countries were excluded, was because America and China are leading actors when it comes to blockchain technology (Insights, 2019; Sardi et al., 2020, p. 4). Norway was included because this thesis looks at the Norwegian healthcare sector. Last step of paper-filtration was to only show publications in English and Norwegian. The results were further narrowed down by adding filters to the searches, as well as limiting the research area. See figure 13.

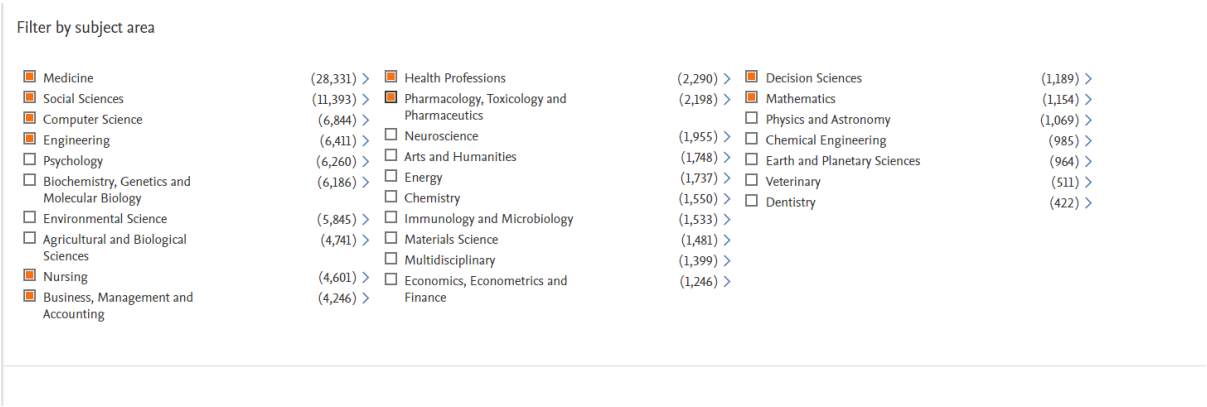


Figure 13: Overview of filters applied on our literature search

In figure 14 the literature collection process with exclusion is presented in a PRISMA CHART (PRISMA, 2020). Papers from the four different databases were collected into a folder in EndNote 20[6]. A relevance sentence was created to evaluate the papers. This relevance sentence was: It must include a system utilizing blockchain to improve EHR access to a user. This was done to find the studies which resemble what the goal of the design in this thesis is. Six different iterations of exclusion were used in the following order:

1. Exclusions based on duplicates.
2. Papers were excluded based on title. Any non-relevant titles were removed.
3. Papers were excluded with regards to abstract and conclusion. If there were little to no relevance, they were excluded.
4. First full read of the papers. Some were excluded based on their content as it was not relevant to the work in this thesis.
5. Based on the reader's evaluation of the papers, more papers were excluded.
6. After reading the 83 papers from the literature collection, we used a rating system in Endnote20 to rate the relevance to the proposed research goals. This was based on how close they were to this thesis' vision. After evaluating based on relevance, the number of papers were narrowed down to 12.

[6] EndNote 20 is a reference management tool.

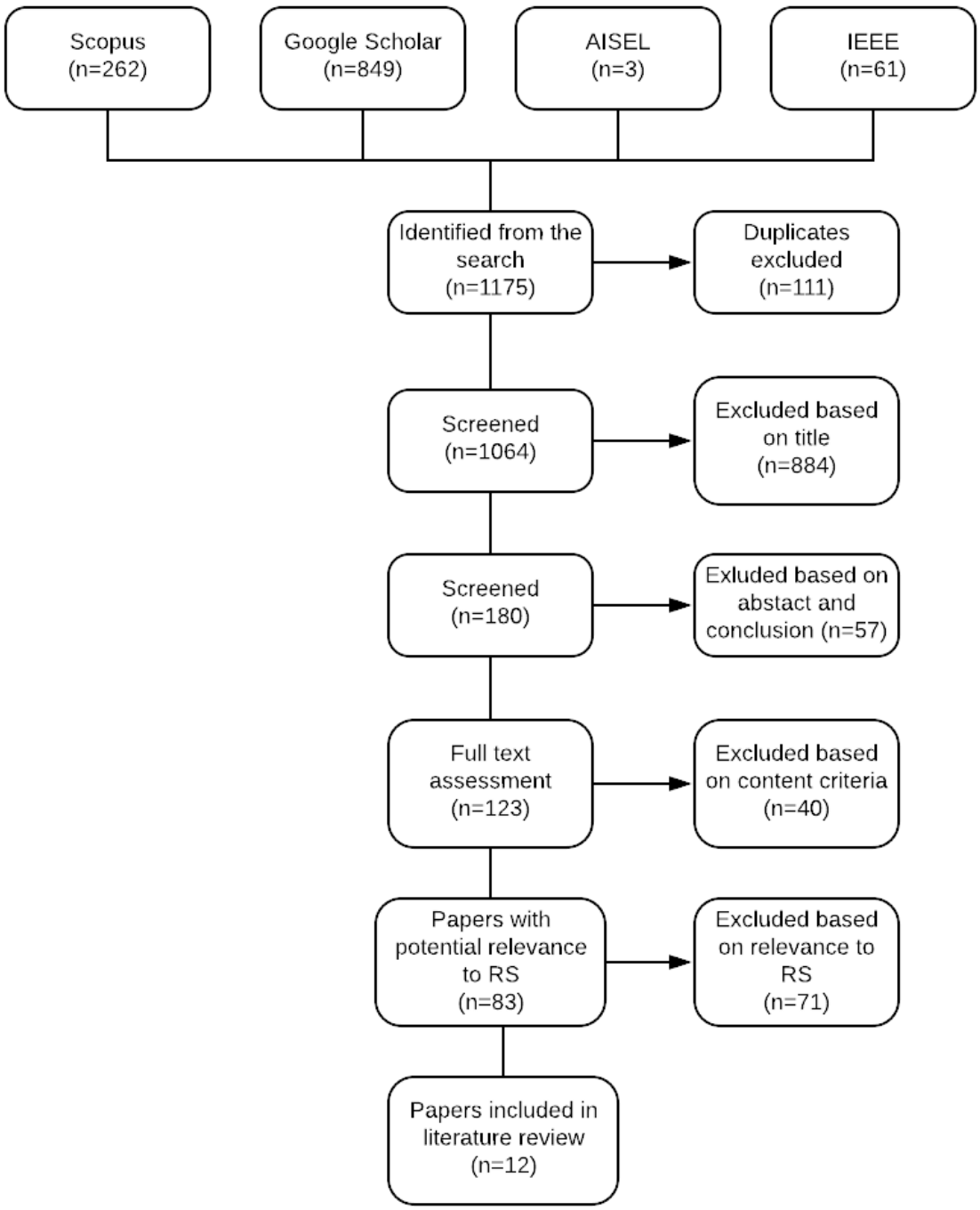


Figure 14: PRISMA chart of the SLR

The next chapter will present the BUC. BUC is a modular system which proposes different solutions to each section. The different sub-chapters elaborate upon options which are best suited in the modular BUC. To make it easier, an overview of the system is presented in the beginning with each modular option presented later. Each option is argued for, and different options are presented.

4 A Design proposal for a user-centered system

The findings in the SLR showed a gap of a holistic system when it comes to blockchain technology. Some papers proposed security layers, others focused on performance and a few focused on a more user-centered healthcare system. This chapter will propose BUC, which combines these previous systems. BUC covers both frontend and backend solutions. The proposal will be explained further in depth for each element in the following sub-chapters. To better understand how they all connect, an overview will be presented first. The solutions in the sub-chapters are synthesized from the prior research and findings from the literature research and interviews. This approach will allow for better judgement of what solutions could be best suited for a system. The modular BUC system can be viewed in figure 15 and everything is centered around the user. They have access to an application (frontend) which allows them to interact with the BUC. Here they can view their data, health appointments (both upcoming and previous) with notes and a tab with who can view their data and the possibility to give and revoke permission to view the data. There will also be a tab which connect third-party applications such as MyFitnessPal, Strava, or Apple Health so the data from these applications can be imported to the patient journal. Helsenorge's current state is lacking the ability to interact with the system. Patients (users) only have the option to view certain information. This is done through "Pasientjournal" (Helsenorge, 2021). Here, the user can view their messages from their doctor, information about the corona vaccine, documents from hospitals and GP to mention a few. The problem lies in what these subsections contain. Talking with someone who has had several surgeries, they mentioned that they were missing proper documentation in their journal. In their journal only one document was visible and that was a reference to a doctor's appointment. This shows that there are some efforts made to give users a peek into the information, but the implementation has failed as little to no information is displayed here.

The backend will consist of a consortium of entities on the blockchain (View part labeled **1** in figure 15). Because a consortium allows only trusted entities into the system and maintains some decentralization, it is best suited for the proposed system (ref table 1). Entities, as explained earlier, will consist of governmental healthcare, private healthcare, physiotherapist, General practitioner (GP), dentists and airports (for vaccines). They have a set of nodes which represents them in the system. These entities will have access to a public patient journal which only contains non-confidential information (**4**). Examples of this information can be name, date of birth, weight, height, and vaccines. The reason behind having this information visible to everyone in the consortium is to make it easier for the healthcare providers (which according to Norwegian law requires immediate access to medical data (Helse- og omsorgsdepartmentet, 2015a, para. 1)) to access basic information and have one single place to find it. Today this information is stored in a database for each entity which creates a bigger attack surface since the information is scattered around. The quick access to basic information will also benefit the user, who no longer are required to sign up at different places. New information will also be connected to their patient

journal. No longer is there a need to export and import data across the entities and systems and the patient's GP can know exactly what their health history is (If the patient allows the GP to view the data).

In the chapter above, the public journal was described, but the private ones are also a vital part of the system (**5**). Epicrisis[7] of surgeries or other sensitive information which individuals might not want to share, can be encrypted and stored privately in an off-chain blockchain. Off-chain blockchain is a separate blockchain which is linked to the main (consortium) one. This thesis will use the term private journal when referring to the encrypted journals which are stored in the off-chain. Each private journal is stored individually and generates a set of encryption keys (PKI) (**4**). The private key remains with the user, but they are able through their app, to share their key with any practitioner they wish. This will grant the practitioner access to the information in the private journal (**3**). In the case of an emergency, a medical doctor has the option to access this data (**6**), but the doctor will be legally bound to provide valid reasoning for why they accessed the data.

With all of this to create a user-centric system and the blockchain technology as a backbone to provide strong security with encryption and immutable ledgers, the system is a step in a more privacy focused future.

