LAPPEENRANTA-LAHTI UNIVERSITY OF TECHNOLOGY LUT

School of Engineering Science

Software Engineering

Boris Godlin

Blockchain-based electronic health records system architecture

Examiners: Professor Jari Porras

Professor Igor Ilyin

ABSTRACT

Lappeenranta-Lahti University of Technology

School of Engineering Science

Software Engineering

Boris Godlin

Blockchain-based electronic health records system architecture

Master's Thesis 2021

86 pages, 49 figures

Examiners: Professor Jari Porras

Professor Igor Ilyin

Keywords: blockchain, electronic medical record, architecture

The research was carried out on the basis of blockchain and the possibilities of its application to the management of patient medical data. The subject of the thesis is blockchain and the possibilities of its application to the management of patient medical data The selected research methodology is Design Science Research methodology. Since the methodology process involves sequential processes, each process is described with its corresponding content in the following parts of the paper. Stakeholders and requirements for an electronic medical records system were identified, a reference architecture model was built, a prototype of the system was developed, and the potential effect of the system was described.

The field of application of results are the public and private medical organizations. The scientific novelty is a built reference architectural model based on the collected requirements. Additionally, the thesis is of practical reference.

Acknowledgements

This work is the result of six years of studying in the fields of business informatics as well as software development. Studying was not easy for me, but nevertheless, I may safely say that the chosen direction was perfect for me.

The chosen topic of the study concerns the field of healthcare. Apart from being a “patient”, I have never been involved in this field. Despite the lack of domain knowledge, the healthcare-related thesis topic was chosen. The key reason is its importance. Qualitative changes in healthcare, including the storage of medical records, are long overdue. The opportunity to directly affect the quality of human life was the main motivator during the writing.

First of all, I would like to thank professor Porras, the research supervisor from the LUT. Regular consultations with comments on the work done by prof. Porras helped me to stay on track. Thanks to prof. Porras, the thesis got the storytelling aspect, from problem designation to IT artifacts, thereby having both the scientific value of the research and the practical value.

I would also like to thank my supervisor from SPbSTU, professor Ilyin. Professor Ilyin and I have been doing academic work together for quite a long time, which has shaped the necessary skills for a researcher in me.

Finally, I would like to thank my parents for their unconditional love and support. My parents observed my motivation, combined with fatigue, in writing the thesis. Thanks to them, I was able to achieve my goals and the expected results.

Boris Godlin

Table of contents

1 INTRODUCTION

The world is not standing still. With the exponential growth in the potential performance of computers and the active concomitant integration of state-of-the-art technologies, opportunities are opening up to improve the quality of human life. Perhaps one of the most influential areas affecting the quality of human life is healthcare. Despite the conservatism of the field, healthcare is no exception and actively integrates the latest information technologies. In Russia, the healthcare market has been actively growing for the last decade, and in parallel, the demand for the quality of the services provided is increasing - the service component is becoming an increasingly fundamental criterion when choosing medical services, both in large cities and in the regions (EY, 2019). With the ever-increasing demand for medical services, both medical private organizations and public medical entities are looking for IT solutions to improve the operational productivity, lower the treatment costs and increase the quality of care.

In addition to the demand for IT-innovations in healthcare from providers, there is a strong demand for IT services from patients. Qualitative changes in the sphere of health protection of the Russian population can be achieved primarily through the introduction of modern scientific developments in the daily activities of medical institutions, in particular information technologies that are aimed at reducing morbidity, disability and mortality. Currently there are many problems remaining that patients have to face when the need for medical care arises. Perhaps one of the key problems is that the patient, for the most part, does not have a single medical record due to the fact that examinations, meetings and analysis are performed in different medical organizations. The development of a unified repository could have a significant impact on healthcare as a whole, since it affects many aspects - from more accurate diagnosis to the use of personal data by research laboratories. The relevant technology to be used to implement such an electronic health record may be considered a distributed ledger - blockchain. The necessity for this particular technology is due to its unique characteristics.

1.1 Problem statement

Modern Russian medical information systems are based on a comprehensive approach to the assessment of individual and public health, taking into account the various environmental influences (natural and man-made) on the human body through the creation of large information spaces, providing uniformity in the analysis and monitoring of

individual areas of medicine based on the integration of data of specialized information solutions at various levels of the health system (Kobyakova et al., 2020). In 2013, Russia formally completed the first phase of the Unified State Health Information System - thousands of medical institutions received secure networks and Internet access, acquired automated workstations and began to master medical information systems . Basic federal services have been created: a register of normative and reference information, electronic registration, a system of integrated electronic medical records, systems for analysis of economic activity, register of medical workers and passports of medical institutions. The main idea was to ensure the vertical interaction of medical organizations and the transfer of primary reliable information and its adequate perception and processing at the regional and federal level.

In development of earlier decisions, the Ministry of Health of Russia approved on 23.06.2016 the Methodological recommendations on providing functional capabilities of regional medical information systems, which specify the purpose, functions and composition of such systems. However, healthcare informatization began *not with* the development of standards for a unified address space, principles of information collection and storage, protocols for exchanging medical data, norms and rules for working in the network, and policies to develop the network and its information resources, but with the development of separate software products for different levels of the healthcare system, which created obstacles to further integration of various information systems and even a certain resistance from some software product developers. The current approach to organizing data storage has significant disadvantages and even potential critical threats.

Probably the most significant one is the lack of *integrity* of patient medical data, caused by the lack of interoperability of current IT solutions. The absence of interoperability limits effective data sharing and management. Thus, patient's health records are spread across many organisations. A consequence of technical limitations in the organization of data exchange between information systems is the need to re-enter patient data and re-examine patients, which in addition to moral costs and time losses leads to additional financial expenditures to the medical organisation.

Another threat is *security*, caused by the centralized architecture of the systems - if a single node or one of the few is compromised, attackers gain access to the data of many users. An intruder who has access to the data can make irreparable and not always noticeable changes to it, which would invalidate the medical data, and its further use could

result in the doctor prescribing the wrong treatment to the patient, which could harm his health. According to a recent investigation, an upward trend in the number of medical records breach each year is present (Seh et al., 2020).

The other major problem in the healthcare field tightly connected with the security threats is data *privacy*. Patients' access policy to the medical data is determined by the owner of the centralized database - the medical organisation. Thus, the patient does not own the medical data, that implies that the medical organisation may be selling the data, violating the legislation. However, even without the presence of malicious intent, due to the current organization of data storage, patient privacy is at risk. The human factor should not be forgotten - sometimes the employees responsible for data security in information systems do not have the necessary competencies or demonstrate an irresponsible attitude to the issue. But more often the problems arise due to the fault of ordinary specialists: according to the latest research, employees account for more than half of data losses - the majority of them arise due to human-errors or negligence (Kamoun & Nicho, 2014).

These are just some of the disadvantages healthcare faces. As the digitalization of the sector grows globally, so does the importance of these challenges. The following statistic displays the result of a survey, performed by HIMSS, where eHealth professionals from Europe evaluated the current top eHealth priorities for healthcare providers in 2021 (Epalm, 2021):

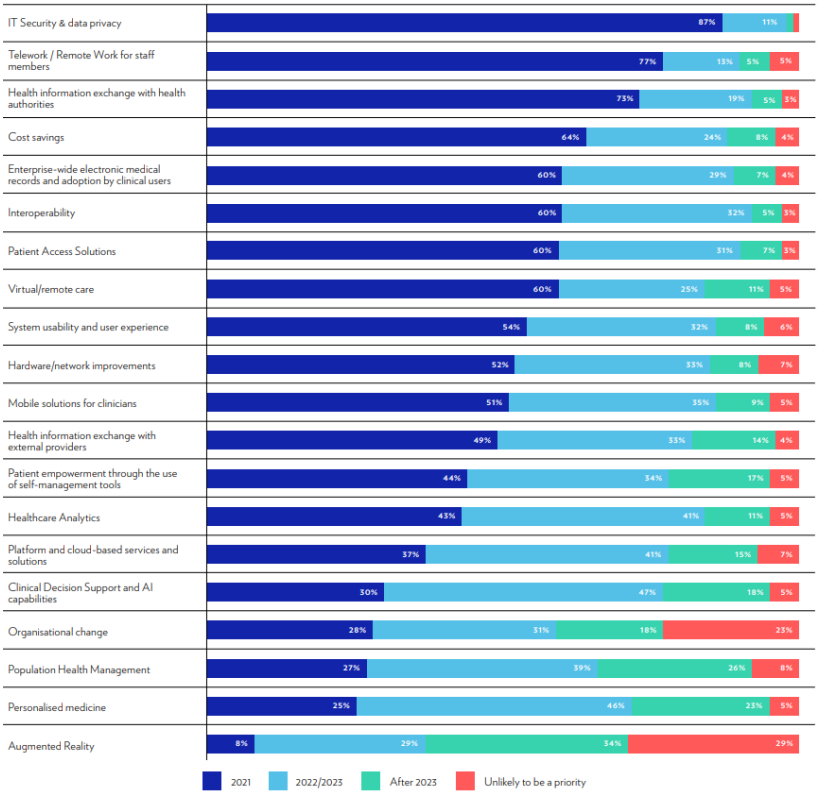

Figure 1 — HIMSS Annual European Digital Health Survey 2021 [5]

87 percent of professionals claimed that IT security is the biggest priority for healthcare providers. Other priorities that are also related to the orientation of the thesis, such as information exchange, enterprise-wide EMRs, interoperability and access solutions are also at the top of the list.

1.2 Research objectives

In this paper, blockchain technology will be proposed to solve the previously described problems. The main objective of the research is to propose a solution based on this technology, which will be possible to integrate into the current architecture. Therefore, the main research question may be posed:

***RQ**: What will be the reference architecture to provide a basis of blockchain-based electronic health records system?*

To give the answer to the research question, it should be divided into sub-questions and the answer for every sub-question should be given. The first step is to outline the current

issues in the area of electronic health record storage. Thus, the first sub-question to be answered is:

SQ1. What are the problems with current approaches to organizing electronic health records?

The study began precisely by the problem identification. With the absence of problems in the field, it may be assumed that the study would have been pointless. Earlier in the thesis the actual problems have already been given, so it could be considered that the answer to this sub-question has been given. Thus, a fundamental rethinking of the approach to organizing the storage of electronic medical records is required.

Architectural design always starts with requirements. Before the development of any system the set of clear requirements, describing the functionality of the system, should be introduced. The requirements are usually stakeholder-oriented. The solution being developed may have different stakeholders, as it affects the healthcare industry as a whole. The scientific literature materials identifying stakeholders, followed by detailed descriptions and alignment of requirements is missing.

Understanding stakeholders requirements is a critical part when designing the architecture of the IT solutions. In ISO 13407 standard it is stated that the user-centred design begins with a thorough understanding of the needs and requirements of the users (Bevan & Curson, 1997). The identification of the stakeholders is one of the first steps that should be completed during the requirement engineering stage, otherwise important use-cases may be not considered that potentially may cause the inability of the developed system to be improved, covering the skipped requirements later on due to initial architectural decisions.

Based on the identified system stakeholders and requirements, it will be easier to evaluate proposed in the scientific literature and real products system architectures. Thus, to answer the posed research question the following steps should be covered:

SQ2. Who are the stakeholders of an EHR?
SQ3. What are the main stakeholder-specific requirements?

To build the reference architecture based on the results of the covered steps, first, an analysis of the current state is needed. A scenario, when the patient has to visit two distinct medical organisations will be used to create this current state.

SQ4. What is the current architecture (AS-IS architecture) of the system and what are its disadvantages?

With the performed introduction of the blockchain features and the disadvantages of the current architecture introduced, a reference architecture may be made:

SQ5. What would be the reference architecture of the system?

After the reference architecture is proposed, it should be validated. The validation will be performed by the means of the following steps:

SQ6. How should the reference architecture be implemented in the scenario context (TO-BE architecture and prototype)?

SQ7. What is the potential impact of a new architecture?

The alignment between the sub-questions and the materials used to answer the sub questions is presented on the following figure:

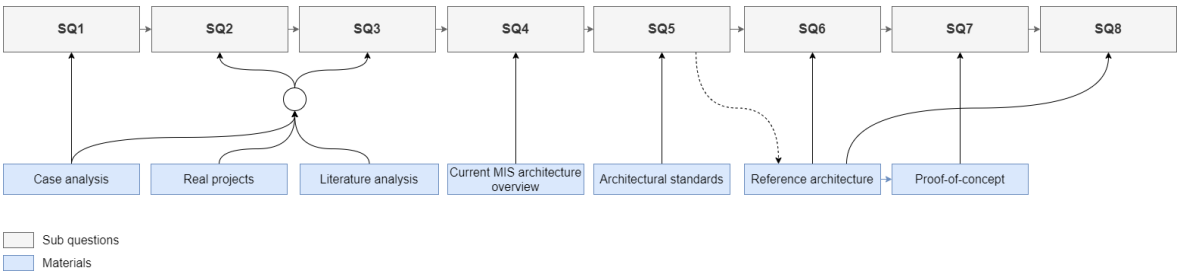

Figure 2 — Alignment between sub questions and materials

1.3 Research methods

To encompass the identified stages, the design science research paradigm is used. It helps solve problems through innovative artifacts. The process in the design science research is switching between development and evaluation processes.

Designed artifacts will be very useful to understand the problems more deeply. In a discussing case, where the number of requirements may be relatively large due to the spread of the stakeholders and where the high quality is critical due the tight connection with the difficult world, design science research would be very suitable.

The selected design science research methodology is the one presented by the Peffers and others (Peffers et al., 2007). The goal of the researchers was to develop a process that would serve as a generally accepted framework for conducting research based on the principles of design science research outlined by other researchers. Rather than focusing on the differences in views between different researchers, the researchers used a consensus approach. The process in presented on the following image:

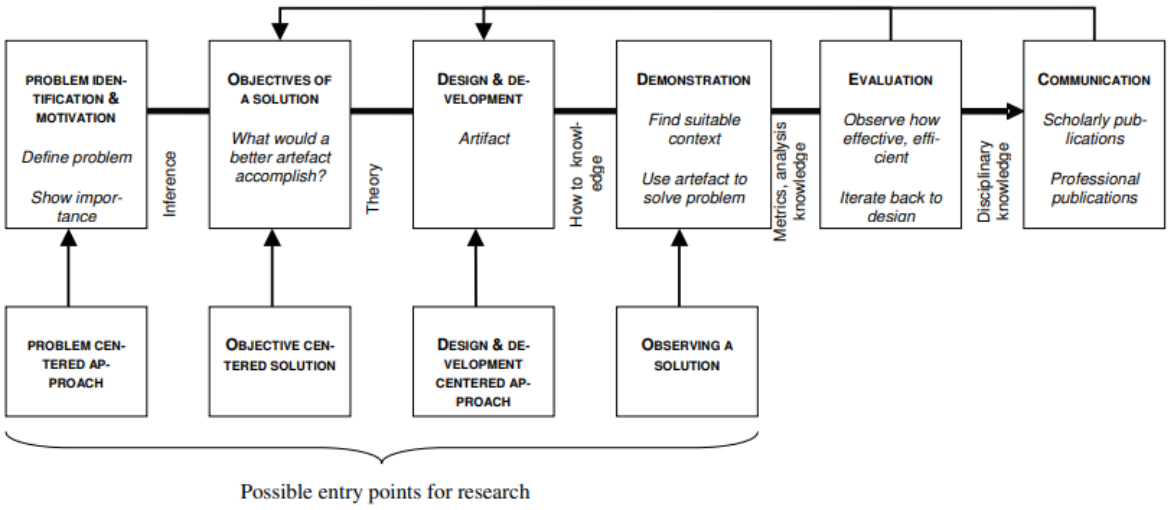

Figure 3 — DRSM process

DSRM implies the 6 activities - the thesis is carrying them out:

1. *Problem identification and motivation*. The problem was discussed previously - it is not yet clear if blockchain is a feasible technology for EHR and yet there is no clear reference architecture;
2. *Define the objectives of a solution*. The objectives of this research are defined in the form of research questions;
3. *Design and development.* The designing artifact in this thesis is planned to be in the form of the reference architecture. It will be based on the AS-IS (current) and TO-BE (desired) models

4. *Demonstration*. A proof of concept in the form of a lightweight prototype will be made to help validate the architecture.

5. *Evaluation*. After the demonstration an evaluation will be conducted.

6. *Communication*. The final remarks about all the research questions and the main research question will be given, some recommendations added.

The performed research will be of *scientific* relevance as it gives new insights in both possibilities and the limitations of the blockchain technology for application in healthcare and other fields as a new possible reference architecture for blockchain systems is introduced. The presented artifacts may be used by the companies to decide whether they should use blockchain or not for their applications. A reference architecture could be used as a blueprint. This gives a *practical* relevance to the study.

2 BLOCKCHAIN TECHNOLOGY

This chapter briefly introduces the distributed ledger technology - blockchain. Both technical and non-technical aspects are discussed.

The term first appeared as the name of a replicated distributed database implemented in the Bitcoin cryptocurrency system. The Bitcoin system, which appeared in October 2008, was the first application of blockchain technology (Bitcoin.org, 2009). However, blockchain technology can be extended to any connected blocks of information.

2.1 Network

Giving a broad definition, the blockchain is a transaction processing network with a set of rules (a "protocol") that participants can follow to a common transaction log view. The implementation of such a system in a centralized manner would have many potential threats. The necessity and the purpose of decentralized and distributed systems over the centralized was highlighted and broadly discussed by Paul Baran (Baran, 1962). The network types are conceptually visualized on the following figure:

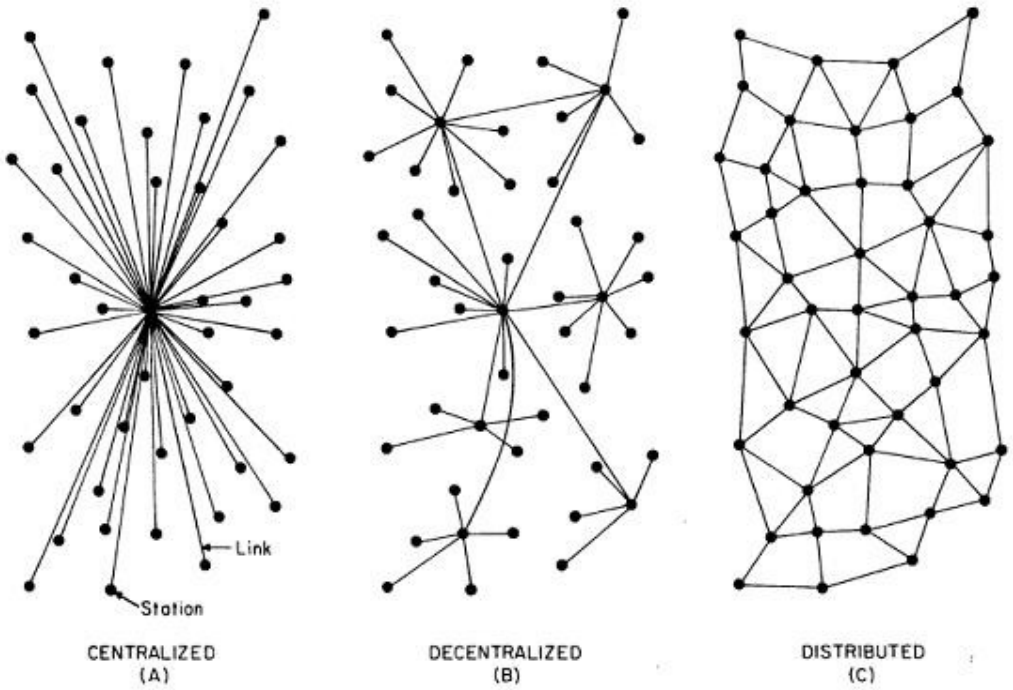

Figure 4 — Visual demonstration of differences between centralized, decentralized and distributed systems (Baran, 1962)

Centralized systems are systems that use a client/server architecture. Client nodes are connected to the server and send the corresponding requests. This is the most commonly used type of system. The client sends a request to the central company's server and receives a response. The biggest problem with this type of system is that it has a single point of failure. It could be seen from the figure that, for two non-central nodes to communicate, the message has to travel via the central node. In case of the disconnection of the central node, the whole system fails.

Another significant weak point of such systems are the potential security threats. In case of the corruption of the central node, all messages sharing between other nodes passing through the central nodes would be compromised. Hence, centralized systems are less reliable.

Decentralized systems is another network type - instead of one central node the decentralized system implies multiple central coordinators. Those coordinators are communicating with each other, passing the information from non-central nodes. The introduction of the multiple coordinators solves the biggest problem of the centralized systems - the single point of failure, as in case of a failure of one coordinating node, message may go via other active coordinating nodes.

In a distributed system each node makes its own decision. The behavior of the whole system is based on a set of solutions of the individual nodes. A computer system can be classified as distributed if the participating nodes do have common physical clocks, do not have shared memory, are geographically separated, and are autonomous and heterogeneous (van Steen & Tanenbaum, 2016).

It would be important to highlight that conceptually the *centralization* refers to the communication, whereas the *distribution* refers to the decision-making. The great comparison visualization was recently introduced by JP Vergne - the figure shows how organizations are shaped by the extent to which their communications are centralized vs decentralized and their decision-making is concentrated vs distributed (Vergne, 2020).

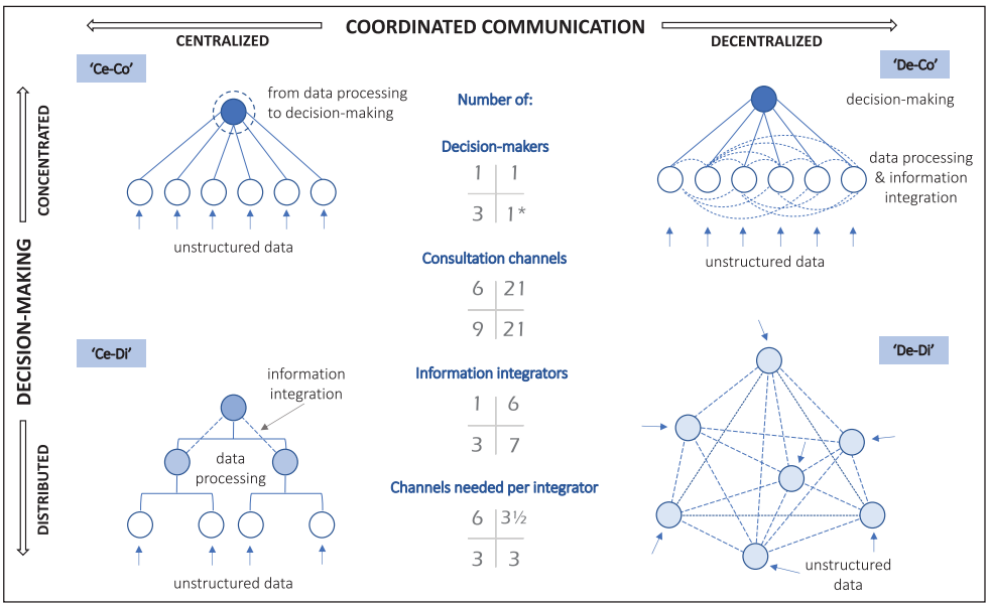

Figure 5 — The decentralization and the distribution of the system (Vergne, 2020)

Blockchain was invented by a person (or group of people) named Satoshi Nakamoto in 2008 for the use as a public recorder (ledger) of bitcoin cryptocurrency transactions. In the whitepaper of a bitcoin cryptocurrency the authors propose “peer-to-peer distributed timestamp server” with “no central authority” to issue the cryptocurrency . The initial proposition of the cryptocurrency implied the distributed and decentralized nature of the network, therefore, categorizing bitcoin by the framework presented by JP Vergne, the organisation of the network of this cryptocurrency has a De-Di group.

2.2 Structure and basic mechanism

As the name implies, giving a more technical definition - a blockchain is a chain of tightly connected blocks, which minimally has the following attributes (Laurence T. 2019):

1. **ID**. Unique identifier in the chain.
2. **The previous block hash**. To ensure immutability.
3. **A nonce**. A specific random number used during the consensus creation process
4. **Transactions**. Activity itself within the chain.
5. **Hash**. The output of a specific mathematical function that is using the above mentioned attributes as an input.

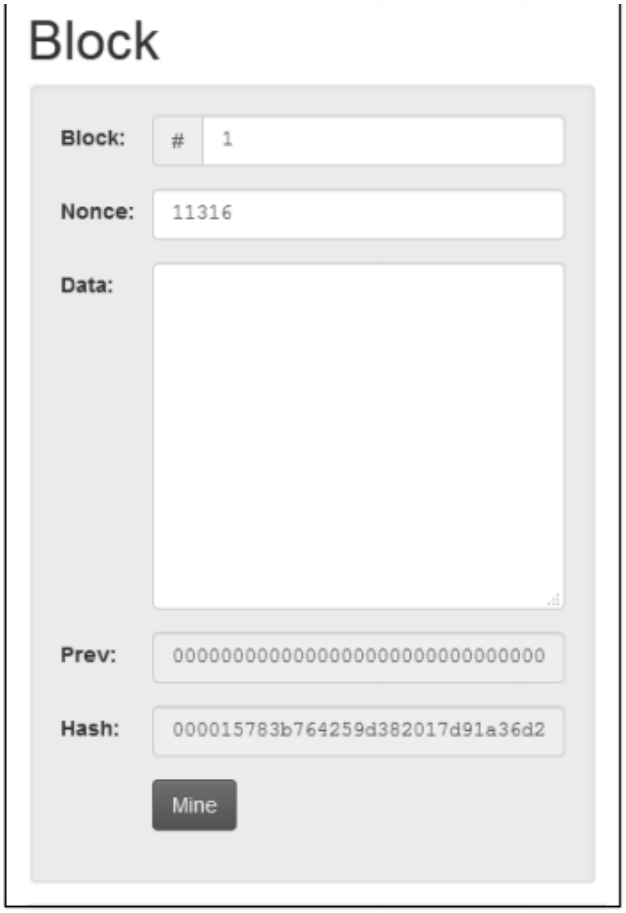

Figure 6 — The block structure

The first block in a blockchain is called a genesis block. It is usually hardcoded when the blockchain is started. This encoding is required to link the next (second) block to the genesis block, because in the blockchain the hash field of the previous block affects the current block. When the parent block changes in any way, its hash also changes, and hence the hashes of all subsequent blocks also change. The presence of a long chain of blocks makes the history of the blockchain immutable, which is a key characteristic of the technology. The model of data distribution in a blockchain can be represented as the following sequence of processes:

1. A transaction is sent to all nodes of the peer-to-peer network, the transaction enters the pool of raw data on those nodes.

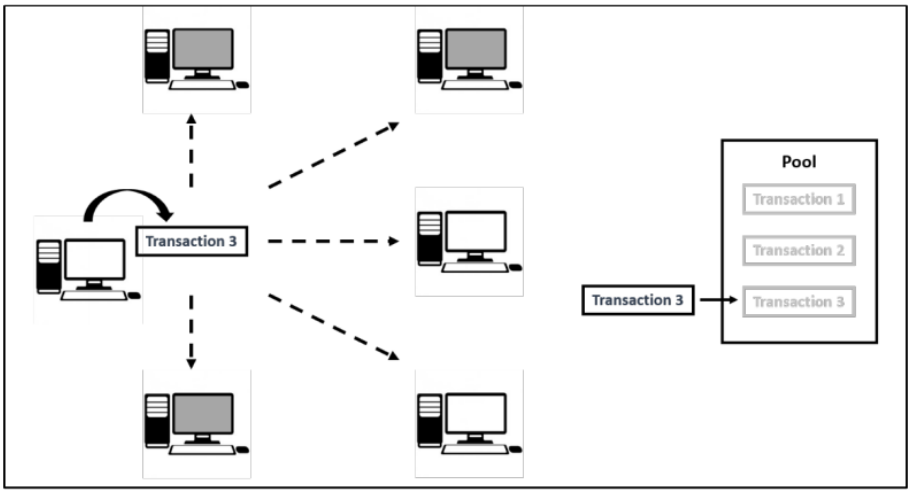

Figure 7 — Adding of the transaction to the transaction pool

2. Certain nodes engaged in mining - activity, associated with adding of the transactions located in the transaction pool to the blocks. Every miner searches for the value of the "Nonce" field, in which hash of the block would satisfy the conditions set by the developers. At the moment, there are also other ways of confirming the right to perform a block entry operation - they are going to be discussed in one of the next chapters.

4. The first miner who receives a block hash that satisfies the condition sends the block of data to all participants of the network, and the miner receives a prize pay (reward) for block adding. It is important to note that in the blockchain, it is not critical if not all nodes receive the block - as soon as the node that missed one of the blocks receives the next one after it, it will request the missing information to fill the missed blocks.

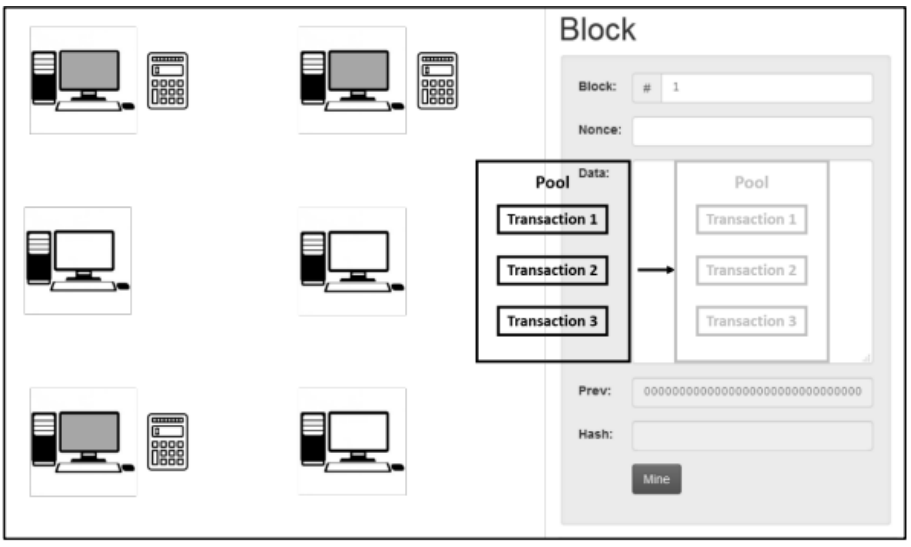

Figure 8 — Adding of the transactions to the block

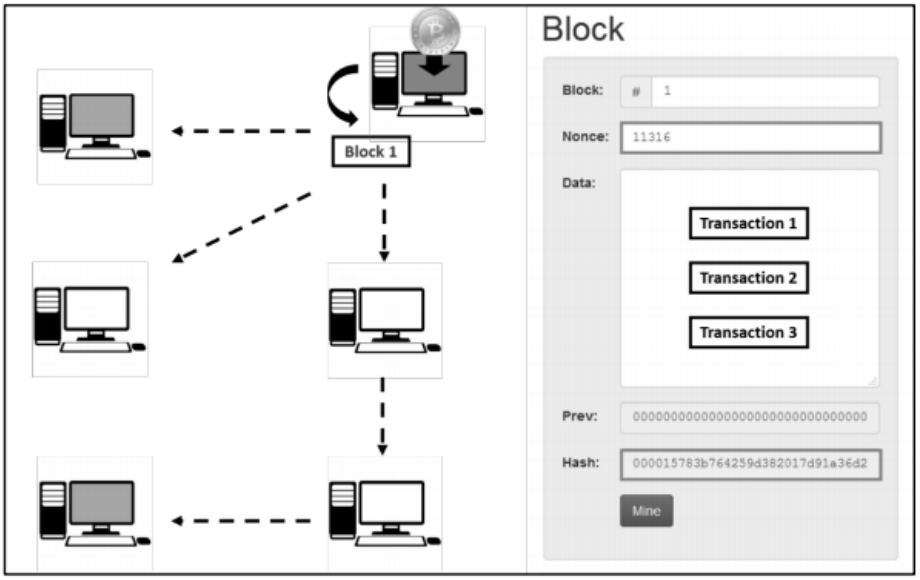

Figure 9 — The calculation of a hash and its sending to other nodes

5. Nodes that receive the block are checking its correctness and absence of so-called “double spending”. If the block does not pass the check, it is discarded.

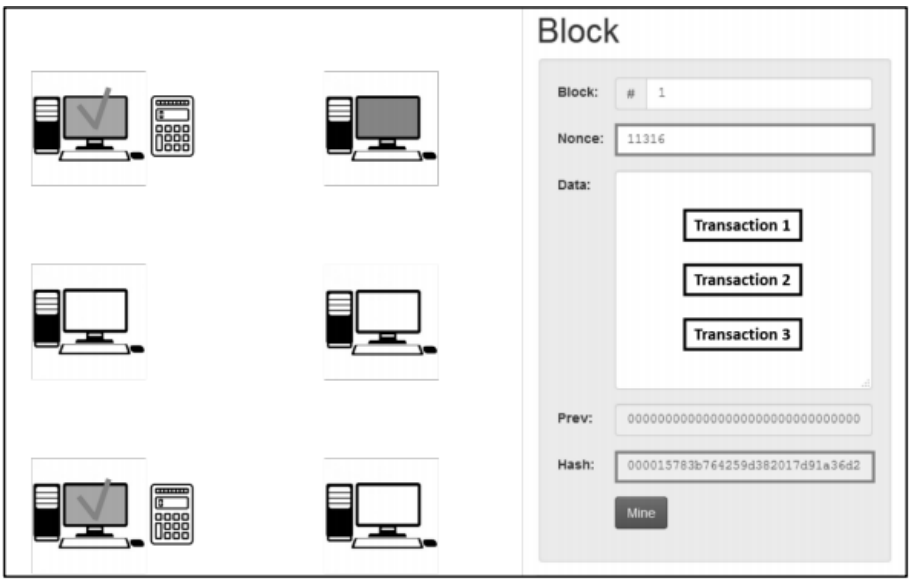

Figure 10 — Block checking

6. If during the checking of the block, all nodes on the network have confirmed its correctness, it is added to the chain, Miner now starts working on a new data block based on the hash of the newly added block.

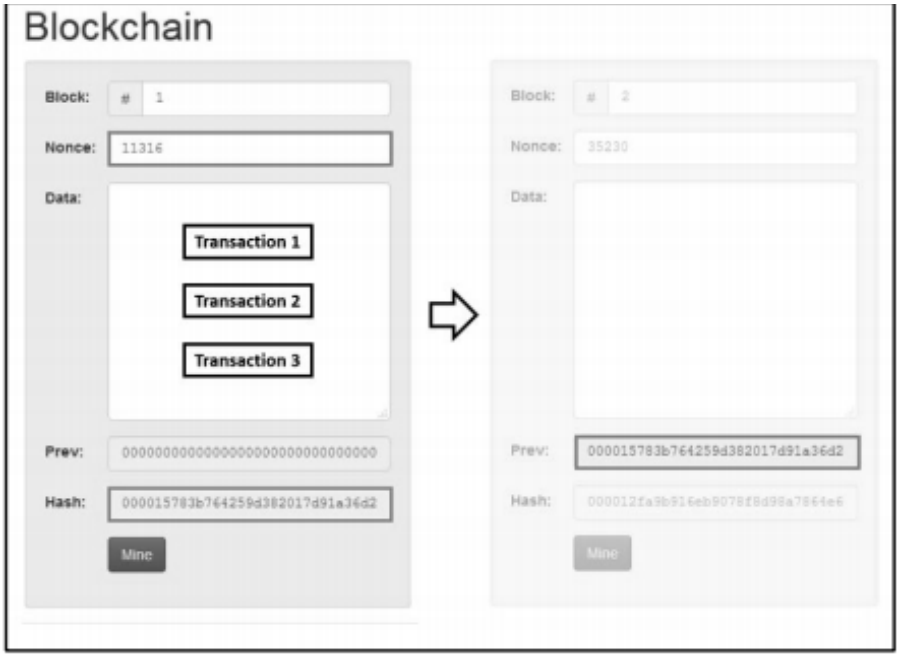

Figure 11 — Adding a new block to the chain

As already mentioned, since the hash of the current block, in addition to other input data, also includes the hash of the previous block, any change in any input data of the previous block will change both the hash of the previous block and consequently the hash of the block following it that way indalivating the whole chain. Thus, the immutability is ensured in the blockchain.

2.3 Cryptography

Transactions information is not transmitted publicly, otherwise everyone would be able to create a transaction by "introducing themselves" to the system as another person, and, thus, send all the funds to themselves. The sender and recipient data is converted into an unreadable character set. Each member of the network, when registering on it and installing the necessary software on a workstation, generates a random set of numbers (private key), which is used to form another, more complex set of characters (public key). With the current level of computing power, it is almost impossible to get a private key from a public key.