[7] «Epicrisis is a short, concise, written acocunt of the cause, development and treatment of a patient's disease. The epicrisis is prepared after the exmaination and treatment has been conducted» (Geir Sverre Braut, 2020)

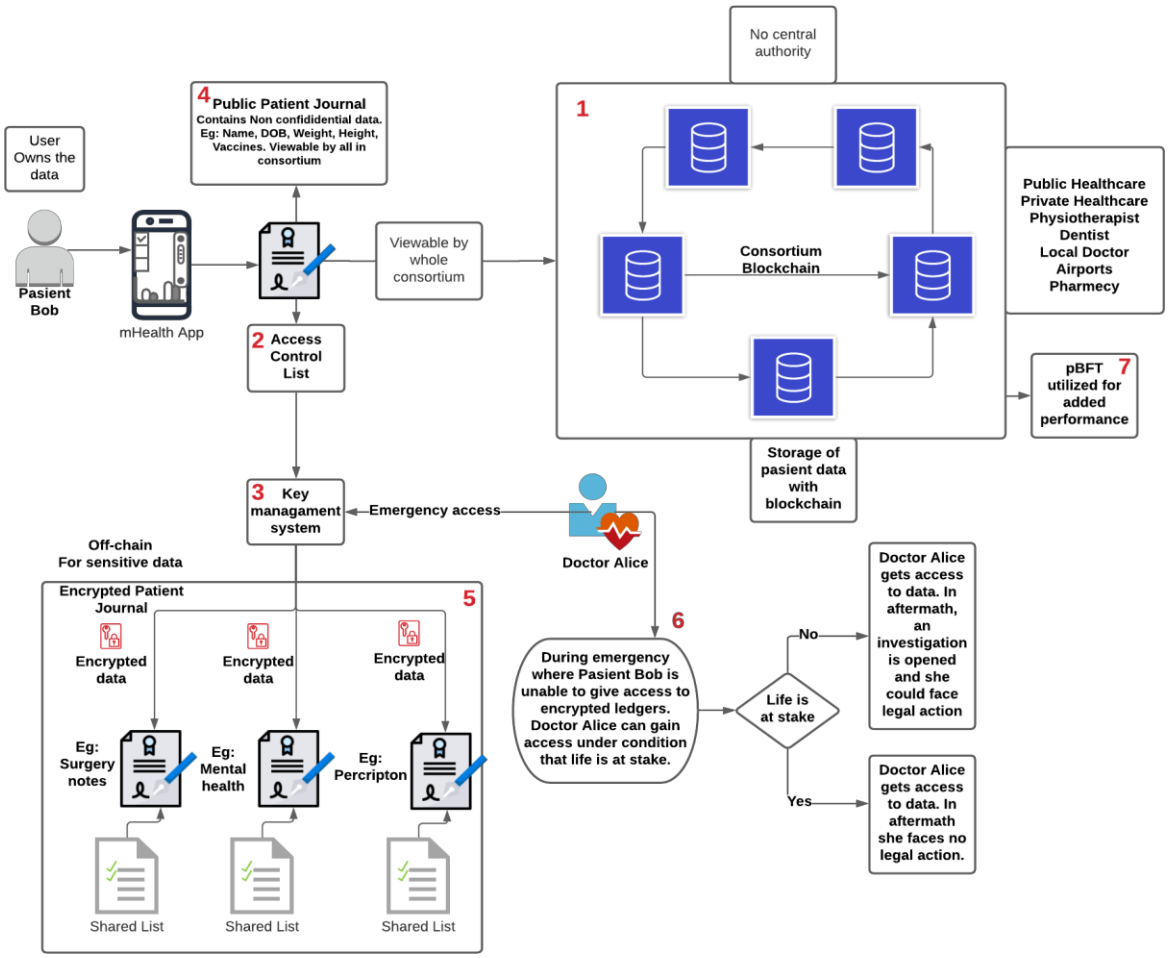


Figure 15: Overview of the proposed system. 1 - Blockchain storage. 2 - Access Control List. 3 - Key Management System. 4 - Public Patient Journal. 5 - Encrypted private journals in the off-chain. 6 - Emergency access. 7 - Consensus Mechanism.

4.1 Storage

Most of the presented solutions in the SLR findings utilized a blockchain technology for the EHR/database search index control. This added a security layer to the database which mitigated the scalability issue. By only storing a pointer or breadcrumbs to the full EHR, the amount of data being stored is rather small. Figure 16 illustrates the concept of the security layer. It creates a safer way to access data by storing the access data in the blockchain. Performance is also not being affected notably because the amount of information being processed, is so small. Decentralization is also achieved to some degree by not only having one entity controlling the access to a database. Even though the database is controlled by a single entity, the access to it is decentralized.

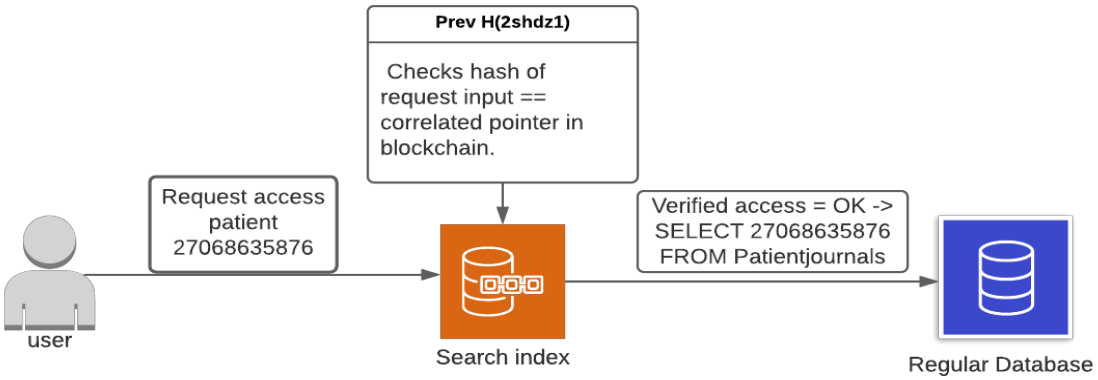


Figure 16: Security layer for search index

A different solution is to just have a regular access control list (ACL) and utilize a blockchain database to store the EHR. See figure 17. Here the user requests access to an EHR with ID “27068635876”. The user must then verify their identity with mobilID. This is a Norwegian national ID verification solution for official use. The ACL checks the hash of the user input and then finds the corresponding table. At this stage it confirms the access to a certain EHR(27068635876) and hands out the correct user rights to the requester. Access to the EHR is granted.

The biggest security improvement in such a system is the immutability which blockchain provides. High encryption standards can be achieved by the system by both systems. The security in figure 17 better due to the immutability feature in the storage itself. Unfortunately, there is one major drawback. The biggest issue with this approach is the scalability. Because the database is immutable, it will continue to grow (in proportion to ever node) every time data is added to the EHRs. This will cause great growth of memory being used in the system. An important note here is to keep reviewing the progress of blockchain technology and storage prices. Both of these have improved tremendously in the last 20 years, and it is hard to predict what the future holds. A safe bet is a lowering of price attached to fast storage solutions.

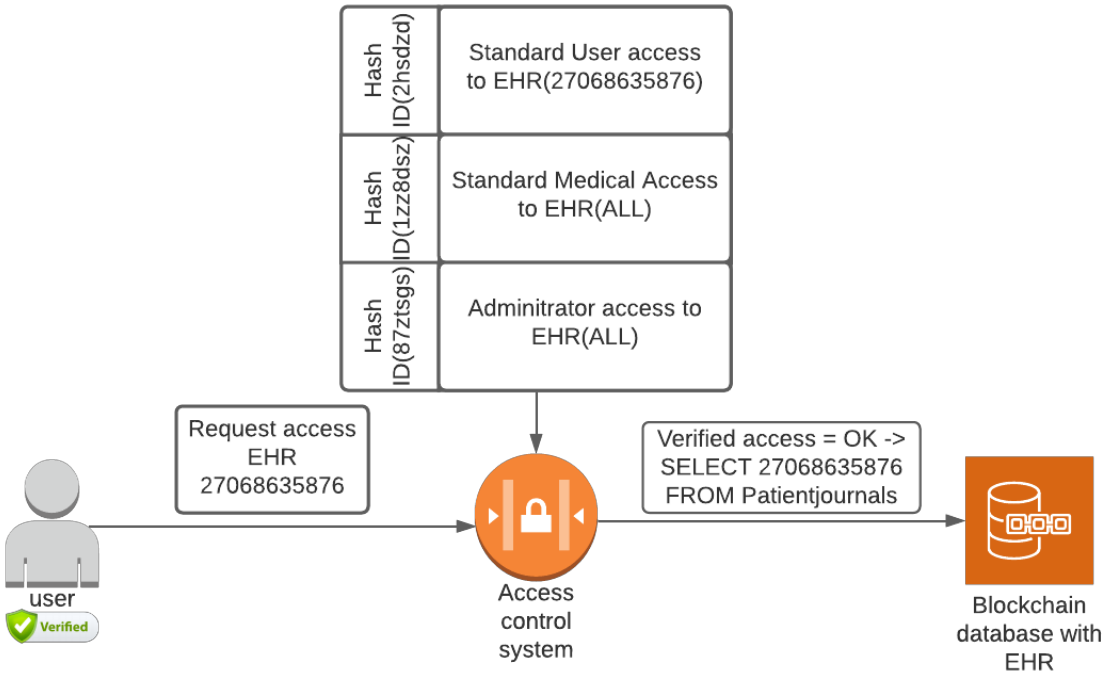


Figure 17: Blockchain as database storage and regular ACL

4.2 Access Control

To manage the access to the private journals, an access (ACL) control list needs to be incorporated. This will have the updated list containing information about which users have access to view the private journal on the off-chain (5). Medical staff and doctors can request access to the private journal, but this must be approved by the patient. This decision can be executed swiftly in the user application by the patient. As shown in figure 18, the process causes an update of the ACL. An important caveat here is that the key set must be renewed. There is a generated PKI pair associated with the ACL. The private key is then shared with everyone on the ACL including the user.

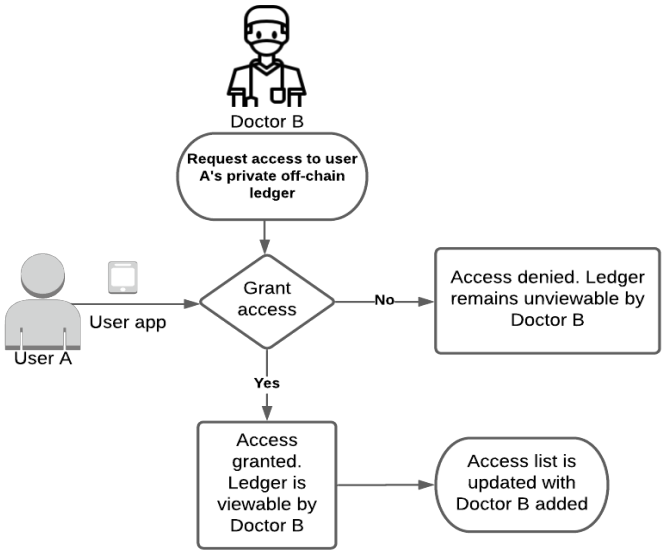


Figure 18: Flowchart of "Grant Access private off-chain"

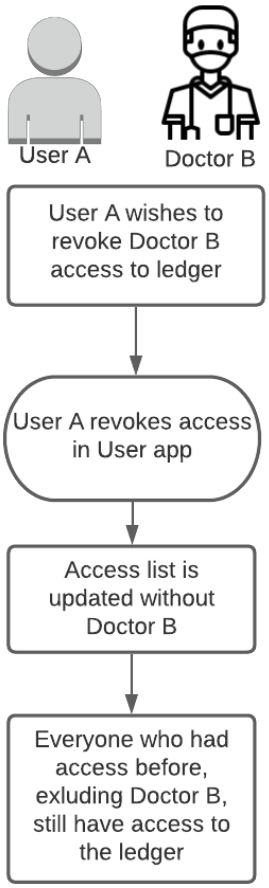


Figure 19: Flowchart of "Revoke access to off-chain"

The patient can also revoke access to the private journal. This is simply done through the user app as well. The ACL is then updated with the new list, which includes all previous IDs except for the user whose access got revoked. It is important to note that the previous keyset, which gave access to the private journal, is now known by the person who got their access revoked. To get around this, a new key pair is generated and is handed out to the IDs on the updated ACL. See figure 19.