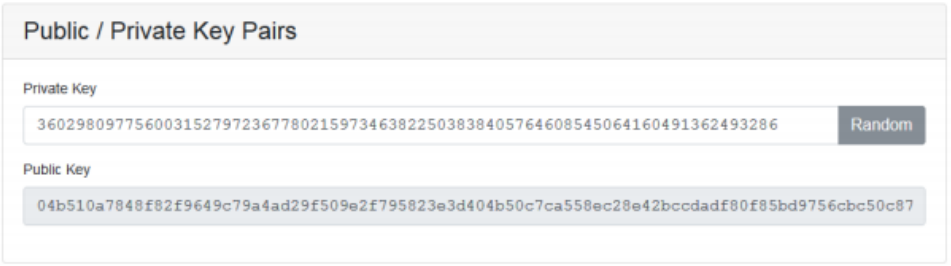

Figure 12 — Private and public keys

A private key belongs only to the user who generated it. It does not participate in transactions and should not be disclosed to anyone. It is used to sign a transaction, but is not shared publicly.

In order to send a transaction, each user makes a signature. In senders he enters his public key to identify his wallet, in recipients the public key of the wallet to which he wants to transfer funds and the amount he wants to transfer.

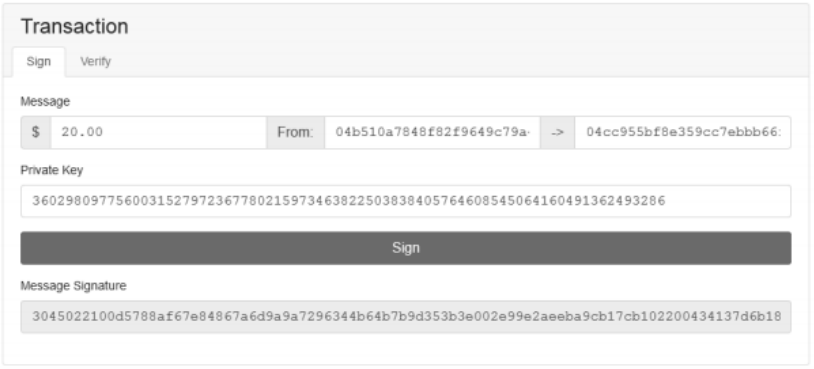

Figure 13 — Transaction signing

Based on these inputs and the private key, a signature is generated and then sent to the other participants to verify and add the transaction to the block.

With the signature and all the input data, each user of the system can verify that the transaction attempted to be entered into the block is signed by a user who has access to the actual private key. Thus, the blockchain no longer has personal data about the individuals transferring funds to one person or another, but only some kind of keys representing the wallets behind which certain individuals and signatures to each transaction are held.

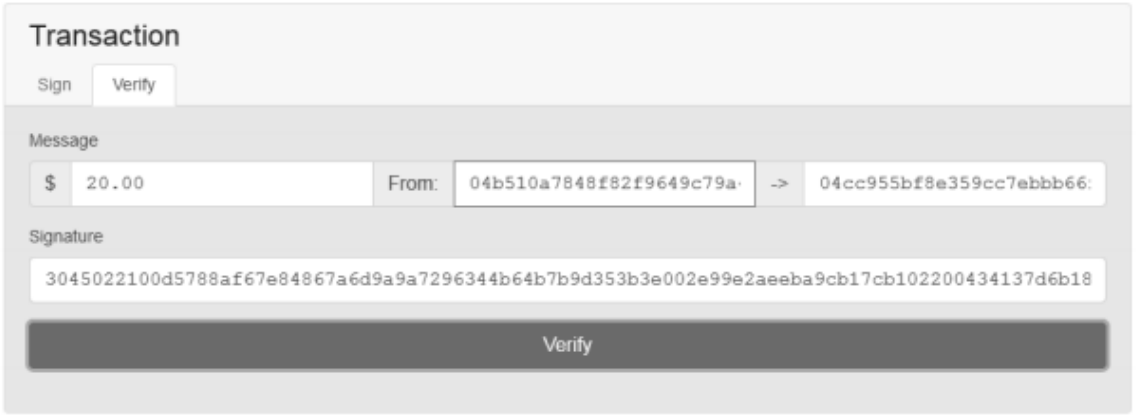

Figure 14 — Transaction signature confirmation

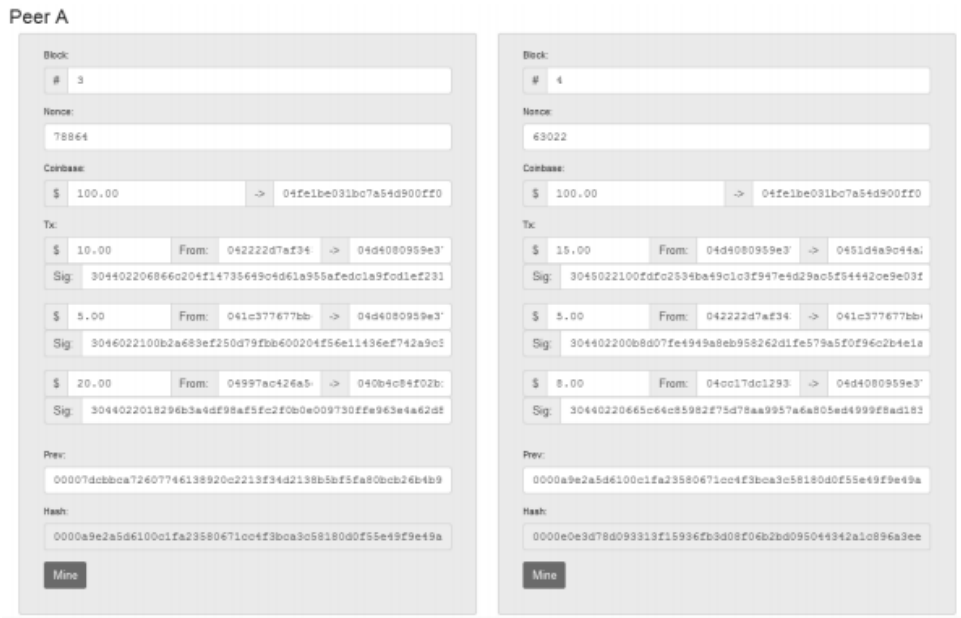

Figure 15 — Scheme of the blockchain with public keys and signatures

2.4 Types

It is considered that there are three blockchain types: **public** (permissionless) - accessible to anyone, **private** (permissioned) - with limited membership and **hybrid** that inherits the characteristics of both types (Niranjanamurthy et al., 2018).

The most basic condition for the blockchain to be considered as public is that it is not accessible to the controlling body. In public blockchains, the processes in the system are monitored by the entire community - from creators and developers to ordinary users. Anyone in the network may access the blocks created in a public blockchain, anyone may

send transactions and expect further inclusion in certain blocks if they are valid, and anyone in the world may participate in the consensus process. To ensure trust, public blockchains are protected by cryptoeconomics - economic incentives with cryptographic verification. The blockchain that are working on top of the cryptoeconimics mechanisms are considered to be “fully decentralized”.

While such redundancy makes public blockchain safe, it also makes it slow when for transaction processing and requires a lot of electrical energy to be wasted. The amount of power needed to execute each transaction increases with each additional piece of hardware, and may not be overwhelming in the long run.

The *advantages* of the public blockchain:

- Accessible. Could be joined without the permission.
- Anonymous. The absence of necessity to provide the network with the KYC information.
- Secure. To attack a blockchain system a vast amount of computational power is required (more than 50% of all computational power that is used in the network), which makes it simply unprofitable for malefactors.
- Absence of censorship. At some point, the creators of the system are not able to change the code or data for their benefit.
- Powerful network effect. In such an open environment, for a developer it is relatively easy to build a large user base around the application.

Private blockchains are characterized by a limited level of access. Confirmation of transactions on such networks, auditing, and database management are available to a single entity. Even the reading functionality can be made both generally available and severely restricted. Thus, such blockchain are considered to have a centralized network design, in which there is no full disclosure.

The *advantages* of private blockchains:

- Cheaper transaction. The absence of the necessity to do the PoW makes less energy to be used and, therefore, making the transactions cheaper. In private blockchains transactions are usually validated by only a small number of high-performance nodes.

- Higher TPS (transactions per second) rate. With no PoW required, there is no necessity to solve the complex cryptographic puzzle, consequently, making the transaction validation process faster.
- Mutability. The company that owns the private network will be able to cancel the transaction, if necessary, by making changes to the blocks.

Whereas public blockchains tend to be decentralized (Bitcoin, Ethereum etc.), private blockchains are usually governed by the single entity or a group of entities. It is discussed that private blockchains should not be called blockchains due to the misalignment with the initial proposed idea.

Hybrid blockchain emerged in an attempt to create an ideal network that combined the best features of each type of blockchain. The best characteristics of every blockchain type were discussed previously.

2.5 Consensus mechanisms

Blockchain updates are implemented through the use of consensus algorithms that guarantee the integrity and validity of data between nodes in the blockchain network (Chowdhury, 2020). Within a public blockchain, everyone can create their own distributed node. Consequently, the consistency mechanism between these nodes, of which there are usually many, needs to be reconciled to effectively reduce the likelihood of a Sybil or DDoS attack. This concept is very difficult to implement, but it could be easily verified. Nevertheless, public or private blockchain platforms must meet the growing demands of the applications for which they are intended:

- High performance: (low latency, high number of transactions per second)
- High scalability
- Low power consumption
- No revocation of transactions
- High resistance to attack

While the PoW mechanism has enabled a robust consensus in the global network, it is not at all suitable for applications that require, for example, very high transaction throughput. New consensus mechanisms have been developed and implemented to overcome these various limitations.

The purpose of the network's consensus mechanism is to allow network members to agree on the current state of transaction history. In other words, it is a process that allows a network sharing a common history (blockchain) to agree on the validity and order of transactions to be added to the history by sequentially adding new blocks. The following goals may be distinguished:

- **Consensus building**: the mechanism unifies all group agreements as much as possible.
- **Interaction**: each group seeks an agreement that is in the interest of the group as a whole.
- **Equal rights**: each participant has the same value when voting. This means that each person's vote is very important.
- **Participation**: every member of the group must participate in the vote. No one is left out of the vote.

Some of the consensus algorithms will be discussed further:

Proof-of-work (PoW)

Proof-of-work is a consensus algorithm used to reach an agreement that determines which blocks will be added to the chain after *mining*. The purpose of this protocol is to avoid cyberattacks such as denial of service (DDoS). It works by adding a task that requires a significant amount of computational resources. It implies the negative ecological impact and is currently widely discussed. Still, PoW is a fundamental concept for cryptocurrencies, and in blockchain this algorithm is a key factor when generating new blocks in the chain. With PoW, miners compete with each other to make online transactions and earn rewards. The database is decentralized and is responsible for all transactions in blocks.

Proof-of-stake (PoS)

Proof-of-Stake (PoS) is a category of consistent algorithms for public blockchains that depend on the economic interests of the validator in the network. In public blockchains based on PoW, the algorithm encourages participants who solve cryptographic encryption problems to validate transactions and create new blocks. In PoS-based open blockchains, a group of validators are voting for the next block, and the weight of each vote depends on the size of the balance amount (deposit). The process of creating and accepting new

blocks is done through a coordinated algorithm in which all existing validators can participate. Significant benefits of PoS include security and energy efficiency.

Leased proof of stake (LPoS)

In the LPoS consensus, holders of low amounts in their wallet will not be able to verify a block - just as miners with low hash rates will not be able to mine a block in PoW. In practice, in both cases, network maintenance depends on a limited number of users with a large spectrum of authority (high amounts or high processing power). However, the more distributed the network is, the more it will be protected from countless types of attacks. LPoS does this by allowing users to lease their balances. Leased balances remain under the full control of the owner and can be moved or spent at any time (when the lease expires). Leased coins increase the "weight" of a node, increasing the chances of adding a block to the block chain. All rewards received are distributed proportionally to the renters.

Proof-of-Importance (PoI)

Proof of Importance is a modified Proof of Stake, as it not only evaluates the number of tokens, but also takes account of account activity and continuous stay in the network. Initially, it was introduced on the NEM platform. Founded in Singapore and launched in 2015, the NEM project aims primarily to create a blockchain called the "Intelligent Asset System," capable of processing a large volume of transactions.

Proof-of-Burn (PoB)

The name Proof of Burn speaks for itself, it is an algorithm that burns tokens. To get a new currency, it is necessary to "burn" an n amount of other cryptocurrency obtained in the pow system. In theory, this will cause each new cryptocurrency to have the value of the burned cryptocurrency. In other words, the process of "burning" tokens represents the power of virtual mining, the more tokens the user invests, the more mining power he has, and therefore higher rewards, because, it will be a greater chance of becoming the validator of the next block.

Proof-of-Authority (PoA)

The Proof of Authority algorithm is mainly used in networks where user authentication is required. It is due to the fact that in PoA the identity of the user must be known. For the network, this means that only trusted nodes can participate in mining. If this trust is broken, the network can block access for that user. In PoA there may be a place for a

complete centralization, as this algorithm can be used in closed pools. Of course, there is also the possibility of decentralization, where the network community selects trusted individuals - as in DPoS (but in DPoS it is possible to remain incognito). Blockchains with Proof of Authority (PoA) are among the private blockchains unlike public blockchains such as PoW or PoS, where, in principle, anyone can participate in the consensus search. The algorithms work in steps. In PoA each transaction selects a node that acts as a mining leader.

2.6 Challenges

When implementing the solution that is based on blockchain technology, certain challenges are appearing. Those challenges could be technical and non-technical - some potential are listed below (Battah et al., 2021):

- *Performance*. Due to the need for the consensus making, blockchain will always have less performance capabilities than the centralized database. As transaction is being sent to the blockchain, unlike the centralized system three extra activities has to be carried out:

    - *Cryptography (signature).* The verification by the signature is the essential activity as nodes are distributed on a peer-to-peer basis and , therefore, the source of the transaction has to be somehow identifiable. The signing is done with the help of the public/private keys cryptography. Generating and verifying these signatures require rather significant computational resources and is a major bottleneck in blockchain products.

    - *Consensus mechanisms*. An active exchange of data between nodes, followed by processing on each, is required due to the requirement for the consensus. A rather high-probability case of network *conflicts* takes place - the situation where a chain has had discrepancies (forks) on multiple nodes. Despite the fact that in centralized systems also cancels transactions are not excluded, their processing is easier for the reason that all requests will go through a central node.

    - *Redundancy*. While the systems with the centralized architecture are processing the corresponding transactions once or several times, in blockchain transactions must be processed independently by each node in the

network. Consequently, much more computational work is done and, therefore, the energy spent, but the result of the transaction is the same as in centralized systems.

- *Regulatory status*. Blockchain and Bitcoin cryptocurrency face barriers to broad adoption by established institutions. Probably, one of the biggest obstacles for the blockchain project's implementation is the GDPR. GDPR was developed in a world where personal data was processed centrally. As a consequence, the active development of decentralized information processing systems poses new questions and challenges to experts.

- *Large energy consumption*. Consensus in the Bitcoin blockchain is achieved by proof-of-work. The miners on this network attempt to prove transactions with 450,000 trillion decisions per second, which requires a high amount of the computational resources.

- *Integration difficulties*. Blockchain applications offer solutions that require fundamental change or replacement of the whole current system. A migration strategy has to be discussed and planned as an additional step in the implementation project.

- *Cost of solutions.* Blockchain may give vast savings on the operational costs and has great technical capabilities. Nevertheless, the high capital costs of the development have to be expected, which is quite a significant limitation in the adaptation of the technology.

2.7 Possible Applications Of The Blockchain In Healthcare

Although blockchain was originally conceived as a technology for a revolutionary financial tool - Bitcoin, the earlier description of the technology suggests that the technology could be applied to other areas, including healthcare.

In twelve years of operation, the blockchain-based Bitcoin payment system has never been hacked. If the technology can provide trust in inherently risky financial environments, it can help in less aggressive ones such as healthcare. However, it is necessary to understand where to use the main advantages of distributed registry technologies - increasing trust, speed of approval of documents and reducing costs by reducing the number of intermediaries. It is also necessary to identify problem areas and see if the use of new technology will be beneficial. This chapter will look at some of the applications of blockchain technology.

Storing patient data with consent management

EHR implemented on blockchain is, probably, the first application possibility of blockchain technology in healthcare that comes into mind, as the requirements for the system are covered fully by the core features of the technology. Since this thesis is dedicated to this particular application, this chapter will not include the corresponding description.

Supply Chain Surveillance

Another application of blockchain in healthcare is to monitor the supply chain of common drugs. Blockchain has been used in supply chain management for a long time so the best practices may be obtained from the similar projects in the different fields (Korpela et al., 2017). Today customers cannot trace what they bought in the pharmacy drug was produced by. When the customer buys a drug, one may ask for a certificate for it. But no one prevents an unscrupulous supplier or seller from faking it. Counterfeit and substandard drugs are amongst current serious problems in the pharmaceutical industry.

The basic idea behind using blockchain for supply chain management is that every transaction brings together all stakeholders in the blockchain: from manufacturers to suppliers and further to pharmaceutical organizations and, finally, to customers (patients). In this case, any changes or attempts to tamper with the prescription will be immediately detected.

Case - blockchain-based supply chain in India

Counterfeit drugs are a serious problem in India. Approximately 3 percent of medicines are substandard or counterfeit (Chatterjee, 2010). There is an extreme need for traceability of the origin of drugs and how they have been handled throughout their journey through the supply chain. Research and interviews have confirmed that the risk of counterfeit drugs arises at the point of transfer between different stages of the complex supply chain (e.g., between wholesalers, distributors, and subdistributors). At each stage of the transfer of drugs from the factory to the consumer, drugs can be substituted or adulterated.

The National Informatics Centre of India has developed and implemented a Drug Authentication and Verification Application (DAVA) (davaindia, 2020). The system is based on the use of serial numbers as the unique identifier provided by manufacturers to identify products. The main goal of the initiative was to improve transparency and help India remain a global leader in the production of safe pharmaceutical products. DAVA provides manufacturer-level product information that can be verified by other stakeholders. However, it has been determined that blockchain can provide more functionality. For example, the system in its current form does not provide visibility into every transaction. In addition, DAVA does not allow products to be tracked throughout the supply chain or track temperature compliance. All of this can be achieved using blockchain and IoT technologies. The National Transformation Institution of India (NITI Aayog) organized a blockchain-based drug-tracking pilot project. Numerous health and technology partners participated in the project: drug manufacturers, carriers, logistics solution providers, and drug retailers. As such, the project required the integration of a number of independent IT systems to transmit information about the receipt and movement of goods. Efforts were made to limit manual entry of such data.

As the drug moved through the chain, each transaction was automatically transferred from internal IT systems and recorded in a registry with a timestamp. In addition, the blockchain recorded location and temperature, making the entire path transparent to stakeholders and limiting the possibility of tampering with the record.

The project demonstrated that blockchain can provide a higher level of transparency, efficiency and reliability of transactions in the pharmaceutical industry. Blockchain allows real-time access to product information, not for manufacturers, transport companies and distributors, but for consumers as well.

Smart contracts for insurers

The third big application of blockchain is smart contracts (Raikwar et al., 2018). In a narrow sense, a smart contract refers to a set of functions and data (current state) located at a certain address in the blockchain. The billing process begins when the patient arrives at the medical organisation and continues until the patient is discharged. It includes several steps: registering the patient, recording the services rendered, sending the information to the insurer, and receiving the insurance reimbursement. The billing scheme can be complicated as some of the services may be paid for by the insurance company and some by the patient.

The current operational difficulty with medical billing is the lack of transparency between medical organizations, patients and insurance companies. With the current systems there is a frequent case of insurance abuse by the patients and even the insurance frauds. Blockchain makes the system transparent, thereby eliminating mistrust. Unlike the traditional centralized systems currently used in healthcare, which allow information to be changed and deleted, blockchain and its characteristic of immutability of data is more suitable for recording important medical data, such as those related to insurance claims.

3 STRUCTURED REVIEW

In this chapter the overview of proposed blockchain-based electronic medical records systems is presented. It should be noted that new papers, reports on startups exploring the use of blockchain in medicine appear every day. The variety of blockchain projects in the medical field today is an indication of how many teams around the world are trying to improve certain aspects of both blockchain technology itself and healthcare in general.

The purpose of this section is to form potential stakeholders of the system and specific requirements for each stakeholder. Reference architectures will also be considered in the analysis - they will not be analyzed in detail consistently, but only taken into account in the design of the reference architecture within this work.

The research method used is the systematic review of literature and developed solutions. Due to the lack of literature, a more explorative approach is used, that varies on the systematic literature review. Also, because blockchain is a relatively new research topic, an exploration outside the scientific literature is used to get extra information. Therefore, to be reviewed: scientific papers, startups and public health government initiatives.

3.1 Scientific papers

This section will explore scholarly articles to help answer the main research question. The methodology will be presented first, after which the search results will be reviewed.

The systematic literature review method was used. To find the related scientific articles the search terms

- *Blockchain EHR*
- *Blockchain electronic health records*
- *Blockchain healthcare*

were applied to the information systems and healthcare databases such as Scopus, MEDLINE, PubMed and Google Scholar. The result of the study will be a list of potential stakeholders and requirements. Based on collected requirements and stakeholders, the possible reference architecture for the systems will be presented.

Not all studies can or will be used, as many are irrelevant or of low quality. The studies that will be used for the literature review must meet the criteria:

- Paper is English language
- Freely accessible
- Study is related to the research question
- Longer than 6 pages

These criteria are used to first select the papers. Finally, 60 unique relevant papers were identified. Some of them will be discussed in the following paragraphs.

Azaria et al. proposed MedRec (Azaria et al., 2016). It is one the first proposed EHR systems based on the blockchain that has been proposed. MedRec is based on Ethereum, and the main function of this platform is to record and store medical records in a form that allows patients, doctors and patient relatives (or any people having the needed consent) to access the medical record. Appropriate confirmation from the patient or person with access will be required to add the information to the blockchain. The medical record contains a comprehensive history of the patient's condition - diagnoses made, treatments performed and other medical manipulations. It is also worth noting that MedRec is a private blockchain developed on the Proof-of-Stake consensus protocol. In addition to its primary task of storing medical data, MedRec will be used for clinical and scientific research in the field of aging therapy. In doing so, each patient will be able to develop a strategy for overcoming health problems with the help of open information about his or her own health status.

FHIRChain is a system that has quite a lot in common with MedRec (Zhang et al., 2018). It is fundamentally encrypted with public and private keys, with which the patient will be able to access the data and also give access to individuals when they request to add data. Thus, it is the key pair that serves as the means of identification. The approach to data encryption is standard - the content is encrypted using the public key and decryption is only possible with the corresponding private key. In order for a doctor to add a corresponding record to the blockchain for a patient, it must first be signed with the private key and then encrypted with the recipient's (patient's) public identification key. When the patient needs to access their data, the block will be decrypted with the patient's private key and the sender's public key will be looked up to verify that the corresponding entry was actually made by the doctor the patient was seeing.

Another interesting solution proposed is Action-EHR (Dubovitskaya et al., 2019). The researchers focused on the technical aspects - the main artifact of the study was the reference architecture. The architecture is built on a system with predefined roles, where there will be a clear functional distinction between doctors and patients. It is this role (membership) component that is responsible for generating public and private keys for identification. Doctors and other medical professionals are verified through a centralized node that stores an up-to-date list of specialists (researchers indicate The National Practitioner Data Bank as the example of such a node). The proposed framework assumes that data is stored locally in centralized databases of organizations, as well as in a cloud platform. It is with the second database that other network participants interact. The absence of the need to abandon the current solution raises the question of data synchronization between local storage and the cloud. The authors also pay due attention to the description of synchronization.

Patientory is a system for storing and managing medical data. The data is accessed through a mobile application. The platform issues its own PTY tokens. In exchange, users will be able to use the network to lease storage space for medical information, as well as make payments and smart contract transactions.

Within OmniPHR authors propose a distributed architecture model (Roehrs et al., 2017). The goal of OmniPHR is to partition the EHR into data blocks. The user can access EHR data through various devices - from mobile devices to special medical computers. Data appears centralized from a logical patient and provider perspective, but it is actually physically decentralized. To ensure interoperability, the proposed model uses the OpenEHR medical data transfer standard. A limitation of the model is that the data must meet this standard. Thus, the architecture implies that patient data that does not conform to the standard will not be able to be stored and transmitted within the blockchain network.

Data storing, consent management, and data sharing in a trust-free environment are the main aspects discussed by authors of MedShare (Yang et al., 2018). MedShare proposes the usage of smart contracts for the runtime logic. Smart contracts should cover the entire functionality of the solution - from secure storage to sharing.

Chen et. al. propose the storage and the consequent sharing approach (Chen et al., 2018). The main focus of the study is the security of data. As a final artefact of the study

the authors propose a service framework. The framework is analysed by certain quality attributes and is compared with the traditional (current) solutions.

The authors of the following article propose a blockchain-based model for the exchange of sensitive data (Dagher et al., 2018). The proposed model is based on the shortcomings of using blockchain technology to create electronic medical records, which are identified in a study of existing healthcare data management systems. The authors identify data privacy, limited storage for big medical data and the possibility of revoking consent to process personal data as fundamental problems with the current organization. The authors recommend a private or hybrid blockchain as the base system for the proposed model. The choice of these types of blockchain is driven by the need for increased performance, reduced energy consumption, and potential scalability.

The creators of BHEEM propose a blockchain-based structure for efficient storage and maintenance of EHRs (Vora et al., 2018). The authors present a potential architecture for the system and further evaluate it. The article suggests that it is unlikely to build an easily accessible and fully interoperable system. Nevertheless, through the use of smart contracts the proposed architecture may provide the patient with significant privacy and data integrity preservation. Furthermore, the authors conclude that encrypting records and ease of use are impossible to be implemented in one system, and, thus, there is a trade-off that blockchain-based EHR developers need to take care of.

3.2 Developed solutions

This chapter examines what projects already exist at the intersection of medicine and blockchain technology. Which of them are in production in the medical IT solutions market, and which are only at the prototype or idea stage.

To find possible developed related solutions a Google searches with the same keywords, presented in the previous chapter were used. 11 relevant projects were identified. The found solutions and their core characteristics were reviewed.

Guardtime uses a blockchain platform to store medical data for more than 1 million patients in Estonia (e-Estonia, 2021). The introduction of the digital health initiative (eHealth) followed the introduction of e-taxes, e-elections and e-schools. Estonia ranks 40th in the world in life expectancy among the 194 member states of the World Health

Organization. The goal of this e-health initiative is to increase the average life expectancy of a citizen from the current 77.6 years.

The key principle of the project's architecture: to ensure the exchange of data about any individual and any situation without restriction for any health professionals working for any health care provider. Estonia's application of blockchain technology in medicine is based on previously existing systems - e-health system in 2008 and e-prescriptions in 2010.

Open Longevity is a startup from Russia (*Open Longevity, 2017*). The developed solution proposes to analyze data on health status, age-related changes in the body and use them to create effective methods of aging therapy. Blockchain is used to ensure the transparency of all participants, easy control of information and access to it by researchers. The developed YEAR token will act as a means of payment within the platform. Users will receive them for uploading personal data to the platform, which will be analyzed in an anonymized form by research organizations.

The UK startup Medicalchain will be considered next (*Medicalchain* 2016). The development was initiated in 2017. The architecture of Medicalchain is built on smart contracts. Each smart contract implements the logic of temporary access to medical data. Temporary access is initiated by the data owner and issued to another member of the blockchain network. The actions of the other participant (e.g., the doctor) are recorded in the blockchain as transactions of different types. The platform also implements logic to provide anonymized data to research organizations. An additional functionality of the platform is telemedicine - a specialist receives cryptocurrency for a consultation through the service. Architecturally, the system is built on two blockchains. Hyperledger Fabric implements data access control logic, and all results of all interactions with the EHR are recorded on the Ethereum network.

BurstIQ is a startup from the US (BurstIQ, 2021). The concept within the whitepaper is designated as HealthWallet. As with other platforms, the user has access to their medical data: test results, diagnostic results, information from a personal fitness device, diet information, etc. The platform also implements the functionality of providing medical data in an anonymized form, as well as the functionality of remote consultations by specialists. The big advantage of the platform is compliance with such data storage standards as GDPR (Europe), HIPAA and NIST (USA).

Blockchain Health Co**.** is a startup from the US (*blockchainhealth.co* 2017). Their mission is to provide a direct link between people who want to share their personal health data with scientists for their research. The means to accomplish this goal is a platform based on blockchain technology. Users will be able to authorize access to and control the use of certain health data through an app. The data to be uploaded can be of any type: images, documents and more. The system will be monitored by experts to verify that information remains confidential. The developers offer full marketing freedom to research organizations that will participate in the project, encouraging them to promote their own data processing applications, subject to their inclusion in the infrastructure.

Pokitdok is a platform from a team based in Silicon Valley, California, that provides a set of APIs for developers who create healthcare experiences (*pokitdok, 2021)*. It can be used to perform X12 transactions, find healthcare providers, and obtain pricing information for medical procedures. The platform is intended for third-party developers of insurance companies, health systems, medical digital companies, in general, anyone who wants to create new applications that would improve the healthcare experience and streamline business processes. It cooperates with 650 trading partners that can be connected to get real-time transactional data.

Another functioning project that implements the process of storing medical data on blockchain is Healthchain (*HealthChain - Blockchain For Medical Devices* 2021). The project was initiated by Stanford University. The service presents the stored data to the patient in a convenient, aggregated form, forming up-to-date information on the state of health and relevant recommendations. Predictive analytics logic is also implemented within the product. The platform implements five types of user roles - patient, health care providers, insurance companies, and research organizations. The developers put the convenience of using informative graphical representations as a key priority.

IRYO is a service built on the EOS blockchain (*IRYO.NETWORK* 2021). The key emphasis in the development was placed on the level of security of data storage and transmission. The platform implements the functionality of anonymized provision of medical data by patients, for which the IRYO platform cryptocurrency will be paid. The product under consideration implements the possibility of creating cross-platform medical applications, as it has open source code.

CareX is a project that is developing through health care payments (*Carex* 2021). It uses its own CAREX token as a financial asset. Owners of the token can store their medical data with guaranteed privacy. The platform implements a chatbot that provides an alternative interface for interaction, which in turn generates predictive analytics results. At the moment, the platform operates only in the U.S.

QuantH is a platform being developed in Texas by a public medical company. The main goal of QuantH is a comprehensive solution that will offer a wide range of medical services on decentralized services on blockchain. The creators also emphasize ease of integration with current architectural solutions.

Synthium Health is a trading platform for creating business relationships between healthcare providers and suppliers for cost-effective exchanges. According to the authors' idea, the platform will enable providers to expand their presence in the marketplace, sell products faster, and reduce operating costs. Synthium Health also plans to partner with logistics companies. The platform has its own token, which is needed to register an account and obtain membership in the portal. The Synthium token (SHP) also allows for transactions. SHPs will be used by buyers and sellers to pay for trades on the Synthium Health platform.

3.3 Discussion

The analysis formed a certain picture of the presented functionality of a variety of solutions. Different solutions are oriented to different stakeholders, however, generalizing, it is possible to distinguish the following groups:

1. *Primary* - those, who are directly concerned
    - Patients,
    - doctors (any specialities) and nurses,
    - pharmacists,
    - laboratories.
2. *Secondary* - rarer involvement case
    - Insurance companies,
    - employers,
    - relatives,
    - research institute

3. *Third* - global-scale stakeholders
    - Society,
    - public authorities.

Primary stakeholders

This stakeholder group is primarily concerned with data security and privacy issues. The main stakeholder in this group is the patient. The patient wants to have full control over access to medical data with the function of granting rights to view and update their medical history.

The most important value for the patient is effective treatment. This is accomplished by presenting the complete medical history in an aggregated form that frees the doctor from having to review the patient's medical history in detail based on the patient's own telling or on the documents that were brought.

The blockchain does not store the files - therefore, the distinct technology must be used. Needless to say, medical data has a relatively high volumes. Medical records can include not only medical conclusions, but also the results of all kinds of medical examinations. The file storage system should have the following characteristics:

- Distributed. Since the entire blockchain infrastructure is distributed, the file repository should also be distributed.
- Data sharding supported. If the application is expected to store huge amounts of data, the storage capacity must be maximised. Full replication of data on each node may be considered as the way of maximisation, as it reduces the chance of data loss in the case of problems with individual nodes, however, with the large network it is extremely redundant to duplicate data on all servers.
- Fast. Popular applications may require hundreds of thousands, if not millions of transactions to store and increment data per second.
- Structured. The repository must be able to maintain an internal data structure to enable applications to link individual records to each other.

If enough data is available for analysis, the system can build predictive analytics. Condition monitoring on collected data from IOT detectors will allow trivial cases to be identified. Since this goes against data privacy, such analytics require logic to anonymize the data.

Potential patients also rely on verification of data added by doctors. Before each online record update, the patient should be able to review the transaction in progress.

Most of the sources reviewed place great emphasis on the ability to integrate with current information systems in use, as this will require fewer operational changes for everyone involved in the process within the medical organization. With the growing popularity of IOT devices, there is also a need to integrate these devices with the network. Covering this requirement involves working with big data, which affects the emergence of new non-functional requirements. However, this is quite an important use case for the system, as the data collected will help to get a more complete picture of changes in the human condition.

Also, the potential patient is interested in a separate stored type of data - data required for emergency care. Such data may include the current medications the patient is taking, the patient's blood type, allergies, etc. Emergency information should not require verification of access by the patient, as there is likely to be a case where the patient cannot physically provide it. Also, it should be noted that this type of information without confirmation by the patient should be available only to a certain role of users - the doctors providing medical care. This requirement again refers to the mandatory differentiation of roles in the system.

Notification services may also be included in the system. The notification system can be personalized by operating on the user's historical data. For example, to remind the user to be examined by a doctor with an appropriate specialization or to take the appropriate medication. Also, with the implemented integration with IOT devices, notifications can be sent to medical organizations if the patient's condition is critical and the data confirms it.
Interoperability and consistent data standards may be used to improve intersectoral communication.

It is also worth mentioning the need for a high degree of usability and intuitiveness of the interface, since patients are not a segmented group of users, but the population as a whole. Different types of interfaces are required, from mobile apps to voice assistants.The implementation of an open API will help developers create their own client applications that maximize the usability of the system. Creating an open source code base can fundamentally increase the efficiency of development and the frequency of delivered functionality, as developers with a variety of skills will be interested.

Secondary stakeholders

Secondary stakeholder requirements must also be considered to maximize the effectiveness of the system being developed. One of the secondary stakeholders could include insurance companies. Earlier in the paper, the case of using blockchain in healthcare was described. Such blockchains and blockchains for storing medical records could be integrated, thereby taking advantage of almost all the best features of blockchain.

Patients are also interested in the ability to fully or partially transfer the management of medical information to certain individuals - for example, relatives or other health trackers. This mode is similar to emergency access mode, but unlike it, all data can be controlled and managed under this mode. not just those that can only be accessed in an emergency situation.

Tertiary

Stakeholders in this category are primarily interested in analyzing aggregated data. These data can be useful for understanding the full picture within health care - the dynamics of specific diseases and viruses, the effectiveness of the treatment provided in different health care organizations, and, most importantly, the conduct of research. Research on large, reliable data sets provides a strong basis for relatively accurate prediction of disease and disease progression. Here, as discussed earlier, special anonymization mechanisms are required to cover the data privacy requirement.

The patient himself may be interested in such functionality because permission to access such information can be monetized. Research institutes or any other interested party will leave a request for data under certain filters and categories describing the purposes of the research being conducted. The patient will be able to choose which project the data will be supplied for, its size and completeness, as well as form the price.