4.3 Encryption and key management

Because BUC requires encryption and sharing of encryption keys to share the off-blockchain sensitive documents, a solution which provides this is required.

Darwish et al. (2020) proposed a mechanism for generating keys with their hybrid algorithm. It utilizes a generated hash from the user's passphrase. This is done with the SHA256 algorithm. The hash is then used to seed a random number generator with the user's credentials. By doing this, a hardcoded key pair utilizing the public exponent is generated for the Elliptic Curve Cryptography (ECC) algorithm. Since the user's credentials are unique for each user and the key pair is hardcoded, it will ensure no keys are the same and will remain immutable.

To extend on this, a symmetric algorithm is used to encrypt the data. To encrypt it, a Random Number Generator (RNB) is utilized. Typically, the algorithm has different key sizes, but in the study from Darwish et al. they only utilize the 128-bit key and data blocks of the same size.

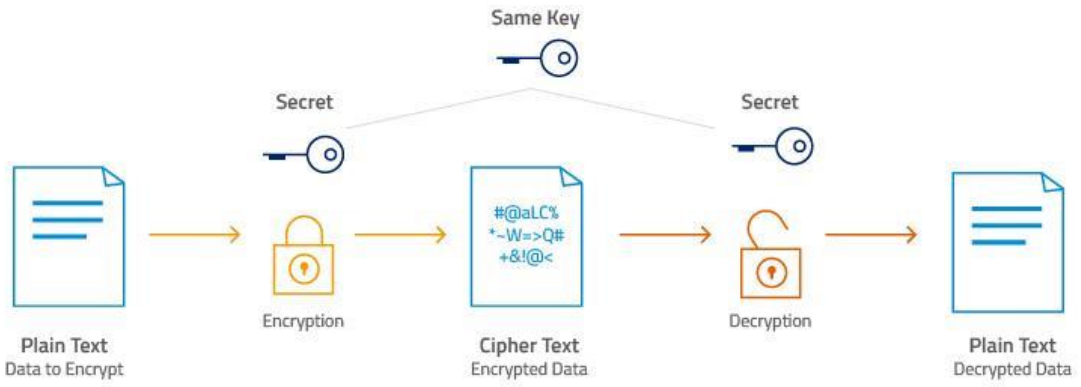


Figure 20: Symmetric Key Encryption (ATP, 2019, para. 4)

The decryption of this data is the same, just in reverse. Figure 20 gives an overview of the AES encryption and decryption process.

In the proposal from Darwish et al. (2020), they use an ECC algorithm. This algorithm utilizes an PKI, which is an asymmetric key generation algorithm. The purpose for this is to encrypt the AES key and then generate a pair of keys to unlock it. By doing so, it is “making it difficult to disclose and facilitate the key distribution between the users and the cloud providers” according to Darwish et al. (2020). Each key is bound with a random number and the user's credentials to create their own private key. For further details on the process, please read Darwish et al. (2020) paper *“*Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid Algorithm*”*.

4.4 User interface

In order for the system to be successful when it is in the hands of the users, having a User Interface (UI) that is easy to understand and navigate is essential. “A user interface, or UI, is what connects users to a product’s underlying technology [...]. By contrast, a user experience, or UX, encompasses the entire experience users have with a product” (McKay, 2013, p. 6). This section will look at elements that can be good to include in a UI to enhance the UX (User Experience) for people interacting with the BUC.

A key element that could be made possible with the integration of third parties, such as MyFitnessPal, massage therapy, chiropractors, etc. is the feeding of additional health related data into the EHR. This type of data could be nutritional values ingested throughout the day, or the thoughts your chiropractor had after an appointment. When it comes to the UI part of this element, the backend might be complicated, but the front end should be as simple as to connect to another app and press “sync” to import the data.

For patients, a way to edit who has access to the journals in the EHR is important. A healthcare system will often have a lot of sensitive data and having a clear and intuitive way to edit these permissions, will reduce the possibility of an error to occur.

Having a system that is more unified than the different systems currently in use in the Norwegian healthcare sector, we can improve upon the user friendliness aspect by making certain tasks easier. By having a settings or user information section in the UI, the user can use it to change emergency contacts, select preferred provider or GP, as well as giving the user the option to opt into being an organ donor or give their data for research analytics.

A simple and straightforward way to schedule appointments with a general practitioner could also be part of the UI. In theory, the same system can be extended to make an appointment with dentist or chiropractor appointments.

4.5 Opportunities for smart contracts in proposed system

Considering the nature of communication and information being sent to and from healthcare personnel, smart contracts might be excessive and unnecessary. Trust is such an important part of the healthcare system, and we rely on giving personal information to doctors and other healthcare personnel and trust that they respect our privacy. As mentioned earlier, a consortium is used with only trusted entities in it.

Some processes might get automated with smart contracts, even though the need for trust is not present. Scheduling appointments at a health clinic, paying medical bills, and exchanging data between hospitals are some examples of how smart contracts can be used to increase efficiency. The need for smart contracts is not great in the BUC currently, but the availability of the technology is present.

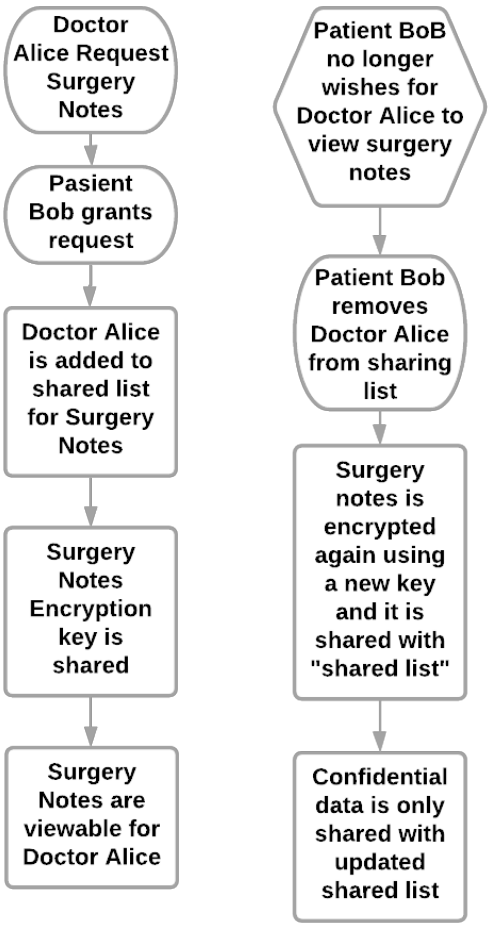


Figure 21: Flowchart of Medical override in case of medical emergency

4.6 Medical override

Giving the user ownership of their own data comes with the risk of the data not being accessible when the patient is unable to access or give access to the data. Therefore, providing doctors the opportunity to override the necessary restrictions to access the private journals in an emergency. By accessing the patient's private information, the doctor is legally bounded to give a reasoning for this action. The doctors are accustomed to patient-doctor confidentiality and the laws which affect their day-to-day work. By providing the doctors with a possibility to override permissions, it would only affect confidentiality aspect.

4.7 Third-party applications

As mentioned in chapter 4.4, by adding data from third-party applications, it can help the general practitioners in their medical examination of their patients. There will be a possibility to important all the data the third-party applications provide, but the patient can also provide predetermined information which can be filled in. This information could include nutritional values, height, weight,

exercise data, data from dentists and chiropractors, etc., and other relevant data. By providing the additional information, the GP can get a more holistic view of the patient's current health situation. Nutritional values may explain different levels of vitamins in the blood and data from Strava might provide insight in the conditioning of the patient.

The patient can choose which data will be imported, and they have the possibility to remove stored data at any time. Data which is produced by GP will be stored in a different location in the BUC UI to differentiate between the data sets.

4.8 Data analytics

Through the frontend of the BUC, the patient will have the option to donate personal health data for research purposes. This action is done easily by confirming which data the patient wants to share. It will all be conducted anonymously. If patients can easily share their data, the likelihood of the patients sharing data for research increases. When such action is conducted through a complicated process, the patient might not bother to hassle with it. It is therefore important that the option to share data is simple, intuitive, and easy to perform. The data being shared would be average statistics and general values which cannot identify an individual. Examples of data can be average increase in blood pressure over a week or month, average weight, trends in calorie intake, nutritional values, and the number of doctor appointments. All the examples would comprise of data collected through voluntary data sharing of all the users of the system.

The data being collected for analytics, could potentially be used as motivation for actors to participate in the blockchain by giving out unidentifiable data as a reward in a PoW system. Although the BUC system in this thesis does not use a consensus mechanism with a reward system to generate blocks, a reward system could be used, and data sharing is a way to reward nodes for generating blocks. Another positive feature of data sharing with blockchain is the increased security. Data will remain immutable after being shared, which gives additional validity for the users. In addition, it is anonymous, which maintains privacy for the users. The ability to provide anonymous data for research increases the desire to research and develop system based on blockchain technology. This could make the development of the technology progress at a faster rate.

4.9 Consensus mechanism

To ensure good performance on the network, the consensus mechanism plays a major role. Choosing a consensus mechanism like PoW will slow down the adding of new blocks drastically, but it will also keep the system public and decentralized. It is important to note what specifications are valued in the proposed system. Specifications that are valued highly are good performance, good scalability, low power consumption, transparency, secure, and at least some decentralization. Because BUC is not public, there is no need to utilize consensus mechanisms like PoW or PoS. They are power

hungry and are best suited for public blockchains. They also require incentives which would add another layer of complexity.

PoET is unfortunately slow compared to pBFT and PoA which also excludes it (Seeley, 2019, para. 8). It does have less power consumption compared to PoW or PoS, but it has no notable difference compared to pBFT and PoA. Either PoA or pBFT seems to be good options, because both show good performance and low power consumption. The biggest difference between the two mechanisms, is that PoA is more centralized compared to pBFT. This could be an issue since we do not want one single entity to have control over the system. pBFT will be the preferred consensus mechanism for the BUC system, because it is fast and retains some decentralized between all the entities on the network. Huang et al. (2020) compared their pBFT based system to other medical systems such as MedRec by Azaria et al. (2016). It showed great performance benefits to MedRec which utilized a PoW consensus mechanism. Figure 22 is a chart from Huang et al. (2020, p. 10)s research paper “A blockchain-based scheme for privacy-preserving and secure sharing of medical data”. Important to note that “our” is not the BUC, but the system proposed from Huang et al. (2020).