After identifying the stakeholders and briefly reviewing the identified requirements, an extension of the motivational map was constructed:

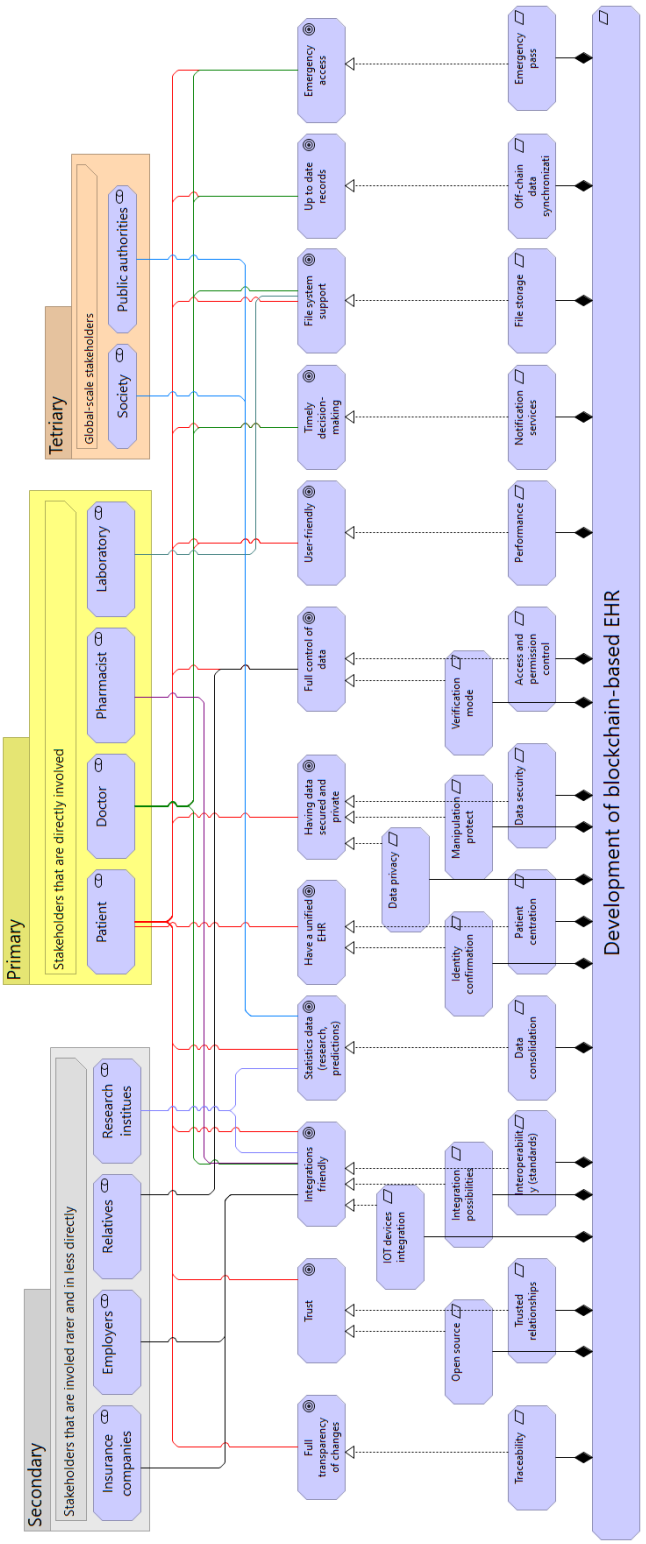

Figure 16 — Mappings of requirements and stakeholders

It is possible to cover the above requirements without implementing blockchain technology, but blockchain-based architecture has undeniable advantages over centralized implementation or distributed non-blockchain. The benefit of blockchain stems

from its key characteristic: decentralization. Thus, the system will not have a single point of failure and is therefore less prone to system failures. In the event of a failure at any node, the system will not be significantly affected.

Blockchain exercises full sovereignty over patient data - now the patient himself owns his data. Medical data does not grab medical records, but is only accessed after mandatory confirmation by the patient. Fundamental mechanisms such as the consensus mechanism make it virtually impossible to manipulate data. Blockchain records will be impossible to tamper with. Cryptographic mechanisms will strengthen the overall security of the system. A system developed on a blockchain with implemented data transmission standards greatly enhances cross-sector communication. The most popular global standards are represented by H7 (Health Level Seven International 2021).

Overall, the benefits of blockchain-based electronic health records can significantly improve patient-centered care. The answer to the **SQ2** and **SQ3** was given.

4 SYSTEMS ARCHITECTURE

This section is the key section of the paper, as it is here that the main artifact - the referential architecture - will be proposed. The first thing that will be described within this section is the description and justification of the chosen enterprise architecture modeling language. The reasons for the choice will be justified. and the meta-model will be presented. Next, the scenario under consideration will be presented - the patient visits two independent organizations separately. The scenario will be broken down into phases. Each phase will be considered in terms of the process within the medical organization.

Regarding the process within the organization, the current enterprise architecture will be constructed. The schema will be broken down in detail. Problems with the current architecture will be cited as well as the lack of compliance with the requirements generated by the systematic analysis.

The next step will be to build a reference architecture. First, a definition of reference architecture will be given. Next, the method used in the design will be described. The methods of evaluation of the built model will also be described.

After the reference model is built, it will be applied and reviewed within the generated scenario and, accordingly, the processes of each medical organization. First, the migration process will be built that will reflect what is necessary for the transition from the current architecture to the target one. Next, the architecture model itself will be built.

4.1 Enterprise architecture modeling language

To get an overview of the impact of the implementation of blockchain in the current system, the whole enterprise architecture must be analyzed. An enterprise architecture aligns business processes, IT systems and the technology used (Choque & Bayona-Ore, 2020). Enterprise architecture aligns mentioned layers with motivation and strategy, highlighting the impacts of implementation. It starts a continuous evolution within dynamic environments (Desfray & Raymond, 2014).

A language used to model enterprise architecture is Archimate (Syynimaa, 2018). The language helps various stakeholders design, evaluate business decisions. The basic entities and relationship types of the ArchiMate can be considered as a framework. On

each of the discussed levels the framework considers the following aspects: active elements, the internal structure, and the elements that determine the use or transfer of information. In other words: subject, action, object. The meta-model is presented on the following figure:

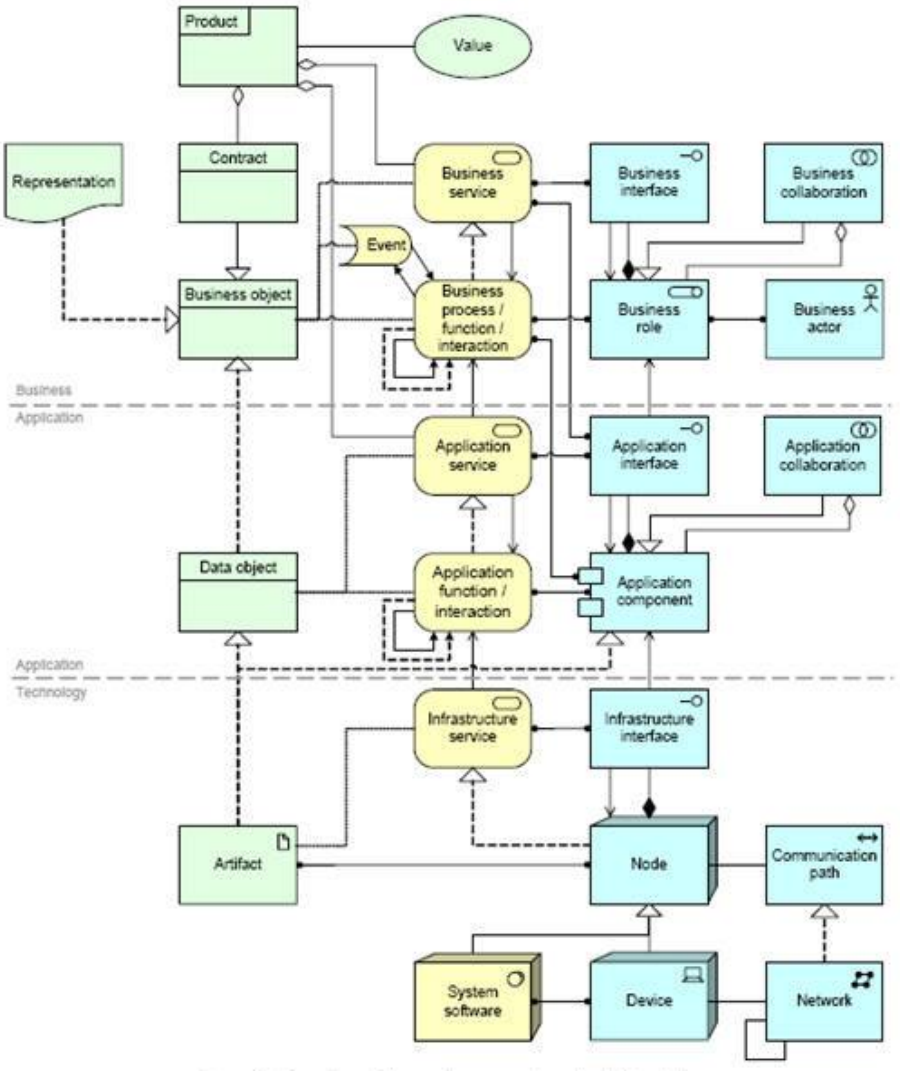

Figure 17 — Archimate meta-model

As it could be seen in the diagram above, conceptually schema implies the usage of service-oriented architecture (SOA). SOA is a style of enterprise or software design in which system components are linked by a Consumer-Service relationship, where one component provides a service to another (Bean, 2010).

Giving the definition of service - it is the benefit that the system provides to its environment while hiding internal operations. For external systems Service provides a certain value, which is the motivation for its existence. In the software context, Services provide an API

and/or UI for interacting with them. In the Archimate notation the key logic of service-oriented architecture is presented on the following figure:

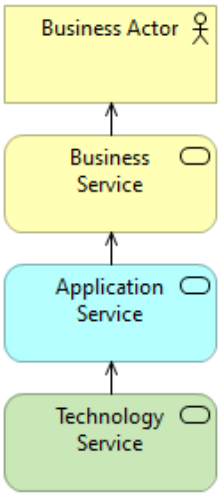

Figure 18 — SOA key logic

4.2 Process

A modern medical organization is a complex system with a large number of heterogeneous objects involved (management technologies, personnel, elements of information and communication architecture and technological infrastructure, material, material and cash flows, data and document flow, etc.), interrelations and interfaces between them. The key factor of successful functioning of such a system is clear relationship and well-functioning interaction of all levels of enterprise management, which is subordinate to a single strategic vision, realizing strategic goals and fulfilling strategic objectives.

Enterprise architecture requires the coordination of the following layers: business architecture (business layer) defines the structure and mechanics of the business, allows to structure and coordinate the implemented functions, business processes, determine the hierarchy and structure of process performers (organizational structure).

Due to the above-mentioned specifics, the main processes of medical activities were identified on the basis of the form of medical care and services. Typical functions of a medical organization (process landscape) are presented below. The proposed models contain a list of functions of medical organizations, obtained in the analysis of existing practices of modeling the activity of medical organizations in Russia.

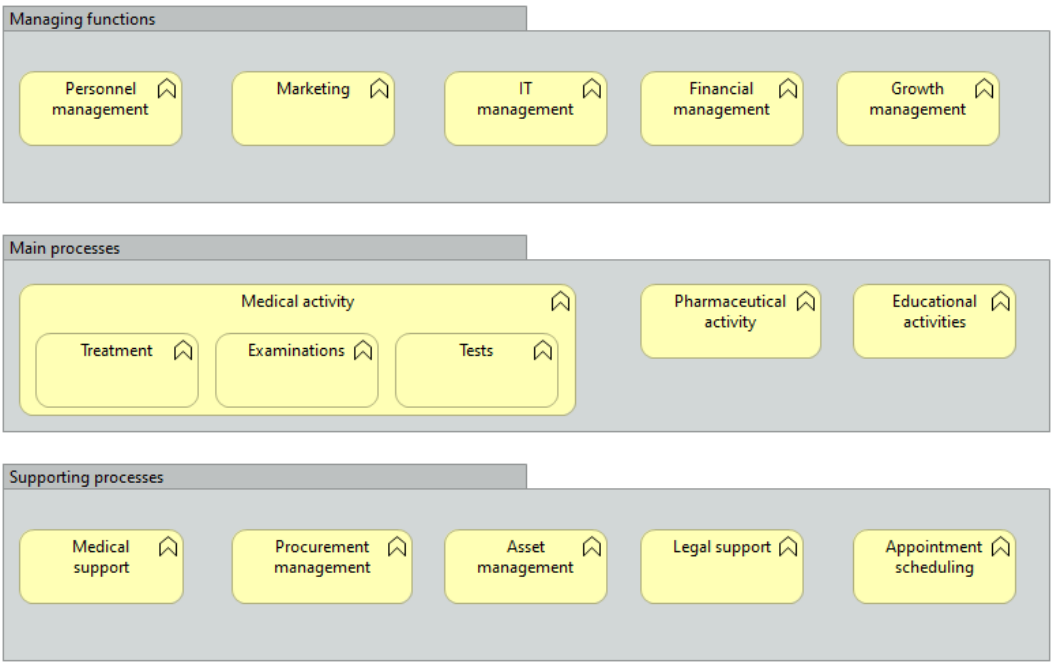

Figure 19 — Landscape of typical processes in the medical organisation

Thus, a medical organization involves many processes, some of which are unrelated to the focus of the company. Although building a complete enterprise architecture model requires a detailed consideration of all processes, this paper will consider only the process of examining a patient by a doctor - *treatment*.

Also, depending on the doctor's specialization, the examination process may be different, as different specializations may imply, for example, different examinations and procedures, both in terms of the level of complexity and the number of participants involved in the process. In this paper a simplified process of visiting a patient to a general practitioner will be considered. The neglect of detail is acceptable, as the main purpose of this work is aimed at the technical components of the system rather than the organization of business processes. After the simplification the business process may have the following form:

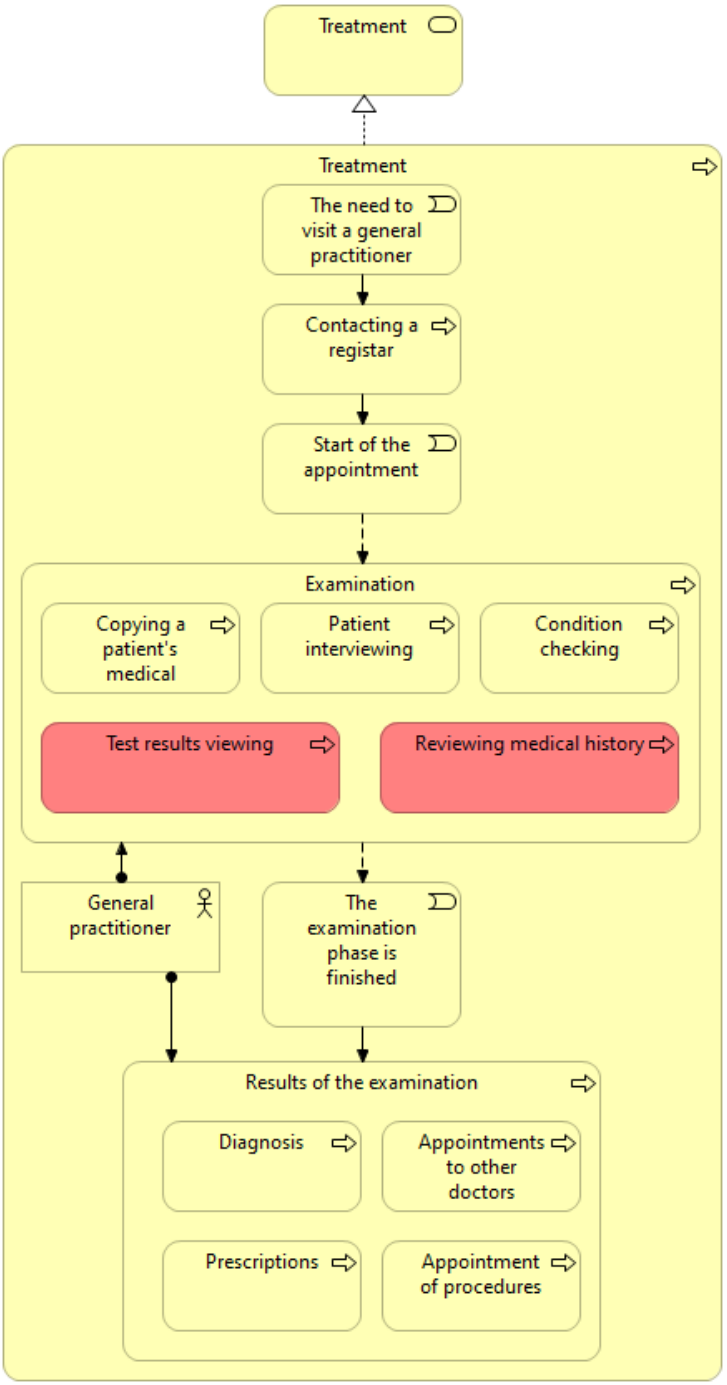

Figure 20 — Landscape of typical processes in the medical organisation

In order to identify the current issues more precisely, the following scenario may be taken as a reference point. The scenario was chosen for consideration because of the frequency with which it occurs and will be modelled as a business process in the following parts of the thesis.

Phase 1: A person went to the doctor in medical organisation 1. Person's EHR was updated.
Phase 2: Emergency case happened in different geographic region (country, city etc.) and a person went to the doctor in medical organisation 2.

Visualizing the scenario as services at the business layer, the following diagram can be constructed:

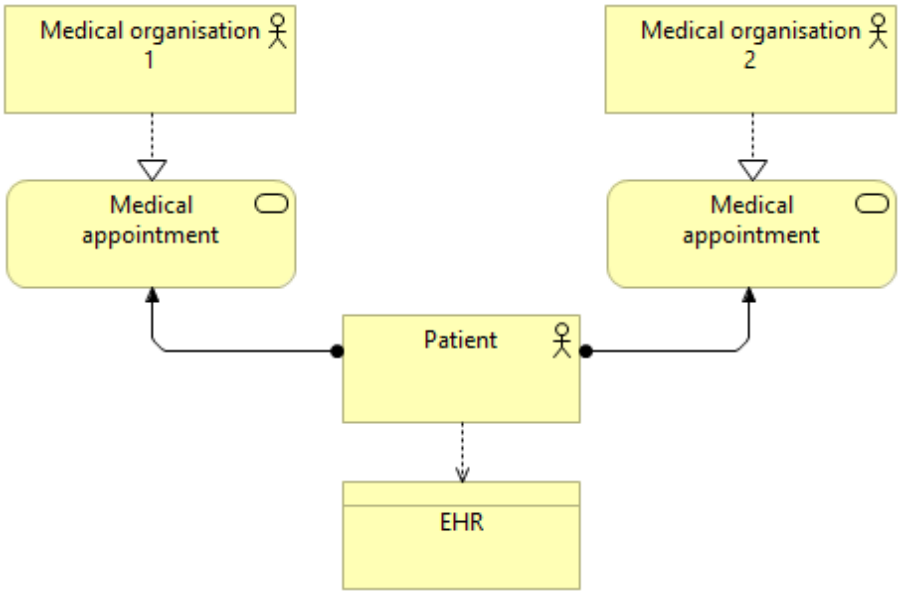

Figure 21 — Scenario visualized

Aligning the scenario with the process introduced above, the following diagram may be considered as detailed process with the given scenario:

Figure 22 — Detailed business process based on the scenario

In order to simplify and avoid duplication and overcrowding within the diagrams, all subsequent architectures will only show the process within one medical organization, not two, as the scenario initially implies. Also, in order to visually align the process elements, these elements will be rearranged.

4.3 AS-IS model

This section will break down the architecture of the typical medical organization for the process presented earlier AS-it-IS. Each level of the architecture will be described. Problems will then be identified and correlated with those described earlier in the paper. Eventually, a motivational extension will be constructed that will map key stakeholders and dissect in more detail their potential interest in changing the architecture.

4.3.1 Architecture

The typical solution architecture that now supports the previously described process is visualized in the following diagram:

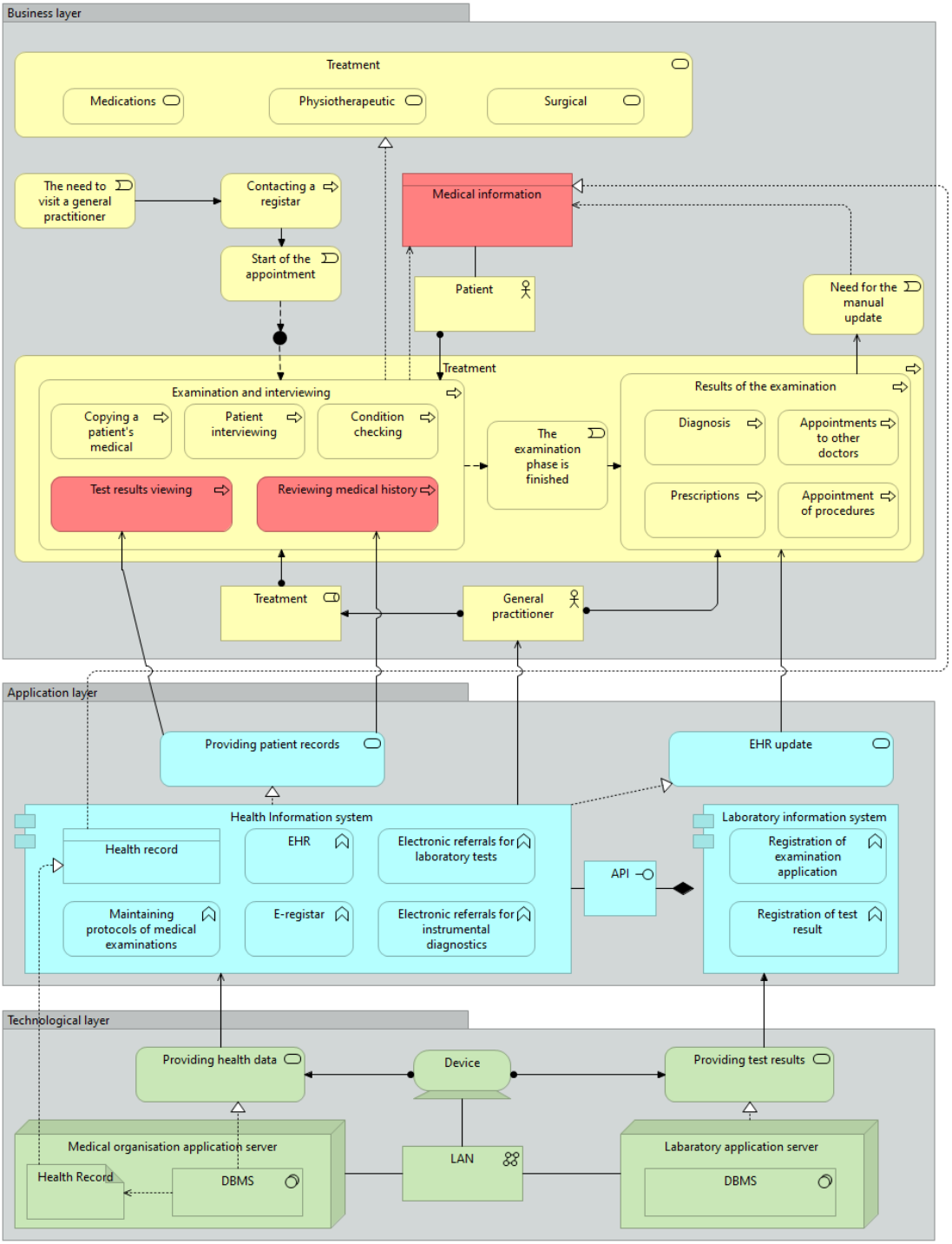

Figure 23 — AS-IS architecture

Below each of the layers of the architecture will be discussed in more detail.

Business layer

The following figure shows the AS-IS business layer:

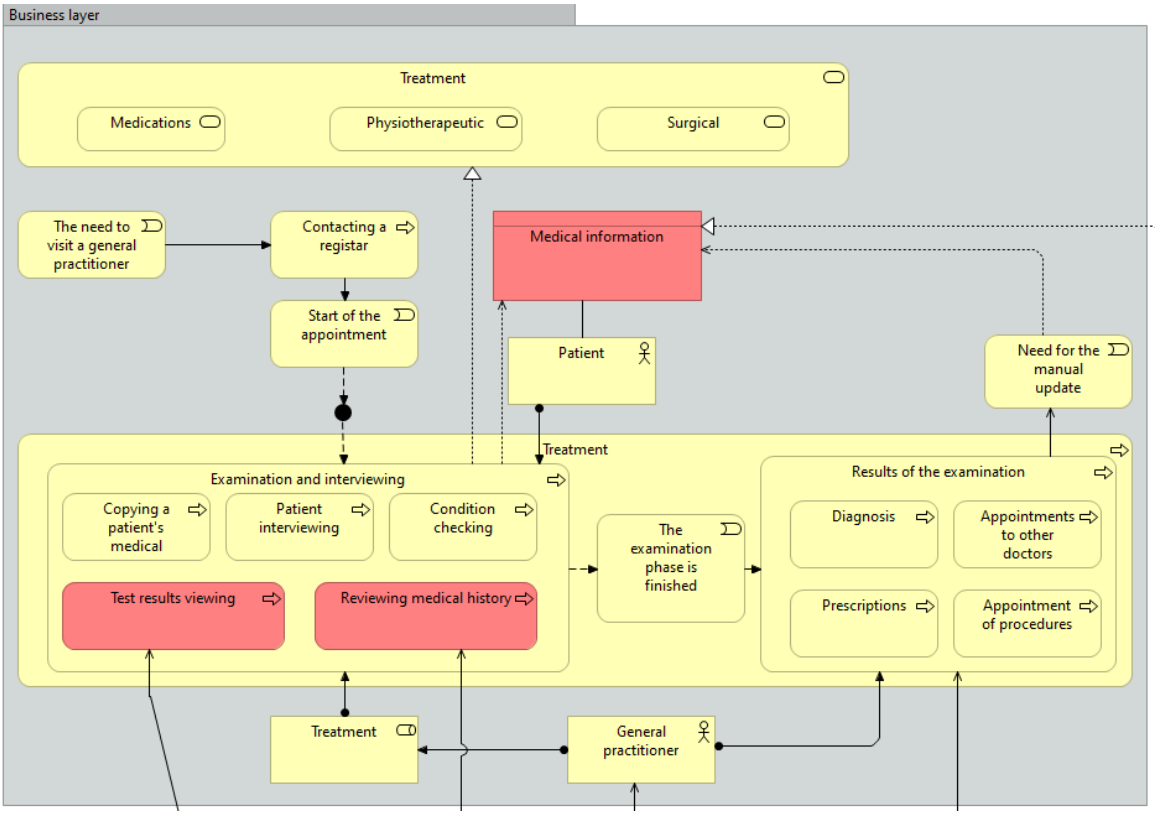

Figure 24 — AS-IS architecture. Business layer

The process within the current architecture does not change, as well as a service treatment. As it could be seen in the diagram, for the examination process, the doctor will be able to obtain data from the patient from two sources - 1. the data are stored within the information system of the medical institution, if the patient had previously undergone the appropriate examinations 2. the data obtained outside the medical institution (past examinations), provided by the patient in the form in which he collected them (can be printed copies, an application on a smartphone, etc.).

In order to get a complete picture of the patient's condition, the doctor needs all the data on the patient's medical condition. While the data under item 1 are standardized and can be presented in a way that displays the information in a convenient way, the data that the patient has provided on his/her own requires some time to systematize.

The highlighted red color processes are those that are served with the local health information system that stores patients' EHRs. Those application layer services will be discussed in the next chapter. Then, one of the other points that is important to be highlighted is that the patient is required to independently aggregate the treatment results after receiving the treatment results to provide them to the next healthcare facility where they will be evaluated.

Application layer

The following figure presents the AS-IS application layer:

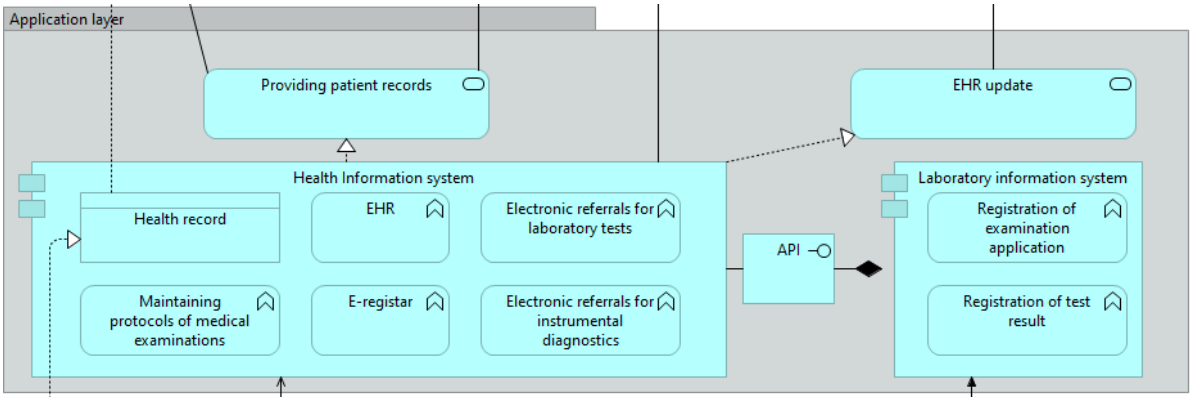

Figure 25 — AS-IS architecture. Business layer

For the treatment process and with the condition of linkage to electronic medical records, two services are required from applications - providing patient data (medical history, examinations, previous reports, changes in condition), and a service for updating medical records after each visit to the doctor.

Each of these is provided by a medical information system that functions locally. Such an information system can have other functionality in addition to electronic medical records (the diagram shows the functionality).

Also, when performing biomaterial analysis, the patient often has to undergo tests within the same organization. The biological material submitted is processed in laboratories, which due to the specifics of the data and other processes most often have a separate information system that has an interface with the central system, for example, through an API. Thus, the central system can receive data from the laboratory information system and correlate it with the patient.

Technology layer

The following figure presents the AS-IS application layer:

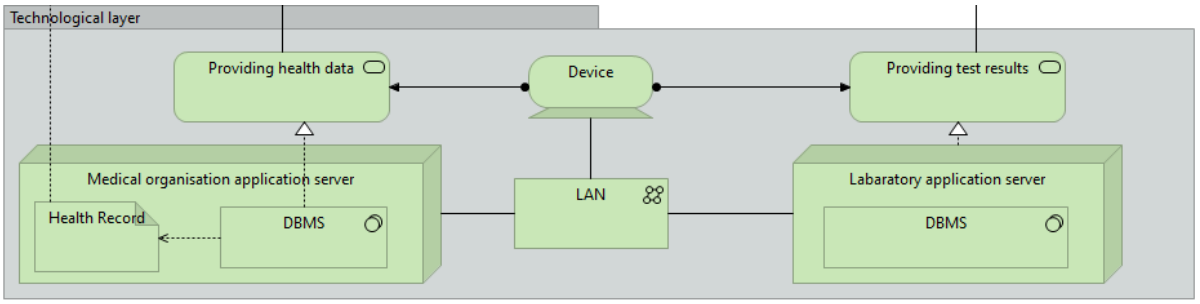

Figure 26 — AS-IS architecture. Technology layer

To allow an application to perform its functions, it is sufficient to let the application perform CRUD operations to keep the records up to date. CRUD queries will be sent from the application to the database management server, which in turn communicates directly with the database. In this regard, the technology layer implies two services - the provision of patient data and laboratory data.

Also, as can be seen in the diagram, all user devices (employees of the medical organization), as well as database management systems, as well as the databases themselves are stored locally. Accordingly, interaction between the nodes also occurs locally.

4.3.2 Problems with the current architecture

Speaking of the problems that are associated with the presented scheme (process discussed), the following may be highlighted:

- Fragmentation of data. Despite the fact that medical records are stored only within medical organizations, patients have the right to make copies of fragments of medical records (results of examination over time, results of tests, etc.). As seen in the diagram, in order for the client to get a complete picture of his health, that is, in fact, his medical record, aggregated for all medical institutions where the patient was examined, the client must somehow update the information manually after each - in the form of printouts, mobile application or in some other way. The fragmented nature of the data, generating a distribution of fragments of the medical record, significantly reduces the likelihood of making timely decisions. Also, in the event of an emergency situation where it is physically

impossible on the part of the patient to describe the condition, any limitations (such as allergies or type of bed), the ambulance will not be able to provide immediate care, again because the patient's medical record is something that is stored within databases of various medical organizations or something that the patient manually aggregates.

- Data Ownership. Under the current architecture, patients' medical records belong to medical organizations and are stored only within the organization. To get access to the full medical records, the patient must make a request, as a result of which the patient will be granted temporary reading access. Thus, in fact, a system is formed where patient data "does not belong" to the patient himself.
- Centralization of the system. When a central server, for example, that hosts the database, fails, the organization cannot perform certain processes related to the technology services that have been disabled. Centralized data storage makes it possible for attackers to access all data at once and, accordingly, perform any manipulation of it without the potential detection of unauthorized changes.

The answer to the **SQ4** was given.

4.3.3 Motivation extension

Since the problems, stakeholders, requirements have been identified and subsequently a motivation diagram correlating requirements and stakeholders has been constructed, it can be used in the context of the considered business process. In the next chapter, in the design of the IT architecture of the reference model, the previously defined requirements will be aligned with the new services that the blockchain-based architecture implements in the context of the current business process.

4.4 Reference architecture

The main goal of this research is to create a reference architecture for blockchain based transaction systems that can be integrated with other systems. In this chapter a new reference architecture is developed. This is done by using a structured method.

4.4.1 Definition

The concept of reference architecture is a part of enterprise architecture. The reference architecture is an abstraction and can be used as a blueprint to create enterprise architectures within a specific domain. It provides the principles, guidelines and best practices to create a concrete architecture. It describes the components that should be used, but these need to be selected for specific systems. An architecture can effectively and efficiently communicate the business processes, the information systems that are used, and the technical infrastructure that supports the application layer.

4.4.2 Method

The method inby Iacob will be used to develop the reference architecture. This method is based on the TOGAF architecture development method (ADM). With a multi-step cycle, TOGAF is used to link business, information systems, and IT structure. Authors use TOGAF in conjunction with the modeling language Archimate. Archimate has been introduced and used previously to create the current solution architecture.

The following shows the TOGAF phases along with the corresponding Archimate layers. As it could be seen, ADM is an iterative process. This will not be done in this study. In this study, the preliminary phase and phases A through E are performed:

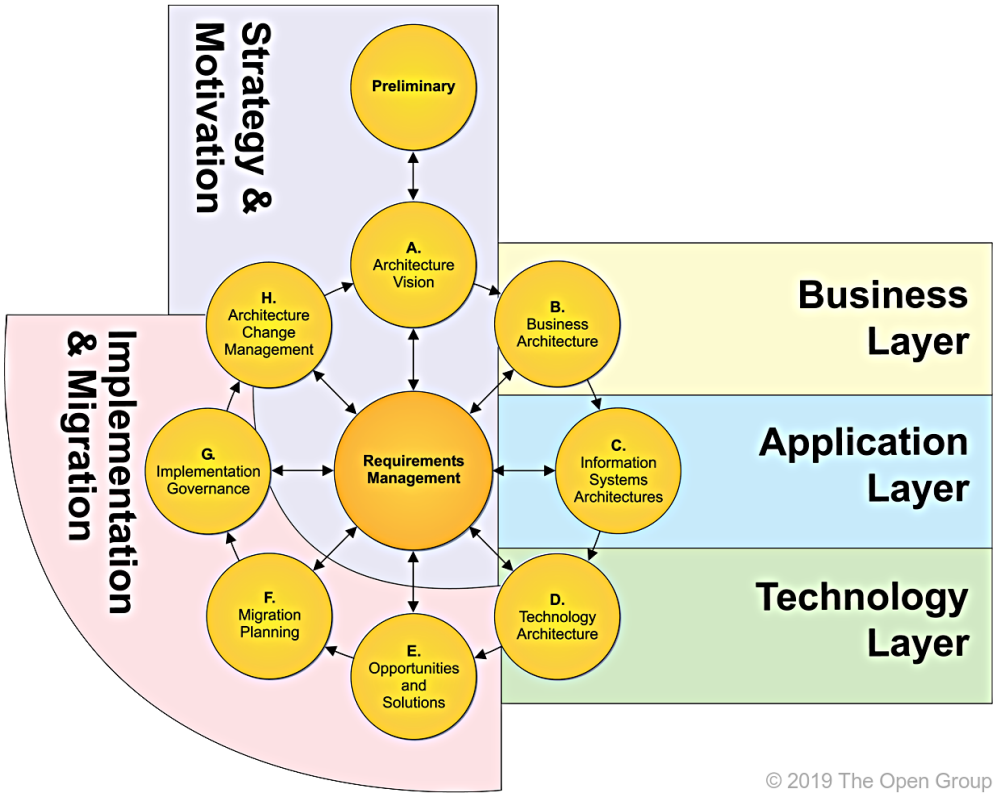

Figure 27 — Correspondence Between the ArchiMate Language and the TOGAF ADM (*ArchiMate® 3.1 Specification* 2021)

The preliminary phase has already been done in previous chapters. A vision of the architecture was presented in the introduction. The literature review and case study analysis were used to gain information about the domain. An architecture vision was also created. The development phase will complete phases B, C, and D, which will create an architecture consisting of business, application, and technology layers. The reference architecture will then be used in the scenario under consideration to create a new enterprise architecture for the target implementation. This will be one of the opportunities and solutions of Phase E. The proposed architecture will then be subject to evaluation. The evaluation will be done from two perspectives: a technical perspective and an impact analysis.