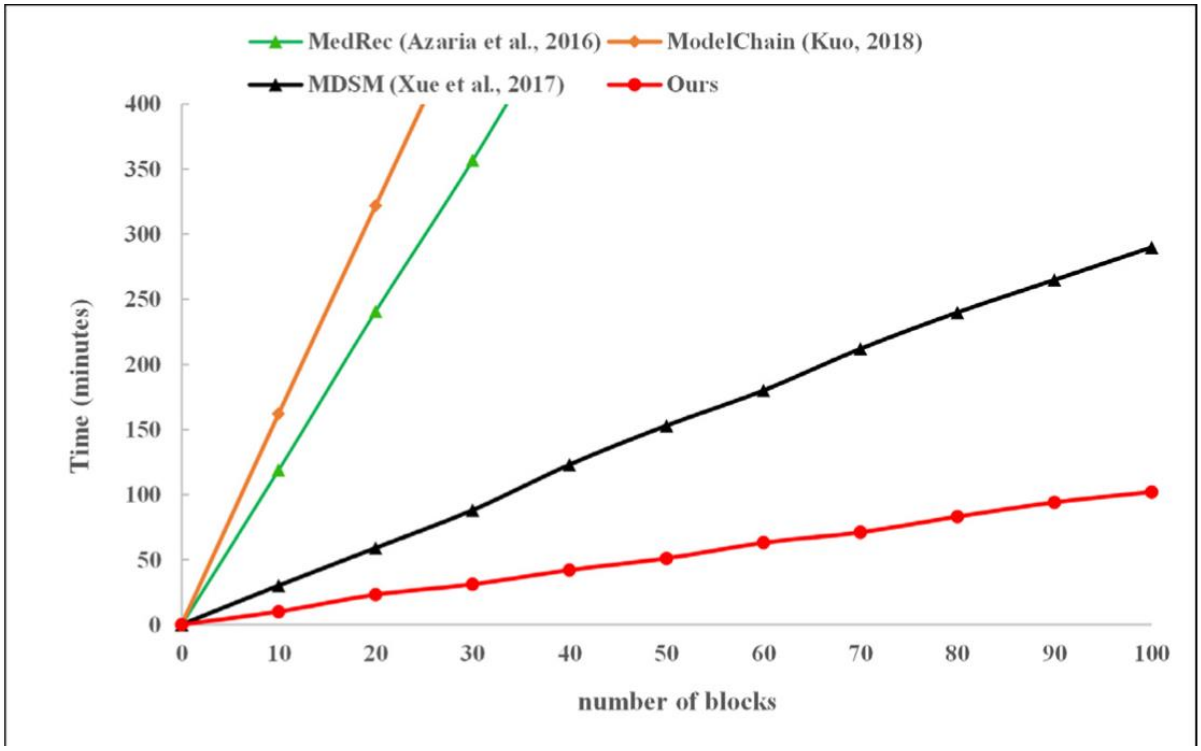


Figure 22: Comparison between different systems on block generation (Huang et al., 2020, p. 10).

5 Evaluation

This chapter looks at the system proposed in chapter 4 and performs an evaluation of said system. The evaluation will be done according to the methods outlined in chapter 3.2. These methods are a **case study** which will analyze BUC in the Norwegian healthcare sector, an **analytical evaluation** (performance based on prior research), and an **informed argument** which uses prior comparisons to other systems to evaluate the proposed system. As this is not a proof-of-concept study, any objective data from the proposed system regarding performance or security will not be offered. The data which are presented, will come from prior research associated with solutions which are being utilized. As mentioned earlier, the data metrics will only be an estimate (at best) and should be followed up with a proof-of-concept study in the future. The first section will look further into the current state of the Norwegian Healthcare systems. It will dive deeper into the laws and regulations which Norwegian healthcare is subdued to and describe how the Norwegian healthcare is divided and the current state of the sector. Lastly it will look at the proposed research goals and evaluate them based on the information gathered in the thesis.

5.1 Laws and regulations

With the increasing spotlight on privacy with the GDPR (2018), came a desire to own your own personal data. It is important that the users are aware of how the data being stored, can be used. Even though the GDPR does a good job of explaining this in the policies and terms of use contracts, the user is forced to consent to be able to use the software or system. With technologies like blockchain, which provide ledger and smart contracts, privacy is one of the advantages that comes with using it. The ability to manage what the data is used for and the ability to choose to deny unwanted use is critical. Blockchain has improved privacy preserving capabilities built in as a feature. These features will help aid in the battle for better privacy for the users of the system.

Norway is not a part of the EU, but they are a part of the EEA. GDPR Art. 3 states “This regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*" (GDPR, 2018c, para. 1)*. Because healthcare data is considered Personal Information (PI), the storage of the PI data is subject to the GDPR. Since PI information will be shared between different nodes and all the nodes contain the same information, questions regarding who owns and manages the different nodes arise. It is important to determine who has the responsibility of the data. Another issue regarding GDPR and blockchain is the immutable feature which blockchain offers. The GDPR art. 17 states:

> “The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the follow grounds applies:

A. The personal data are no longer necessary in relation to the purpose of which they were collected or otherwise processed;
B. The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
C. The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subjects objects to the processing pursuant to Article 21(2);
D. The personal data have been unlawfully processed;
E. The personal data have to be erased for compliance with the legal obligations in Union or Member State law to which the controller is subject;
F. The personal data have been collected in relation to the offer of information society service referred in Article 8(1)" (GDPR, 2018b, para. 1)

This is important because blockchain by nature does not allow deletion of data, these laws must be discussed or altered before implementing blockchain. It is possible to encrypt data on the blockchain and then delete the following keyset which will render the data unreadable. This is currently a workaround to implement data corruption, but not a good solution in the long term as the data still is located on the blockchain. GDPR Art. 5 (c) and 5 (e) concerns with the 'data minimization' and 'storage limitation' principles (GDPR, 2018a). Data stored on blockchain will be replicated on each individual node which will make multiple copies. 'Data limitation' involves limiting the access to the data. With a strict interpretation of the system, one could argue that the sharing of data between nodes is not necessary. This could require a clarification before any implementation of blockchain can see daylight in Europe.

The Norwegian law Pasientjournalloven §1 states that "Giving patients and users health aid of good quality by being provided relevant information in a swift and effective manner, meanwhile it must also protect the information from unauthorized people while also securing the patient and users privacy, patient-security and right to access information and complicity" (Helse- og omsorgsdepartmentet, 2015a, para. 1). This can be divided into several parts which are essential. **First** is the quick and effective access to relevant information to help provide healthcare aid of good quality. The **second** part is to protect this information from unauthorized people. Any health-related information is a privacy concern and when being accessed, the data is being transferred from a database to medical personnel. As discussed earlier, this can be a cause of security concern due to the many interception and manipulation techniques available to malicious actors. That is why it is important to provide a secure way to store and transfer the information. The **third,** and last part of the law, says that it should secure the patients and users privacy and right to access information and complicity. This is further explained in Helseregisterloven § 24 and 25 which says that "The registered [person] has the right to information and insight [into this information]" (Helse- og omsorgsdepartmentet, 2015b, para. 46). The next paragraph states that "The registered [person] has the right to insight into who has accessed, or has received data

regarding information that can be tied to the registered person’s name or social security number” (Helse- og omsorgsdepartmentet, 2015b, para. 50).

A goal for the healthcare sector is to unite all their systems. But with stricter regulations for privacy and the increase of data breaches (Whitney, 2021a, para. 2), changes are hard to pass through. A big benefit of a united system is the interoperability between systems. Today's healthcare uses separate systems and according to informant ID λ3, if a doctor needs logs from another hospital, they need to request them. The hospital which has the logs stored must then export the logs. Finally, the hospital that requests the logs, must import the logs from the transfer channel. BUC will reduce the need for importing and exporting data as it is one singular system. A consortium blockchain will provide decentralization to this aspect. This means that no one owns all the data, but instead, patients own their own data, which is on the network. Blockchain benefits from using strong cryptographic protocols and smart contracts. As blockchain is built up with multiple machines (nodes), the data exists on more than one of them, which again improves the availability for the system. Because of the tamper detection that blockchain has, the technology provides data verifiability and data transparency.

In the Norwegian healthcare system, third-party applications are hard to implement due to regulations. The only example is blood sugar values for diabetics. Here, a new blood sugar reader is placed on the user. The chip can read the blood sugar level and has a near-field communication (NFC) chip, which can be scanned by the user's phone. The user has a specific app which takes the data and exports it from the phone to the hospital's cloud server. The app also displays the values for the users to manually adjust the insulin pump. Even though an automatic pump has been created, it is not currently in use in Norway. Based on a conversation one of the authors of this thesis had with an IT employee in the Norwegian healthcare sector, the above-mentioned issues created some headache for the privacy regulators in Norway. In the end they concluded that the benefits outweigh the risks. They gave the users the option to use the service, but the users had to sign a Terms of Use which mentioned the risk of sharing data with the cloud. However, this is also the only example in which third-party applications have benefited the users in Norway. There is a lot of potential remaining in this area. Data from various health and fitness apps such as MyFitnessPal, Strava, Apple Health and Fitbit can give medical doctors a great insight into the real health status of a user. Not only does exercise and nutrition impact how well a person performs in various activities, it also gives a good indication of their cardiovascular status. Nutrition can also explain if different blood values are higher or lower than typical or give reasoning to their current weight status.

When it comes to third-party data, the apps can be created outside of Norway, which currently is not considered safe by default, but exceptions can be made (as with the diabetes example). BUC is not currently in compliance with the laws if one concretely interprets them. As BUC import third-party data and is blockchain based, it is crucial for the laws to be changed to make it legal.

5.2 Norwegian healthcare Sector

The infrastructure in the Norwegian healthcare sector was developed separately from each other. This has caused the different sectors to develop independently from each other in terms of using different systems and different suppliers for their respective systems. The result is potentially slower exchange of data between different regions and between the different systems. The healthcare sector in Norway is divided into four regions (Helse- og omsorgsdepartmentet, 2020):

- **Helse Sør-Øst RHF**. The southeast region, which is the largest region and is responsible for 11 hospitals or other health facilities.
- **Helse Vest RHF**. The west region, which is responsible for six hospitals or other health facilities.
- **Helse Midt-Norge RHF**. The middle region, which is responsible for four hospitals or other health facilities.
- **Helse Nord RHF**. The north region, which is responsible for six hospitals or other health facilities.

Each region uses ICT consultants to further complicate the structure

Every region operates with different IT systems, and sub-sections of the regions also use different systems. This makes the communication process more complicated and slows down the communication flow. As with every other sector, time is money and poor communication flow results in increased cost. Unifying the regions into a singular system, where information is stored in the same architecture, will increase workflow, and minimize time spent exchanging data. Blockchain technology will increase security and privacy with strong encryption and immutable ledgers. It can also help maintain a decentralization within the system, even though it is being unified.