4.4.3 Architecture

In this section, the reference architecture will be presented. The information gathered in the first chapters is used to come to this architecture. Each layer will be explained, to give a clear view of the architecture. The proposed reference hase a following look:

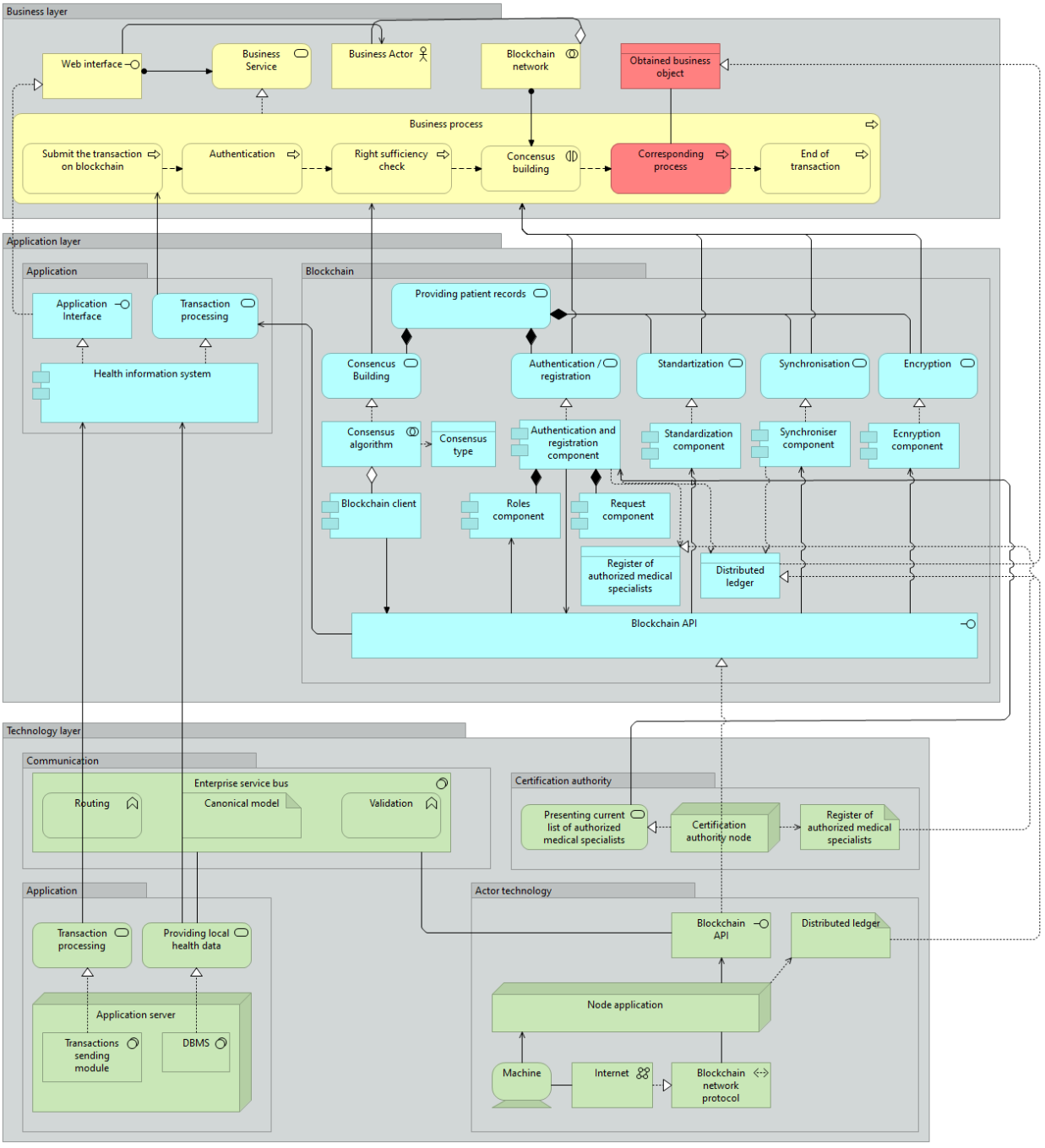

Figure 28 — Reference architecture

Business layer

The business layer of the reference architecture has the following look:

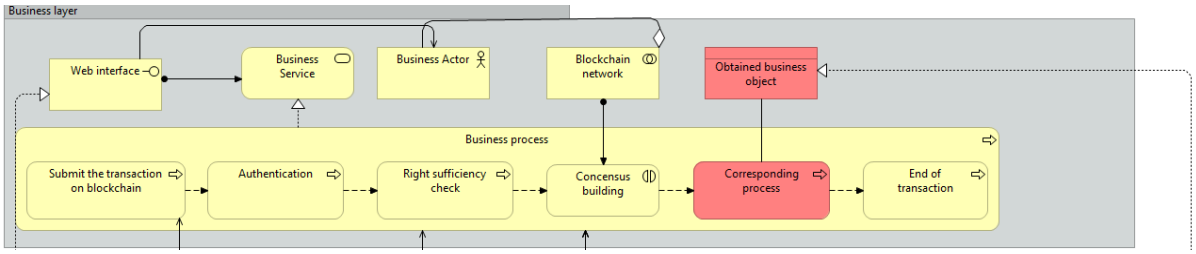

Figure 29 — Reference architecture. Business layer

One of the goals was to create a reference architecture to support the processes occurring within a medical organization. With the architecture presented, it is possible to support a diverse range of processes as long as they correspond to the elements present.

The first element considered is the business actors . The actors within this element can play different roles and there should be several such roles. They can be modeled in a single actor element, but it is required that there be more than one participant. This is because these participants must be part of a collaborative blockchain network. Together, they are responsible for interacting to achieve consensus within the process.

Actors will use the web interface as their access interface. As discussed earlier, it is recommended that an open client application API be implemented for the potential diversity of applications. This business service is implemented by a business process. A business process in the meta-model implies an organization's business process (marked in red and can be anything), but it has several mandatory elements (all others within the business process). The business process starts with sending a transaction to the blockchain and ends with reaching consensus. After validation of the transaction (the sender of the transaction has enough to make it happen) the corresponding business object (in the case in question - a medical card) is returned, which is a value for the actors. After successful consensus, the business process can continue.

Using this business layer for the reference architecture, the reference architecture can support multiple business processes and services.

Application layer

The application layer has the following look:

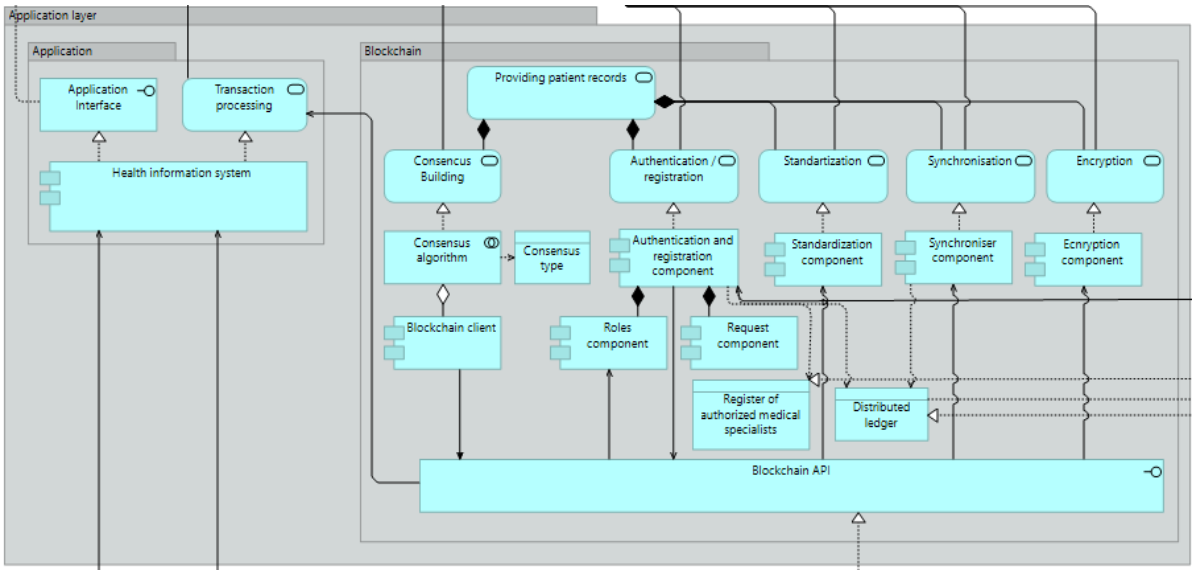

Figure 30 — Reference architecture. Application layer

To minimize the resources for switching from the current architecture to the new one, this group is almost unchanged, except for connecting the module for sending requests to the blockchain via the blockchain API. All interaction between the current system and the blockchain will be implemented exactly through the API.

The Blockchain Layer group are application elements of the blockchain. The most important service is the provision of the EHRs. As it could be seen, ulike the current architecture, this service is realized now by the blockchain application, not by the local information system. They work on the application of an actor technology layer node - this implies that each actor hosts a node in the blockchain network. Each of these nodes has all the elements of a blockchain application. The blockchain client is the software component that is responsible for communicating with the outside world; it serves the blockchain API to provide a common ledger for processing web application transactions.

In the figure an application data object in the diagram that represents all the transactions stored in the blockchain. This object is key within the reference architecture because it expresses the essence of blockchain technology. The blockchain client can access this ledger to retrieve data or to send a new transaction when the consensus algorithm succeeds. Some components interact with it.

Standardization component: implemented for constructing, storing, and transmitting records according to the clinical standards. This component controls the formatting of EHR data so that it conforms to the rules set.

The Authentication component is responsible for authenticating system users who have access. The types of users are pre-defined and can be as follows: doctors, hospitals, clinical centers and patients. To authorize health care providers on the blockchain, the component uses an appropriate data object that is continually updated by the government system. This one also generates public and private keys for the user. The public key is stored in the blockchain network so that other users, such as physicians, can add records addressed to other users (patients). Only the patient has access to the private key. Each time a user attempts to access the system, they will need to use it to authorize themselves. The component itself consists of two subcomponents, Roles and Requests.

The "Roles" component is responsible for managing access to each role. Each role has a predefined set of accesses and gives the corresponding functionality in the system. The functionality of different roles may overlap.

The request component implements the logic for granting or denying access to personal data. Requests will be sent from doctors, clinical or other organizations to patients. Until the patient gives appropriate approval, personal data access will not be granted.

The encryption component performs strong data encryption with pre-obfuscation. The user's private key will be used for encryption. Thus, even though every user will be able to get the encrypted data, only the patient himself or the persons to whom the patient has given decryption access will be able to decrypt it.

The synchronizer component maintains a synchronous state between the medical organization's local database and the data stored in the blockchain. This component allows the medical organization not to abandon its current solution, thereby making the transition to a blockchain-based architecture as easy as possible. Also, the synchronization component will allow in the event of a medical organization's failure to write in the blockchain, after the connection has been restored, to put the data that appeared during the lack of connection.

The consensus algorithm engine is responsible for the work that needs to be done to achieve consensus. Basically, it's computing hashes for the blockchain. How consensus is achieved between all the nodes is recorded in the "consensus type" data object. This indicates that the reference architecture can be used by all consensus algorithms. This consensus building service then serves consensus building for business interactions. This indicates that all layers of the blockchain will need to collaborate to achieve consensus.

Technology layer

The technology layer has the following view:

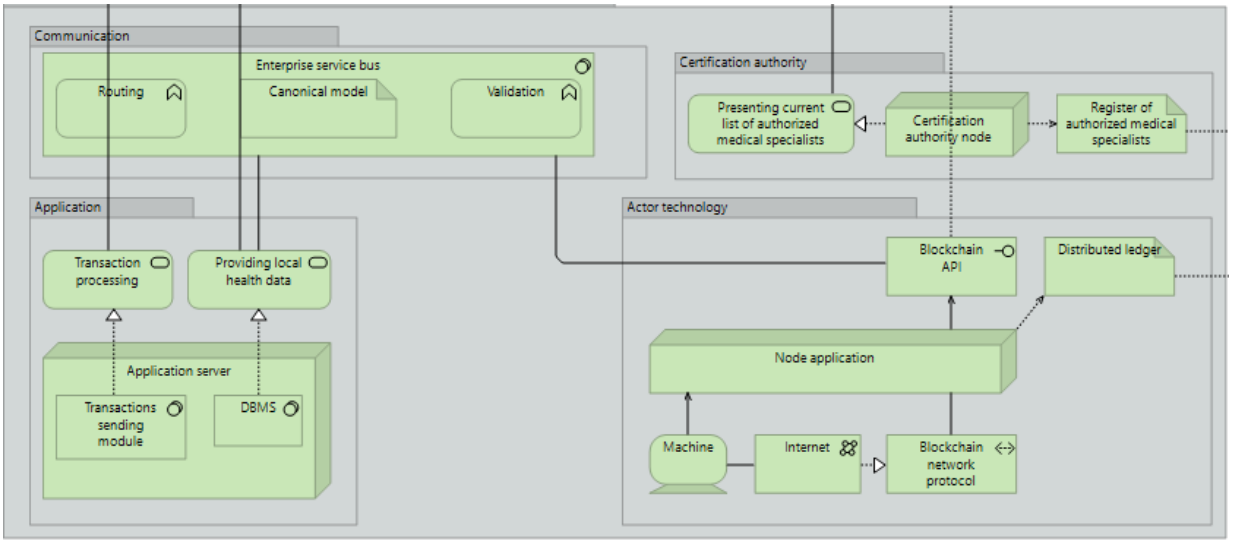

Figure 31 — Reference architecture. Technology layer

First, the Application group. This is the application server that hosts the web application. Basically, here the infrastructure of the current system is placed. Here, it almost copies the current state infrastructure, but as the transaction sending module was added previously to the application layer, the corresponding technological service should be added too. The transaction processing service is the implementation of the application transaction processing service.

To create fast integrations with other systems, the enterprise service bus was added to the architecture to handle the communication between all the different technology nodes. This enterprise service bus is modelled as a system software component. The enterprise service bus can be hosted anywhere. It has some general elements like routing and validation functions and it uses a canonical data model to map incoming messages to the desired output for each system.

The user's technology layer represents the technology layer of each of the actors/participants within the system. Each user must be active in order to participate in the blockchain network. Therefore each user should run a node application on a machine. This could be a virtual machine, or hosted on a local server, but it should be active. The nodes communicate with each other when a new transaction is submitted and will build a consensus. This is done directly between the nodes, over the internet using a specific blockchain network protocol. This protocol will depend on the blockchain technology that is used. The node application implements both the blockchain client and the algorithm engine. As said, they were separated to indicate the difference, but they run on the same node. The nodes will communicate with each other through their own protocol, but the communication with the application goes via the blockchain interface and the enterprise service bus.

The communication between the application and the blockchain go through the use of the enterprise service bus. It was chosen to create a modular architecture. With the introduced modularity the application and blockchain technology can be easily replaced.

Returning to the service bus, it receives all the messages and responses, it is the first node to be notified when a consensus is reached, and a transaction is successfully submitted. The enterprise service bus can then notify all the integrated systems. A last advantage is that a blockchain can now easily be used by multiple servers or even applications in general. Each system can easily integrate with the blockchain, because it is already up and running.

Finally, the certification authority group. This technology group is used to serve the authentication and registration component and used for the verification of medical specialists, who are trying to join the network. The integration between certification authority and the blockchain service is done via the Register of authorized medical specialists artifact, which is continuously being updated after the initial certification authoritie's data source was updated.

The presented artifact answers the **SQ5**.

4.4.4 Discussion

The evaluation will be based on the quality attributes distinguished by Neimi and Pekkola (Niemi & Pekkola, 2013). The high quality of the reference architecture is critical as it will be used as a blueprint in the new enterprise architectures. After the reference architecture was proposed that following quality attributes may be highlighted:

- Clarity and conciseness: The reference architecture gave a general and clear view of the environment and used a logical order of elements. The application layer of the blockchain could have been simplified a bit more, but this would have missed important details.
- Granularity: Following the previous point, the blockchain layer could be simplified, but then it would lack a sufficient level of detail.
- Uniformity and integrity: The architecture is built using Archimate standards, which are respected. In addition, a similar reference architecture has not existed before, and this architecture can be used to transform existing architectures into the architecture of the future.
- Correctness: This item is difficult to evaluate because such a thing has never been done before. Demonstration and evaluation of the architecture will show whether the architecture is complete and therefore correct.
- Usefulness: This point is fulfilled, the architecture can be used to design blockchain-based transactional systems.

Concluding, as the above-mentioned quality metrics are followed, it could be stated that the reference architecture is of high quality. The answer to the **SQ6** is given.

4.5 TO-BE model

To validate the reference architecture, the discussed scenario is being used to test the reference architecture. This is done by migration of the current architecture medical organisation to a target one. The framework to the migration is the developed reference architecture.

4.5.1 Migration

In order to perform the transition to a system based on the reference model presented earlier, it is necessary to perform those global steps that are presented in the migration expansion:

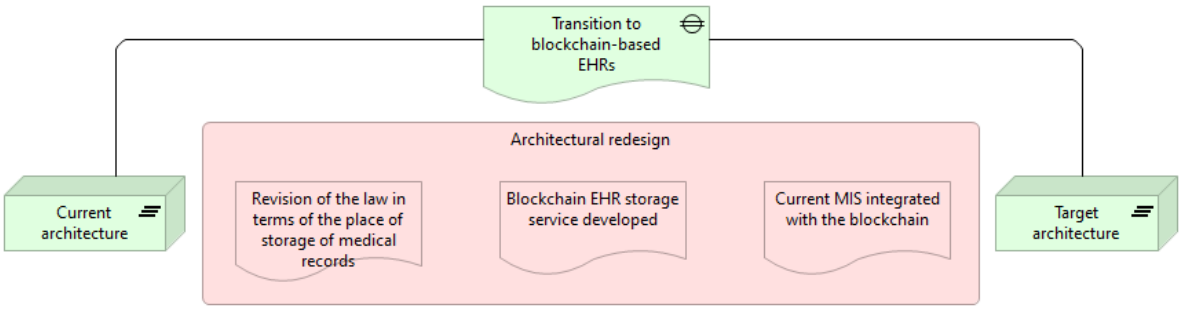

Figure 32 — Migration extension

The first step, which must be carried out is the revision of the legislation and the abolition of the compulsory affiliation of the EHR to the medical organization, where the treatment was initiated. Without passing this stage, the functioning of the system of EHRs, where the right to manage their data remains with the patient, remains unattainable.