An estimate from Deloitte was made of the current expenditure from the Norwegian Government on national healthcare. They estimated the cost associated with development, maintenance and work with registers which could be enriched by blockchain, to between 11 000 000 000 and 13 000 000 000 NOK (Deloitte, 2018, p. 20). These are potential areas which blockchain will affect and might help reduce the cost associated with them.

Lysneutvalget was tasked in 2014 with discovering digital vulnerabilities in the society by the Norwegian Government. They highlight that critical infrastructure are dependent on value chains which are comprehensive to get an overview of. The value chains can often extend into different sectors and countries. They also mention that this is amplified in the health sector, where the responsibilities are divided even further (Direktoratet for e-helse, 2019, pp. 22-24). Christine Bergland, former director for e-health in Norway, said in an interview with tu.no (Valmot, 2020, para. 4) that there are

around 17 000 different actors in the health sector, which makes the implementation of online journals difficult to work with. Reading Direktoratet for e-helse (2019, pp. 24-25), we can understand that this could be due to lack of investment in information technology (IT) and legacy code that is dependent on older IT solutions. “A lack of IT security competence appears as one of the bigger challenges when it comes to IT security” (Direktoratet for e-helse, 2019, p. 22). From this quote we can understand that the authors of the report believe that by having better educated and more aware personnel is a step in the right direction. The paper also mentions that a wide range of attack vectors are used against the hospitals and patients. Both private and state actors are represented as attackers.

With the BUC system, the four regions will be unified as one. It will mitigate any import and export issues and reduce the transfer time of data. Data will also be more securely available to both users and medical professionals. No exact cost savings are presented since no information is presented in the literature of the complicated savings of blockchain technology in the healthcare sector. It can also be beneficial for security analyst to monitor one system instead of 4 different ones.

5.3 Performance evaluation

Comparing a blockchain solution with a regular database solution (as is being used today) is also important. Performance-wise a blockchain solution would be slower than a regular database. In the paper by Stamatellis et al. (2020, pp. 9-11) they compared their own solution (PREHEALTH) with a regular database (PostGresSQL database) and two other blockchain solutions (MedRec-Azaria et al. (2016). and Blockstack-Ali (Ali, Shea, Nelson, & Freedman, 2017). The figure (24) is taken from “*A* privacy-preserving healthcare framework using hyperledger fabric” from Stamatellis et al. (2020, p. 9). It displays the results from the comparison.

From figure 24, the time to read and write data is quite slow compared to a regular database in the lower numbers of EHR. But when the amount of EHR increases (bigger database), the read time difference is minimized compared to the blockchain solution with 136.19 ms (PostgresSQL) vs 183ms (PREHEALTH). Unfortunately, the testing stopped there, but we can expect the continuation of this trend when the database size increases. This is an important point as the need for healthcare increases with the ever-increasing population both in Norway and in the world. At one point the current databases will become as slow as the blockchain solutions, which results in less downsides by switching to a blockchain based solution. It will be important to consider the cost of scalability vs the improved data handling at larger scale. Because blockchain offers better handling on a bigger scale it could be better suited for the future since the population is still increasing. The cost of equipment to make a system big enough to handle the data (scalability) will be the cost evaluation which needs to be conducted.

Number of Records:		10	100	1000	10,000	100,000	1,000,000
PREHEALTH	Read Data Time	183 ms	183 ms	183 ms	183 ms	183 ms	183 ms
	Write Data Time	58 ms	58 ms	58 ms	58 ms	58 ms	58 ms
PostgresSQL Database	Read Data Time	1.73 ms	1.79 ms	2.38 ms	8.76 ms	43.52 ms	136.19 ms
	Write Data Time	4.32 ms	4.48 ms	4.47 ms	4.37 ms	4.39 ms	4.45 ms
MedRec—Azaria et al. [29]	Read Data Time	177 ms	186 ms	194 ms	199 ms	205 ms	210 ms
	Write Data Time	81.5 ms	86.9 ms	79.6 ms	71.6 ms	63.2 ms	79.6 ms
Blockstack—Ali et al. [33]	Read Data Time	360 ms	360 ms	360 ms	360 ms	360 ms	360 ms
	Write Data Time	530 ms	530 ms	530 ms	530 ms	530 ms	530 ms

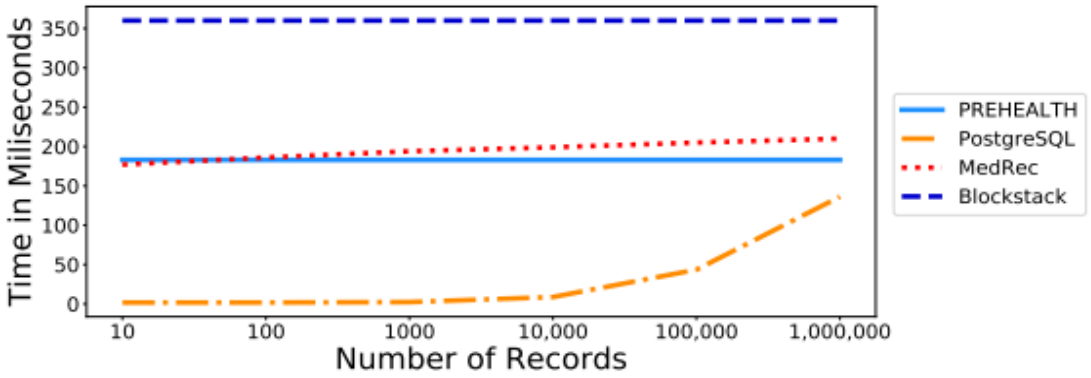


Figure 23: Performance comparison between blockchain solution and SQL database (Stamatellis et al., 2020, p. 9)

5.4 BUC in the Norwegian healthcare sector

Over the last years, users have become more critical to the handling of their data. In 2018, the European Union (EU) released GDPR which helps regulate the data protection laws in the EU. Users were then made more aware of this topic. This is when the question arose regarding how sensitive data is handled by the national healthcare. Users are forced to trust that their data is safe with the notional healthcare institution. Throughout this thesis a lacking connection between the different entities were discovered. If one had a surgery at a hospital, and needed a follow-up at the local general practitioner, the GP would not always have access to the epicrisis from the surgery. This is due to the utilization of different systems which was discussed earlier. From this, the idea of a more user-centered and user-friendly healthcare system arose. To give more control to the user over their own data, but in the meantime making it easier to exchange and share information. An interesting next step was to utilize blockchain to increase the privacy and security of the new system. Unfortunately, blockchain is not only positive. After monitoring blockchain's success in the cryptocurrency domain, it was an intriguing technology.

The results from the evaluation show an improvement in not only security and privacy, but also user-friendliness. With databases in the magnitude which the healthcare operates, one could speculate that blockchain performance has already surpassed current database solutions (based on the performance metrics presented in 5.3). A

user-centric system does not necessarily have to utilize blockchain technology. In other words, there is a possibility to gain these two different benefits at different stages. Since there is an increase in attacks towards the healthcare sector during the Covid-19 pandemic, it is uncertain that it will continue after the pandemic passes. Another important aspect which was brought up by informant id $\lambda 2$; "The healthcare sector is mostly exposed to ransomware attacks and not by specific and specialized attacks from bigger threat actors" (E.g APT[8] groups). This was also confirmed by $\lambda 3$. We could also speculate that the root of development can be traced back to the health department, operations and culture. According to $\lambda 2$, the Norwegian healthcare sector lacks the incentives to develop and trial new technologies. As he explained to us, there were no active groups or single entities who actively tried to improve the current system with new technology. $\lambda 3$ found this statement interesting but justified it by sharing his opinion that the Norwegian Healthcare sector never wanted to test any technology younger than 10 years. In addition, it had to be well tested before they would consider using the technology. This supports the argument that they have little interest in new technology, but if there is good evidence for one it can be considered in the future. For us, this approach resembles a passive approach to new technology and solutions. An active approach would be a research division within the department to investigate and pilot new technologies. $\lambda 3$ also brought up an interesting opinion; is there a need for a blockchain solution if the current system holds up in the current situation? This question will be discussed further in section 6.3, but he had a valid point. It also reflects his other position in the earlier finding.

We can also see the current integration and attention which mHealth receives in the health domain. mHealth is defined by WHO as "use of mobile and wireless technologies to support the achievement of health objectives" (WHO, 2011, p. 9). From $\lambda 3$, the moving field and opportunities within mHealth will have a big impact in the coming years. This will be done regardless of the storage medium being utilized. Connection between apps like MyFitnessPal, Apple Health and Strava will still be a long way from being incorporated into such a system, but more niche applications which help certain monitoring systems will see the first benefits of mHealth. Examples of this are heart monitors, fall detection devices and blood pressure monitors. The IoT generation is here with the aid of 5G.

[8] APT groups are Advanced Persistent Threat groups, usually connected to a nation state which. APT typically has good funding and gives them the opportunity to gain unauthorized access to computer networks and remain undetected there for longer periods of time. (Lord, 2018)

6 Discussion

This chapter presents a discussion of the evaluation findings in light of previous works on this topic. It is presented as opportunities and hindrances of blockchain in the healthcare sector. Further, this chapter will discuss the proposed research goals and evaluate them based on the information gathered in the thesis. Later parts of the chapter elaborate upon some relevant projects in the EU with regards to blockchain and the healthcare sector. In the end this thesis' contribution to the literature and limitations of the thesis are presented.

6.1 Blockchain in the Norwegian healthcare system

After performing an SLR and conducting interviews, the interest in new technology might be on the rise. There are different reasons for this. Some of them are IoT and 5g (mHealth), as well as how covid-19 has made many aspects of our daily lives, online activities. There is good reason to believe that remote doctor's appointment and distance consultation will become a regular practice following the COVID-19 pandemic. Information gathered in the interviews are pointing towards a lack of motivation and resources allocated to innovations. The Norwegian healthcare sector often look towards other healthcare systems and implements systems that have been thoroughly tested.

Considering the previous research presented in chapter 2.2 and the current environment of the Norwegian healthcare system, we can see there is a distinct disconnect. The lack of motivation from the Norwegian healthcare to investigate future technologies is low and the current research on blockchain is too small within healthcare. The proof-of-concept studies show some good results, but also presents downsides. Therefore, Norwegian Healthcare should investigate further into new technologies and trial them. IT security is a rapidly growing field due to the increase of cybersecurity related issues with hackers, ransomware, and APT groups. Technologies which can help withstand the increasing pressure on the current systems will only benefit the Norwegian healthcare in the future. This comes at a major cost, which for now is prioritized to the treatment of patients.

This next part of the discussion will look at some opportunities and reasons for implementing blockchain technology in the healthcare sector, as well as some hindrances that could make implementing blockchain in their systems difficult.

6.2 Opportunities of blockchain for security and performance

All the reviewed studies underline the strong security incorporated in blockchain. The reason for this security is the strong encryption being utilized by the technology. With the benefits of the blocks of data being stored in a chain (see chapter 2.1.2) it creates an immutable ledger which further increases the security. It is impossible to change the data which has been approved to the ledger. Malicious actors cannot manipulate data which is stored on the chain without being detected. A typical blockchain attack

which is exemplified throughout the literature is the 51% attack. This demonstrates that if one entity manages to take control over 51% of the nodes in a system, it can control what is being accepted to the blockchain and which information is discarded. This attack will be irrelevant since the BUC is utilizing a consortium instead of a public blockchain. A consortium only allows approved entities on to the system.

Performance has also seen promising results in the literature. The literature shows improvements related to the scalability and previous issues with performance. Based on evidence found in the literature review, blockchain-based databases do not provide additional performance compared to a regular Database Management System (DBMS). An important caveat is the use of blockchain as a search index layer. This technique showed similar to slightly favorable performance outcomes for the blockchain system. Even though this area needs further work to improve and testing to ensure the stability, it seems promising.

Another important aspect which is crucial for healthcare services is uptime. Even though the current system has reported hundred percent uptime in 2019 (Norsk Helsenett, 2019, p. 4), the system utilizing blockchain will have the information available on as many nodes as desired (the more is better). Each node will contain the exact same data which increases the chances of accessing the data. The physical range to a node will also be reduced with blockchain, but because the low latency in today's communication, the benefit of changing to blockchain technology will likely be negligible, especially in Norway when a high percentage of the population (>86%) have access to optical fiber (Enger, 2019).

BUC is a consortium based blockchain which allows for only invited entities to participate. The entities manage a node which adds new blocks to the ledger with the pBFT consensus mechanism. An acceptance quality control should be performed to ensure the validity of these additional entities. Initially the system can be used for the government and then add more entities gradually.

6.3 Hindrance of blockchain for security and performance

As presented in related works, many of the proposed systems mentioned scalability and performance as potential downsides of blockchain technology. The reason why scalability and performance are an issue is due to the immutable feature which will not allow any changes to be made to the ledger. If anyone wants to update or change any of the information on the ledger, it needs to be added. When data is being added, but never removed, the system will grow at an exceptional pace.

The systems that saw the most promising potential were the ones that used blockchain as a security layer but did not use blockchain to store data. This points to both scalability and performance as being the main hindrances which might be too big to overcome in the near future.

Based on what was learned during interviews, some IT professionals are skeptical when it comes to implementing blockchain. This is not necessarily because it is viewed as a bad technology, but because they do not see the reason to spend resources on changing systems that work. They also do not see how blockchain will significantly improve the systems, or if it improves them at all.

Even though blockchain provides increased privacy and security for data, blockchain might not be needed. Current systems do provide sufficient privacy and security, and they follow strict guidelines from Normen and the GDPR. On one side we see that utilizing an up-and-coming technology like blockchain, which has merits for improved security and privacy could be looked as future-oriented. On the other side we see that it could be an expensive move as new technologies warrant thorough testing. Testing is an expensive part and often time consuming. The managers and leaders need to make a financial decision regarding where to allocate the money in the best interest of the patients. Unfortunately for IT, this typically means a lot of money being allocated towards the health of patients (since it is healthcare) and a smaller portion towards operations. It is important to note that IT has become a critical infrastructure to remain operational and it could see bigger allocation in the future (Regjeringen, 2018, para. 4). This is the typical approach we see today from the Norwegian healthcare, which takes a more leaned back approach to new technologies. As previously mentioned from the interview with expert λ3, any technology younger than 10 years is not even considered due to the limited testing.

During the interviews, questions regarding the need to update the systems and if the current systems are good enough, arose. On the side of the argument for updating the systems are staying ahead of malicious attackers, as well as improving the user experience for the healthcare personnel and the patients. As mentioned earlier, the cost of designing and implementing these new systems will likely be high. If the current systems are “good enough” there will not be incentive from the Norwegian state to make the systems better, especially considering the money that is required to develop a new system. It is possible the new systems would save more money in the long term than it would cost to implement. However, predicting the future can be difficult, and as long as the incentives are not present, we are unlikely to see any reasonable motivation in this area. The only aspect which can spark interest is if the efficiency of the proposed system can be shown to be good in practice. This raises the question; do we really need blockchain?

A cost of being careful when it comes to implementing new technology could be that you do not get to reap the benefit that others do. Example of this could be if blockchain technology reduce the overall cost of the healthcare sector by 10%. If the Norwegian healthcare waits ten years before implementing the technology, they will miss out on 10% cost reduction over a ten-year period.

Regardless of what the choice is for improving or just changing the current system, a risk assessment is recommended. Outweighing the pros and cons and having a specific proof-of-concept study with numeric values showing the positive versus the negative can help ease the decision. It is important to set limits for what is considered too high risk and be critical of the results of the assessment. Handling risk is a very complex process and should be approached with the right set of tools and the right set of people. A privacy-by-Design is also recommended, even though blockchain already has this intuitively built into the technology. From the Deloitte report (Deloitte, 2018, p. 68) on blockchain in the public sector, such an approach can still be important as other aspects of the system need privacy centered design.

6.4 Discussing the research goals

What are the opportunities and hindrances of blockchain in the Norwegian healthcare system regarding security, privacy, and performance?

This thesis has presented several opportunities and some hindrances when it comes to implementing blockchain technology in the Norwegian healthcare sector. Blockchain can provide possibilities with increased privacy, strong encryption, immutable ledgers and up time. The problem is that some of the benefits also are the hindrances. The immutable ledger is good to ensure data is not being manipulated, but it also causes scalability issues. Unfortunately, these scalability issues are not easily fixed as the size of such a system is quite large. Of course, some solutions to minimize the impact have been promoted from Fan et al. (2018) and (Chen et al., 2019) with their security layer approach. The security layer is the search index layer which all users will interact with and stores the data pointers[9] to their patients' EHR in the database. A simple illustration of the security layer can be viewed in figure 23.

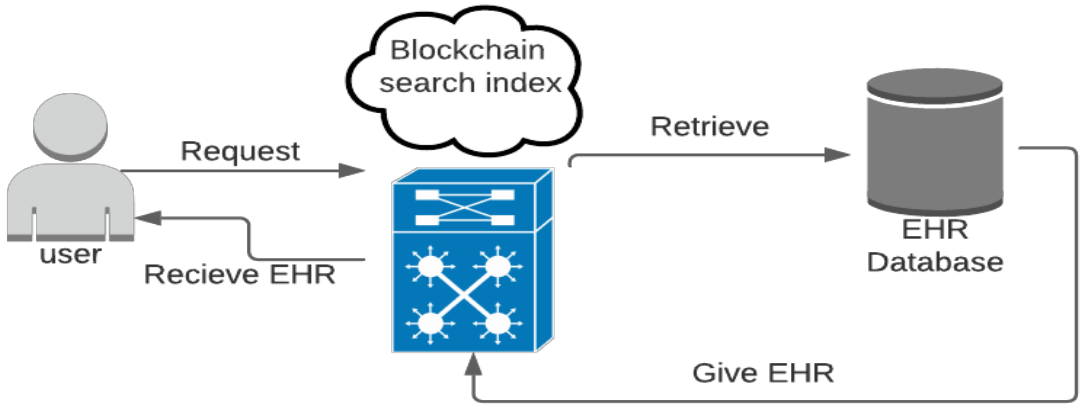


Figure 24: Security layer illustration

[9] Data pointer is a variable which holds the address of another variable or function (Microship, Unknown).

The other possibility is to store the data in a blockchain database, but this will cause a scalability issue. This issue comes down to some key aspects which need to be considered. One aspect is if the technology is good enough, and if in the future technology advancement has improved so much it minimizes the scalability issue. Since it is only an issue due to limited resources of storage. The other key aspect is cost. If a blockchain database is desired, currently the cost of adding massive amounts of storage will limit the size of the system. Prices of storage are as of today (03.05.2021) $1.318 per Terabyte of data (Diskprices, 2021). When every node needs to store the information, the amount of money needing to be spent on storage goes up rapidly as more information is added to the blockchain.

Blockchain gives security improvements in several different ways as discussed by Fan et al. (2018, pp. 7-9), Chen et al. (2019, pp. 6-9), Darwish et al. (2020, pp. 6-8). The tamper proof storage (immutable ledger) helps ensure the data integrity. If any efforts of tampering with the data is conducted, it will be discovered fast, as the blockchain will not work as intended due to the chain storage mechanism. Any takedowns of the system will also be hard as it consists of multiple nodes (as many nodes as wanted by each entity), and all of them contain the same information. This is different from a single point of attack on typical databases. Not only will it be hard to take down all the nodes, but this has the benefit of if one goes down, all the other nodes contain the same information. This makes the uptime quite reliable.

The access mechanism also provides anonymity of data to the system. It helps protect the privacy of the users. Zero Knowledge proof also aids in the protection of user privacy (Fan et al., 2018, p. 9).

There are both benefits and drawbacks with both solutions, but the best suited for healthcare in 2021 is most likely the security layer. Currently we can see that blockchain is probably a few years from even being considered in the Norwegian healthcare system. The technology still has big scalability issues. That does not mean that trying to develop a more decentralized infrastructure in Norway is a bad idea. A lot of the problems we see in the current system would not need blockchain to be solved. Performing an overhaul on all the systems in the healthcare sector will cost a lot of money, and the benefits might not outweigh that cost. Blockchain could be implemented later if needed. Based on the research in this thesis, the cost is just too big to justify a blockchain database at this point in time

How could a user-centered system be designed in relation to third-party applications and privacy?

To accommodate this research goal, we employed a DSR to design the artifact. The data gathered in the research showed that regarding scalability, some consensus mechanisms appear to be better suited for the proposed system than others. PoW requires mining and is slower, while pBFT is based on a voting system, which makes processing a large amount of data significantly faster. Therefore, when designing the

system, it seems likely that a pBFT consensus mechanism will be better suited for the system than most other consensus mechanisms.

Using blockchain opens up for the possibility to use smart contracts. While it is not immediately apparent how much of a benefit this could be, due to the nature of the blockchain having the option to use them if the need for them is discovered the proposed system will allow for that.

As presented in chapter 4, different technical solutions are possible for a more user-centered system. But the fundamental change is to focus on the user as a main objective and then develop an ease-of-use system around them. There are big benefits to modernize the current healthcare system and unify it. In Norway alone, it will vastly improve the workflow between regions and healthcare personnel. No downsides are apparent by doing such a change other than financial cost.

The BUC system is user-centered by giving power of sharing information to the user. It also allows for importing third-party data. Blockchain helps with privacy, as well as the consortium extends the privacy by only allowing trusted entities to view the EHR's.

6.5 Relevant projects in the EU

6.5.1 EBSI

In the future networks such as European Blockchain Service Infrastructure (EBSI) can help bring blockchain and the healthcare sector together. EBSI is an infrastructure which works across borders in the EU, Norway and Liechtenstein (CEF-Digital, Unknown, para. 1). A user account is created on the network and the account can be used to sign into taxes, apply for jobs (either nationally or internationally), or studies. Solutions like this already exist in the national level (MinID[10] for Norway), but it cannot be used outside the Norwegian borders. An infrastructure like EBSI will verify the user and by having it in an immutable ledger, everywhere, will make it tamper resistant. If the proposed design study in this thesis could later be added to such a system with the public profile open and having sensitive data stored off-chain, it would vastly improve the versatility of the healthcare system. It will also aid if any medical accidents happen outside the Norwegian borders.

6.5.2 My health my data

My health my data (MHMD) is an EU funded project that aims to provide an anonymous and secure way of storing and publishing data for research purposes. The project uses smart contracts to automate data transactions, and provides trusted identities of data owners and users (Cyberwatching, 2019, para. 4). The project is in compliance with

[10] MinID is an authorization tool which gives access to public services with security level 3 in Norway(difi, 2021).

the GDPR because it allows for tracking of data transactions, accountability and the automation of transactions because of smart contracts. The users of the system gain control compared to current systems by allowing them to set customized consent preferences. The goal of the project is to create an information marketplace, where access to data is an incentive to invest and participate in the peer-to-peer network (Cyberwatching, 2019, para. 3-5) (European Commission, 2019).

MHMD touches on many topics covered in this thesis. They want to include the users more and give them more control over their own data. Blockchain is the preferred technology for this project. This shows that there is motivation for the use of blockchain in the healthcare sector. If this initiative is shown to be successful and profitable, it could mean the Norwegian politicians would be more motivated to trial blockchain in the Norwegian healthcare systems.

6.6 Contributions to the literature

During this DSR, there have not been any new revelations compared to the prior work done by, for example, Fan et al. (2018) or Azaria et al. (2016), but a more specific look at how a rejuvenated Norwegian healthcare IT system can be built to better the usability of it has been proposed. A gap in the literature was highlighted as prior research either focused on a blockchain EHR or a user-centric system. This thesis presented an artifact as a combination of both and specifically tailored to the Norwegian healthcare system. The current systems in Norway focuses on operations within the region or locally on the hospitals, but there is a lack of focus on including the patients. This will likely become a bigger focus point in the coming future as patients will increasingly demand more control and interaction with the system. It is our belief that Google and Apple have shaped the technology industry in such a fashion that users expect the ease of use and integration in other platforms as well. This expectation or need has become clear to the designers of the healthcare department and designers of the next system.

BUC presents a new idea of how healthcare IT infrastructure can be made. New technologies such as blockchain, show good metrics in security aspects, but that does not mean it will be suited for everything. BUC proposes a united healthcare system regardless of technology, which would most likely increase the usability and communication flow between hospitals in Norway. The current environment, with data scattered around in different databases, is not in line with the new regulations in the GDPR (2018). The GDPR regulations further emphasizes the need for a united system and increased privacy in the Norwegian healthcare sector. This thesis has contributed to the literature by looking at a specific sector; the Norwegian healthcare sector. This was done by proposing an artifact in the form of BUC and interacting with the field.

From this thesis, we learned to incorporate previous research and environment status into improving the Norwegian Healthcare system. By conducting an SLR, we gathered

information around the blockchain technology and user centered EHR systems. The data helped enrich our knowledge on the technologies and their performance and security metrics. The interviews gave us good insight into the current environment and status of the Norwegian Healthcare sector. It also explained the current IT culture in this domain. In addition, we learned to utilize an DSR to design our own artifact (BUC) and evaluate it.

A notable limitation with this thesis is the lack of proof-of-concept. A theoretical system with theoretical evaluation of it has been proposed. All the metrics are based on prior studies on the different solutions. Such a method will leave performance and scalability metrics at best as estimates. Another notable limitation is the number of interviewees. 12 experts were contacted, but only 4 responded. To compensate for the lower number of interviewees, a more comprehensive SLR was conducted. This will put the contribution to at Technology Readiness Level (TRL[11]) level 2 (General Annexes, 2015). Compared to the prior work in the field, which mostly consisted of proof-of-work DSR (TLR level 3), this thesis separates from them by also including the specific user-centered system. It is also important to underline, the reason for this thesis is to spark the idea for a better healthcare system. It will require further work, better refinements, and testing before such a system can be implemented in the healthcare sector.

[11] TRL is a method for estimating the maturity of technology during the building phase

7 Conclusion

This thesis has proposed a user-centered design architecture enhanced with blockchain technology. In theory, the security and privacy protection level can be better compared to the current one used by the Norwegian Healthcare System. Blockchain shows improved security, privacy, and similar performance at bigger database sizes. Unfortunately, blockchain also has issues with lower quantity performance and scalability issues regarding expenses.

The Norwegian healthcare sector should on the other hand look further into unifying the healthcare regions, even if they decide not to use blockchain technology to do so. Not only will it allow for better workflow, but it can help with security from an operational standpoint. The department of health should review the current system and allocate more time and money towards improving it. If the philosophy of changing a system continues, where the Norwegian healthcare sector looks towards successful improvements in other systems before implementing it into their own, it will take a considerable amount of time before new technologies are implemented in the Norwegian healthcare sector. This will result in the Norwegian healthcare systems always lagging behind modern technology.

Further testing and development of blockchain to solve the scalability issue will be warranted before any recommendation can be made for the utilization of blockchain in the Norwegian healthcare sector.

8 References

Algorand. (Unknown). Algorand's Permissionless Blockchain. Retrieved from https://www.algorand.com/technology/permissionless-blockchain

Ali, M., Shea, R., Nelson, J., & Freedman, M. J. (2017). Blockstack: A New Decentralized Internet. Retrieved from https://docs.huihoo.com/blockstack/Blockstack-A-New-Decentralized-Internet.pdf

Annexes, G. (2015). Technology Readiness Levels (TRL). Retrieved from https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

ATP. (2019). Secure your data with AES-256 encryption. Retrieved from https://www.atpinc.com/blog/what-is-aes-256-encryption

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). *MedRec: Using blockchain for medical data access and permission management.* Paper presented at the Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016.

Benvenuto, C. J. (2012). Galois Field in Cryptography. Retrieved from https://sites.math.washington.edu/~morrow/336_12/papers/juan.pdf

Bosri, R., Uzzal, A. R., Al Omar, A., Bhuiyan, M. Z. A., & Rahman, M. S. (2020). *HIDEchain: A User-Centric Secure Edge Computing Architecture for Healthcare IoT Devices*.

CEF-Digital. (Unknown). Experience the future with the European Blockchain Services Infrastructure (EBSI). Retrieved from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

Chatterjee, S., Xiao, X., Elbanna, A., & Saker, S. (2017). *The Information Systems Artifact: A Conceptualization Based on General Systems Theory*.

Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems, 95*, 420-429. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167739X18314134

Chitu Okoli. (2015). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Communications of the Association for Information Systems, 37*(43). doi: 10.17705/1CAIS.03743

Chukwu, E., & Garg, L. (2020). A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *IEEE Access, 8*, 21196-21214. doi:10.1109/ACCESS.2020.2969881

ComputerPhile (Producer). (2019, 22.11.2019). AES Explained (Advanced Encryption Standard). Retrieved from https://www.youtube.com/watch?v=O4xNJsjtN6E&ab_channel=Computerphile

Creswell, J. W. (2015). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. USA: SAGE publications Inc.

Cyberwatching. (2019). MYHEALTHMYDATA: A NEW PARADIGM IN HEALTHCARE DATA PRIVACY AND SECURITY. Retrieved from https://www.cyberwatching.eu/projects/1479/myhealthmydata-mhmd/news-events/myhealthmydata-new-paradigm-healthcare-data-privacy-and-security

Darwish, M. A., Yafi, E., Al Ghamdi, M. A., & Almasri, A. (2020). Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid

Algorithm. *Arabian Journal for Science and Engineering*, 1-10. Retrieved from https://link.springer.com/article/10.1007/s13369-020-04394-w
Deloitte. (2018). Distribuert sannhet - potensial og barrierer for blokkjeder i norsk offentlig sektor. *Distribuert sannhet*, 85. Retrieved from https://www.regjeringen.no/contentassets/f5db1086d5324ec786f440afcb5cde52/blokkjeder_offentlig_sektor_deloitte.pdf
difi. (2021). MinID. Retrieved from https://eid.difi.no/nb/minid
Direktoratet for e-helse. (2019). *Overordnet IKT-ROS for helse- og omsorgssektoren*. Retrieved from e-helse: https://www.ehelse.no/publikasjoner/overordnet-risiko-og-sarbarhetsvurdering-for-ikt-i-helse-og-omsorgssektoren/Overordnet%20risiko-%20og%20s%C3%A5rbarhetsvurdering%20for%20IKT%20i%20helse-%20og%20omsorgssektoren%20(PDF).pdf
Diskprices. (2021). Diskprices. Retrieved from https://diskprices.com/
Enger, H. J. (2019). 86 prosent har tilgang til bredbånd med høy hastighet. Retrieved from https://www.nkom.no/aktuelt/86-prosent-har-tilgang-til-bredband-med-hoy-hastighet
Ethereum. (2021). Decentralized Storage. Retrieved from https://ethereum.org/en/developers/docs/storage/
European Commission. (2019, 31 December 2019). My Health - My Data. Retrieved from https://cordis.europa.eu/project/id/732907
Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of Medical Systems, 42*(8), 1-11. Retrieved from https://link.springer.com/article/10.1007%2Fs10916-018-0993-7
Fatokun, T., Nag, A., & Sharma, S. (2021). Towards a Blockchain Assisted Patient Owned System for Electronic Health Records. *Electronics, 10*(5), 580. doi:10.3390/electronics10050580
Frankenfield, J. (2020). Proof of Elapsed Time (PoET) (Cryptocurrency). Retrieved from https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp
Frankenfield, J. (2021). Proof of Stake (PoS). Retrieved from https://www.investopedia.com/terms/p/proof-stake-pos.asp
GDPR. (2018a). *Principles relating to processing of personal data*. Intersoft Consulting Retrieved from https://gdpr-info.eu/art-5-gdpr/
GDPR. (2018b). *Right to erasure ('right to be forgotten')*. Intersoft Consulting Retrieved from https://gdpr-info.eu/art-17-gdpr/
GDPR. (2018c). *Territorial Scope*. Intersoft Consulting Retrieved from https://gdpr-info.eu/art-3-gdpr/
Geir Sverre Braut. (2020). Epikrise. Retrieved from https://sml.snl.no/epikrise
Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *Managment INformation Systems Research center, University of Minnesota, 37*(2), 337-355. Retrieved from https://www.jstor.org/stable/43825912
Hackernoon. (2020). Zero Knowledge Proof: Explain it Like i'm 5 (Halloween Edition). Retrieved from https://hackernoon.com/eli5-zero-knowledge-proof-78a276db9eff
Hafez, A., & Mokhtar, A. (2010). A new chaos Advanced Encryption Standard (AES) algorithm for data security. Retrieved from

https://www.researchgate.net/figure/The-shift-row-step-representation_fig2_235801070
Hart, C. (1998). Doing a Literature Review. *SAGE publications*. Retrieved from https://www.cuzproduces.com/producinganew/files/resources/HART_Doing%20a%20literature%20review_1988_ch1.pdf
Helse- og omsorgsdepartmentet. (2015a). *Lov om behandling av ehlseopplysninger ved ytelse av helsehjelp (pasientjournalloven)*. Lovdata Retrieved from https://lovdata.no/dokument/NL/lov/2014-06-20-42?q=pasientjournal
Helse- og omsorgsdepartmentet. (2015b). *Lov om helseregistre og behandling av helseopplysninger (helseregisterlover)*. Lovdata Retrieved from https://lovdata.no/dokument/NL/lov/2014-06-20-42?q=pasientjournal
Helse- og omsorgsdepartmentet. (2020). De regionale helseforetakene. Retrieved from https://www.regjeringen.no/no/tema/helse-og-omsorg/sykehus/innsikt/nokkeltall-og-fakta---ny/de-regionale-helseforetakene/id528110/
Helsenorge. (2018). *Bruksvilkår for innbyggertjenester på HelseNorge*. Retrieved from https://www.helsenorge.no/globalassets/dokumenter/bruksvilkaar_for_helsenorge.pdf
Helsenorge. (2020). Om helsenorge.no. Retrieved from https://www.helsenorge.no/om-helsenorge-no/
Helsenorge. (2021). Pasientjournal. Retrieved from https://tjenester.helsenorge.no/pasientjournal
Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems, 19*(2), 7. Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1017&context=sjis
Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *Managment INformation Systems Research center, University of Minnesota*, 32. Retrieved from https://www.jstor.org/stable/25148625?seq=1#metadata_info_tab_contents
Huang, H., Zhu, P., Xiao, F., Sun, X., & Huang, Q. (2020). A blockchain-based scheme for privacy-preserving and secure sharing of medical data. *Computers & Security, 99*, 102010. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404820302832?dgcid=rss_sd_all
Hyperledger. (Unknown). Hyperledger Fabric. Retrieved from https://www.ibm.com/downloads/cas/0XMOQJNP
IBM. (Unknown). What are smart contracts on blockchain? Retrieved from https://www.ibm.com/topics/smart-contracts
Insights, L. (2019). China's Baidu launches health blockchain. Retrieved from https://www.ledgerinsights.com/health-blockchain-baidu-medical/
Interaction-design. (Unknown). User Centered Design. Retrieved from https://www.interaction-design.org/literature/topics/user-centered-design
IPFS. (Unknown). What is IPFS? Retrieved from https://docs.ipfs.io/concepts/what-is-ipfs/#decentralization
Kumar, S. (2018). The Ultimate Guide to Consensus in Hyhperledger Fabric. Retrieved from https://www.skcript.com/svr/consensus-hyperledger-fabric/
Lake, J. (2020). What is AES encryption and how does it work? Retrieved from https://www.comparitech.com/blog/information-security/what-is-aes-encryption/

Lord, N. (2018). What is an Advanced Persistent Threat? APT Definition. Retrieved from https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition

Marr, B. (2019). What is Homomorphic Encryption? And Why Is It So Transformative? Retrieved from https://www.forbes.com/sites/bernardmarr/2019/11/15/what-is-homomorphic-encryption-and-why-is-it-so-transformative/?sh=6f8d68967e93

McCauley, A. (2020). Why Big Pharma Is Betting On Blockchain. Retrieved from https://hbr.org/2020/05/why-big-pharma-is-betting-on-blockchain

McKay, E. (2013). *UI is communication - How to design intuitive, user-centered interfaces by focusing on effective communication*. USA: Elsevier Inc.

Medium. (2019). Consensus Series: PBFT. Retrieved from https://medium.com/thundercore/consensus-series-pbft-3e011e7f3691

Memon, M., Bajwa, U. A., Ikhlas, A., Memon, Y., Memon, S., & Malani, M. (2018, 2018). *Blockchain Beyond Bitcoin: Block Maturity Level Consensus Protocol.* Paper presented at the 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS).

Micali, S. (2020). Algorand Co-Chains. Retrieved from https://www.algorand.com/resources/blog/algorand-co-chains

Microship. (Unknown). Data Pointers. Retrieved from https://microchipdeveloper.com/tls2101:data-pointers

Microsoft. (2018). Public Key Infrastructure. Retrieved from https://docs.microsoft.com/en-us/windows/win32/seccertenroll/public-key-infrastructure

Miguel Castro, B. L. (1999). *Practical Byzantine Fault Tolerance.* Massachusetts Institute of Technology, Cambridge. Retrieved from http://pmg.csail.mit.edu/papers/osdi99.pdf#page=5

Mubarakali, A., Bose, S. C., Srinivasan, K., Elsir, A., & Elsier, O. (2019). Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. *Journal of Ambient Intelligence and Humanized Computing*. doi:10.1007/s12652-019-01420-0

Mullen, T. (2017). Data in Transit. Retrieved from https://www.sciencedirect.com/topics/computer-science/data-in-transit

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. 9. Retrieved from https://bitcoin.org/bitcoin.pdf

Namestnikova, M. (2020). Healthcare security in 2021. Retrieved from https://securelist.com/healthcare-security-in-2021/99571/

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton and Oxford: Princeton University Press.

Norsk Helsenett. (2019). *ÅRSRAPPORT 2019*. Retrieved from https://www.nhn.no/om-oss/sentrale-dokumenter/_/attachment/download/d268ef47-198b-45ce-8713-b5e697634688:8526658913d62c2bffb015716816f7df121c1a23/arsrapport-nhn-2019.pdf.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Communications of the Association for Information Systems, 37*(1), 879-910. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1954824

Paloalto Networks. (2021). Highlights from the 2021 Unit 42 Ransomware Threat Report. Retrieved from https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/
Phillips, D. (2021). What is Algorand? A Speedy, Scalable Platform for Dapps. Retrieved from https://decrypt.co/resources/what-is-algorand-a-speedy-scalable-platform-for-dapps
PRISMA. (2020). PRISMA Flow Diagram. Retrieved from http://prisma-statement.org/prismastatement/flowdiagram
Qureshi, H. (2019). Merkle Trees. Retrieved from https://nakamoto.com/merkle-trees/
Rahmadika, S., & Rhee, K.-H. (2018). Blockchain technology for providing an architecture model of decentralized personal health information. *International Journal of Engineering Business Management, 10*, 1847979018790589.
Ramzan, Z. (2013). Bitcoin: Proof of work. Retrieved from https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-proof-of-work
Random Wits. (2012). Advanced Encryption Standard (AES). Retrieved from http://randomwits.com/projects/aes
Reen, G. S., Mohandas, M., & Venkatesan, S. (2019). *Decentralized Patient Centric e-Health Record Management System using Blockchain and IPFS.* Paper presented at the 2019 IEEE Conference on Information and Communication Technology.
Regjeringen. (2018). Tidenes største sating på digitalisering. Retrieved from https://www.regjeringen.no/no/aktuelt/tidenes-storste-satsing-pa-digitalisering/id2614074/
Saleh, F. (2020). Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies, 34*(3), 1156-1190. doi:https://doi.org/10.1093/rfs/hhaa075
Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. *Sustainability (Switzerland), 12*(17). doi:10.3390/su12177002
Seeley, L. (2019). Announcing Sawtooth PBFT 1.0. Retrieved from https://www.hyperledger.org/blog/2019/10/31/announcing-sawtooth-pbft-1-0
Shahid, Z., Chaumont, M., & Puech, W. (2013). Joint Entropy Coding and Encryption in AVS Video Codec.
Sharma, T. K. (Unknown). Types of blockchains explained- public vs. private vs. consortium. Retrieved from https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/
Sheffield, N. (2018). pBFT - UNderstanding the Consensus Algorithm. Retrieved from https://medium.com/coinmonks/pbft-understanding-the-algorithm-b7a7869650ae
Spagnoletti, P., & Tarantino, L. (2013). User Centered Systems Design: The Bridging Role of Justificatory Knowledge. In (pp. 105-121): Springer Berlin Heidelberg.
Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors (Switzerland), 20*(22), 1-14. doi:10.3390/s20226587
Storj-DCS. (Unknown). Storj DCS - Introduction. Retrieved from https://docs.storj.io/
Toshniwal, B., Podili, P., Reddy, R. J., & Kataoka, K. (2019). *PACEX: PAtient-Centric EMR eXchange in Healthcare Systems using Blockchain.* Paper presented at the 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2019.

Valmot, O. R. (2020). Digitalisering av helsetjenester er mer krevende enn banktjenster. Retrieved from https://www.tu.no/artikler/digitalisering-av-helsetjenester-er-mer-krevende-enn-banktjenester/492402
Vorotnikov, A. (2015). Parity Ethereum. Retrieved from https://github.com/openethereum/parity-ethereum
Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly, 26*. Retrieved from https://www.jstor.org/stable/4132319?seq=1#metadata_info_tab_contents
Whitney, L. (2021a). 2020 sees huge increase in records exposed in data breaches. Retrieved from https://www.techrepublic.com/article/2020-sees-huge-increase-in-records-exposed-in-data-breaches/
Whitney, L. (2021b). How ransomware is evolving as a threat to organizations. *Techrepublic*. Retrieved from https://www.techrepublic.com/article/how-ransomware-is-evolving-as-a-threat-to-organizations/
WHO. (2011). *mHealth - New horizons for health through mobile technologies*. Retrieved from WHO: https://www.who.int/goe/publications/goe_mhealth_web.pdf
WHO. (2020). WHO reports fivefold increase in cyber attacks, urges vigilance. Retrieved from https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
Øyvann, S. (2018). Helsevesentet henger etter. *ComputerWorld*. Retrieved from https://www.cw.no/artikkel/it-helse/helsevesenet-henger-etter

9 Appendices

Appendix A – Interview Protocol

Administrativt

- Hva er hensikten med flere helseregioner?
- Hvem regulerer denne delingen?
- Er det mulighet for å se en oversikt over nåværende system?

Sikkerhet og teknologi

- Hvilke sikkerhetstiltak er inne for data i bevegelse?
- Hvordan foregår deling av pasientjournaler mellom de fire helseregionene, privat og andre helseorganisasjoner (Eks: tannlege, fysioterapeut, kiropraktor, fastlege)?
- Hvor blir data lagret? (Eks: sky, egen server i Norge, egen server i utlandet, lokalt)
- Er det noen planer for oppdatering av systemer? (Større endringer i teknologi)
- Er blockchain i bruk (evt pilotprosjekter? Hvis ikke, er det noe dere har sett på for fremtiden?
- Har dere oversikt over fremtidig teknologi og hvordan den vil påvirke helsesektoren? (Mobil helse, IoT, 5G etc)
- Fungerer nåværende system godt for deling av data? Det oppleves som det er mangel av delingsmuligheter i pasientjournaler
- Hvilke sikkerhetsfunksjoner er på plass for å ivareta dataintegritet og personvern?
- Er nåværende system dyrt å drive?
- Er systemene raske/krever de mye prosessorkraft?
- Hvordan er trusselbildet?
- Hvem anser dere som største trusler? (APT, aktivister, tilfeldig angrep som ransomware/phishing)

GDPR

- Hvem eier informasjon (pasientjournalen)?
- Har pasienter tilgang til sin egen journal? Eventuelt mulighet til å legge inn verdier/tester/relevant informasjon?
- Har brukere mulighet til å slette egen data?
- Normen og GDPR stiller strenge krav til personvern, hvilke tiltak er iverksatt for å oppnå dette?