After taking appropriate measures, the blockchain service itself needs to be developed according to the requirements discussed earlier in the paper. Once such a service is developed, integration of current medical systems with it will be required. The presented architecture provides a fairly high level of modularity, which will simplify integration.

4.5.2 Architecture

The target architecture after the transition to the blockchain base, built on the previously presented abstract model is presented in the following figure:

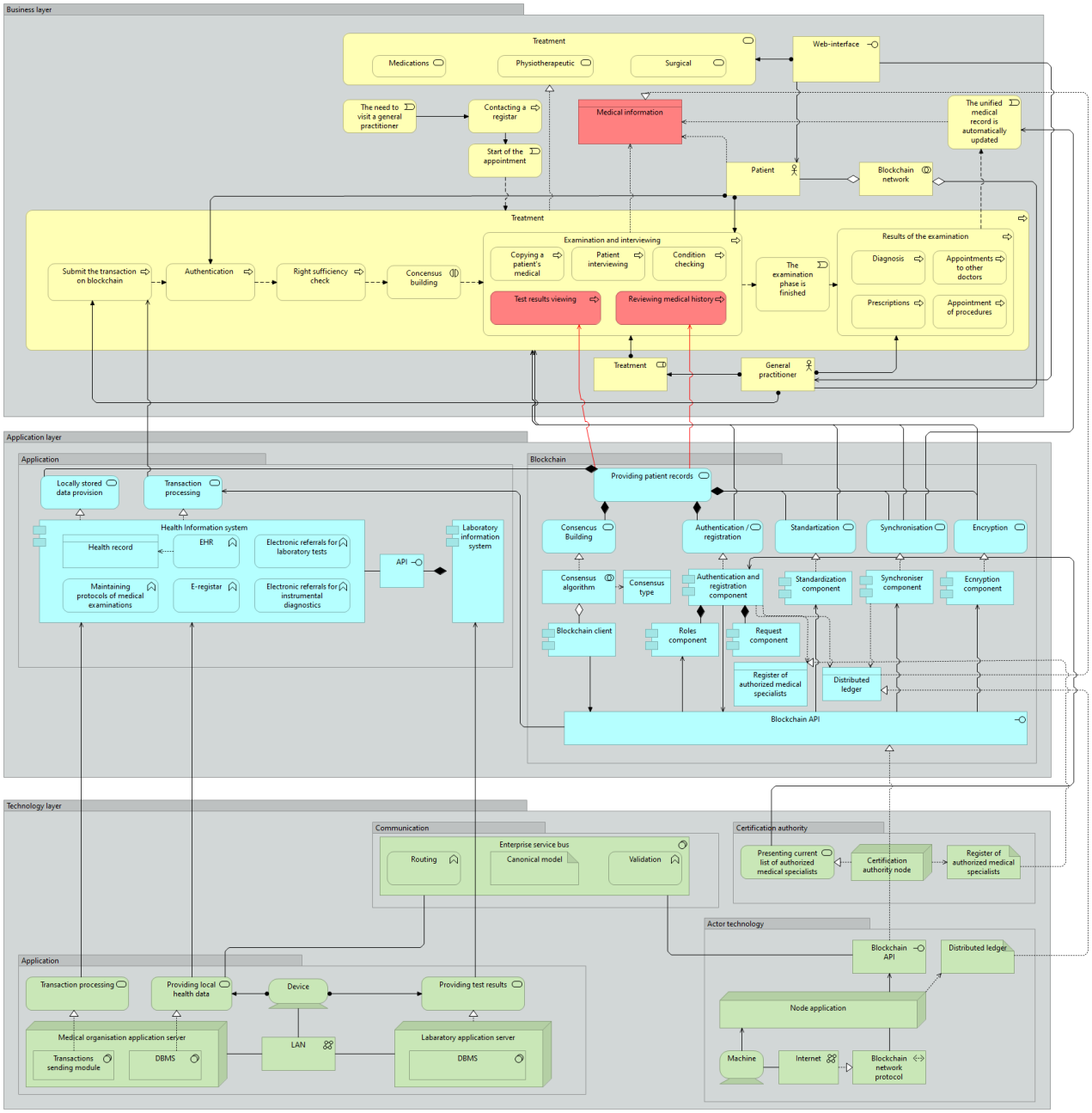

Figure 33 — TO-BE architecture

For the purposes of this section, the architecture will be examined in its entirety without any subdivision into layers, as it is built on the reference model, which, in turn, has been decomposed into layers.

As it could be seen in the diagram, the treatment business process now implies prior access to blockchain services to obtain patients' medical data. The doctor must receive confirmation from the patient in order for access to read the medical record to be granted.

After reading the data, as before, there is a transition from the examination process to the process of making a diagnosis, recommendations to tests, and general conclusions. However, once a new medical record is created, it is automatically saved to the blockchain rather than locally and the patient does not need to manually aggregate the information, so the user can access all the information immediately using a private key.

It is worth noting again that the fundamental change is the migration of the medical record service from local infrastructure to blockchain. Together with the service, the artifacts are moving as well - now the business artifact "Medical information" is implemented by the data object of the "Distributed ledger" on the application layer.

Speaking of the changes that will need to be made to the current information system, the only thing that will need to be added is methods of interaction with blockchain, i.e., the ability to send commands to blockchain via API and subsequently receive appropriate responses. This would require the implementation of transaction processing services at the application level as well as at the technology level.

4.5.3 Discussion

The migration of all the enterprise layers, using the reference architecture, result in a new enterprise architecture. The new enterprise architecture implies the presence of the current medical information system as one of the components of the system. The storage of EHRs is moved to the blockchain.

By doing this migration, the first step of phase E of the ADM and evaluation of the reference architecture are completed. In the case of the treatment the reference architecture can be used to migrate the current enterprise architecture to a new enterprise architecture. The next step of phase E and the evaluation is creating a prototype to “visualize” the value of the blockchain.

5 PROTOTYPE DEVELOPMENT

This chapter will describe a lightweight prototype built on blockchain to implement the 3-phase scenario presented earlier. The task set for the design and development of the prototype is to map the logic of a medical records system built on blockchain technology. Making reference to the built architectures, this section will propose an algorithm describing exactly how the user patient and doctor interact, i.e. describing the lower-level logic.

It is worth noting that the concept of the system does not cover all of the requirements identified earlier in the paper, but only some of them. Since in the scenario under consideration there are 2 stakeholders - the user and the doctor, respectively, the requirements that do not apply to these stakeholders will not be covered by the prototype functionality. In order to simplify the prototype, not all of the identified requirements for patients and doctors were covered.

First the approach to prototyping is presented, as well as the technology that was used. Finally, a description of the prototype is given.

5.1 Used technologies

Ledger

BigchainDB is a database that has some of the blockchain properties and database properties (*BigchainDB. The blockchain database.* 2021). BigchainDB is also often referred to as IPDB (InterPlanetary DataBase), the solution to all data warehouse problems.

Three properties are inherited from the blockchain:

1. Decentralization
2. Immutability: permanent data cannot be changed.
3. Creation and transmission of digital objects: manipulation of independent objects.

BigchainDB can store any type of data, but it is designed specifically to store registrations and asset transfers:

- Two types of transactions: a CREATE transaction and a TRANSFER transaction.
- A CREATE transaction registers any kind of assets
- A TRANSFER translation is transferring the created asset from one user to another

File storage

The current iteration of the Internet is not decentralized as it is based on some outdated protocols. The problems addressed by IPFS are related to problems with the current HTTP protocol of the Internet (*IPFS Powers the Distributed Web* 2019). IPFS is a distributed file system technology based on DHT (Distributed Hash Table) and BitTorrent. It allows file systems on different devices to be interconnected at the same time, using content forwarding. Unlike HTTP, where the content is addressed by its precise address (URI), the IPFS accesses the content by its hash. Integration of IPFS in the blockchain-based architecture makes sense as immutable persistent links may be placed in blockchain.

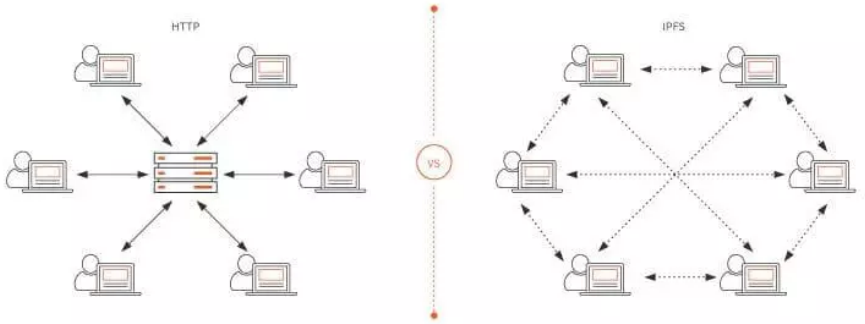

Figure 34 — HTTP and IPFS comparison

Programming language

The programming language used to write the prototype is Python. This language was selected due to its flexibility. Although Python is among one of the most popular languages it has an interpretative nature, which implies weaker performance, therefore, for the real solution to be able to process vast quantities of data and transactions it is recommended to choose the compiling language such as GoLang, C or C++.

Interface

In order to simplify the developing proof-of-concept the selected interface is chosen to be a CLI (command line interface). The command handlers are written on the python framework for the CLI application development called click.

5.2 Operations logic

The description of the prototype in this section will take the form of storytelling. Key points will be commented on and supported by appropriate screenshots.

As in the script, there will be three users within the prototype. Since the CLI was chosen as the interface, the background color of the interface for each of the users will be different for a more visually comprehensible display. For the purposes of this work, gray is the patient, black is Dr. 1, and blue is Dr. 2.

The first step that has to be done is the declaration of the identity and the public key. Every user does it. The following command allows the user to be created:

```
(MBC) godlin@DESKTOP-2VLSJ5D:~/patient$ MBC createuser
Name of patient: patient
Phone number: patient
[+] Writing Name and Phone
[+] Generating BigChainDB keypair
[+] Generating RSA keypair
[+] Serializing to JSON
Writing private key data to a json file. Please be sure to save it s
ecurely. You will need it to log in later.
Press any key to continue ...
[+] Writing file to disk as: user.json
```

Figure 35 — Creation of the user

For the sake of simplicity the name of the user and the phone number (the identifier that will be used by the doctors to allocate the patients) will be the same as the role - *patient*. Same approach is used during the creation of the doctors accounts. As could be seen after the creation of a user the access data was generated and saved to the distinct file. The content of the file are presented on the following figure:

Figure 36 — User information

Each user will have a public and the corresponding private keys. This file may be used as an access key on different devices, even on the RFID card. Next one is login. After the creation of the keypair, the user may login to the system with the following command:

Figure 37 — User login

As could be seen, the user has successfully logged, but not yet registered to in the blockchain (bigchainDB) - the corresponding message is present and zero blocks. The following step is the registration of the user on the blockchain. The user may be registered to the blockchain with the following command:

```
(MBC) godlin@DESKTOP-2VLSJ5D:~/patient$ MBC register
[+] Serializing to JSON
[+] Preparing CREATE transaction with {'schema':...
[+] Signing with private key
[+] send_syncing to the Blockchain
[+] Sent transaction {'asset': {'data': {'bigchain': '7wykKg7u6EnH9mCty
EYTCpeuoc4q5AuL1v4AuJF2yisu', 'name': 'patient', 'phone': 'patient', 'r
sa': '-----BEGIN PUBLIC KEY-----\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg
QC0tBkc3H2QANZj9XIeymjxpSxn\nEXQEQ2czenSFuNf3YX74qACHwFsWbbR8yEqeyLmcAC
fJmGekSOsOF7gVzaHyoPXY\nE8RUGiZ5fmcnhsOnmjziecnGAXvsd6219ECRiR4WkoYl5w6
Myrs8cgShHOm2z/dL\nO+S9OUiL9W0u2ScyJQIDAQAB\n-----END PUBLIC KEY-----',
 'schema': 'MBC.user', 'version': 'v0.01'}}, 'id': 'fe49cd334128ca3bd13
e2e0c504753c711957a624da5d138dbe5b7082f68395b', 'inputs': [{'fulfillmen
t': 'pGSAIGc7pjJwO5ox5pLNN9f6ZMh2MCDKureJ3K2xBEz0_qIcgUBqviZ5YfMRpxe-mN
GhaLr-kwSrDN8TYLTzWp0f5R-23KuKrzfIJ1K2i1b1A-N2NTnxzPyftnCU975VLt3MYnkE'
, 'fulfills': None, 'owners_before': ['7wykKg7u6EnH9mCtyEYTCpeuoc4q5AuL
1v4AuJF2yisu']}], 'metadata': None, 'operation': 'CREATE', 'outputs': [
{'amount': '1', 'condition': {'details': {'public_key': '7wykKg7u6EnH9m
CtyEYTCpeuoc4q5AuL1v4AuJF2yisu', 'type': 'ed25519-sha-256'}, 'uri': 'ni
:///sha-256;SJjeKp-ERIGpH-hX-StLf3SX-YEpeXw33cqBY0qrxF4?fpt=ed25519-sha
-256&cost=131072'}, 'public_keys': ['7wykKg7u6EnH9mCtyEYTCpeuoc4q5AuL1v
4AuJF2yisu']}], 'version': '2.0'}
```

Figure 38 — User registration in blockchain

After the user was registered, when executing the login command again the registered status will be changed to registered in the blockchain - the blocks now are able to be added to the user.

```
Registered on the Blockchain!
Blocks: 0
```

Figure 39 — Number of the owned blocks

The patient came to the doctor 1. The doctor 1 is performing an examination and after it is done, the report is documented. By the end of the treatment the doctor has two files - .txt file with the report and .jpeg image (extension does not matter). The sample files are presented on the following figure:

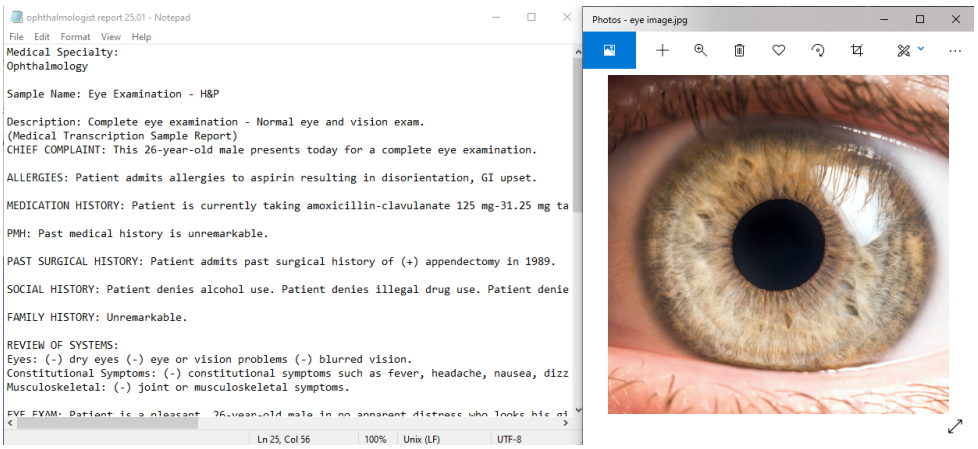

Figure 40 — Sample files to be sent to blockchain

Now the doctor 1 has to apply the obtained documents to the patient's electronic health record. It is done with the following command:

```
(MBC) godlin@DESKTOP-2VLSJ5D:~/doctor 1$ MBC add --phone patient eye\ ima
ge.jpg
[+] Fetching user data from the blockchain
[o] Got more than one record for the same version. Last registery will be
 taken
[+] Got Public RSA key
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzQYLZf4a0E4S45r5UTJOnwDiN
BRGEnYBnuFTNzz4FZf3IkcqlwSJ2o6c1QaR5OpWSFHLPb6nXYHxNIOuWPNjmRtRU
CpBzB7dsX9eOOBZ9nBWVcqvO0C8MJhJdL8c9vCQDkZJUTi28hfr6JuLK7YqEuDjR
7py8CHUY9emE/inZVQIDAQAB
-----END PUBLIC KEY-----
[+] Generating random AES key
[+] Encrypting data...
[+] Writing encrypted data to IPFS
[+] Connected to local IPFS node
[+] Data written to IPFS: QmNuUgkoMrugkvpPBAiRUW99masfpTNWk8Jc3M9gz2yF2G[
+] Encrypting AES key with RSA public key
[+] Preparing CREATE transaction with {'schema':...
[+] Signing with private key
[+] Creating Block on the Blockchain
[+] Created: 670b7709ce3cc662d9d7058800de2c145fc2f12f5be41b18625c63517b7e
2f3e
[+] Transfering Block to patient: 3awboX1G4vsh43RV7b4zLKKsJzCMYpYm5uSxNgB
SodUv
[+] Preparing TRANSFER transaction with encrypted key
[+] Signing transaction
[o] Waiting for the asset block to confirm on blockchain. Sleeping for 0.
5...
[o] Waiting for the asset block to confirm on blockchain. Sleeping for 0.
5...
[+] Asset block confirmed on the blockchain: 66119
[+] send_syncing on the blockchain
[+] Transaction sent: 69430ad3cf1b9dc52ef66136244247c2c189bff00fb37c1cc9c
f3617d23ade97
```

Figure 41 — File sent to blockchain

The steps on the image are speaking for themselves. Two identifiers appear on this step - the id of the block and the hash of the file that was saved to IPFS. In the current version of the prototype each block contains one file. Logging back by the patient and listing the

assigned blocks, two blocks are displayed that means that the files were successfully saved in the blockchain:

```
(MBC) godlin@DESKTOP-2VLSJ5D:~/patient$ MBC list
[o] No address or phone number provided. Loading current logged in user
-----------------------------------Block 1-------------------------------
-----
ID: 6a79e3cc8e2c91c9d38876cfc02a42bdb07a997ee9aa6cb311095e4ba9952692
IPFS hash: QmRrwc4Tx4NMSpMzKzfWq12VH3rnKdhuiCsh79VVP3UhNy
File Format: txt
Permitted addresses: 1
Current user can decrypt
-------------------------------------------------------------------------
--------
-----------------------------------Block 2-------------------------------
-----
ID: 670b7709ce3cc662d9d7058800de2c145fc2f12f5be41b18625c63517b7e2f3e
IPFS hash: QmNuUgkoMrugkvpPBAiRUW99masfpTNWk8Jc3M9gz2yF2G
File Format: jpg
Permitted addresses: 1
Current user can decrypt
-------------------------------------------------------------------------
--------
```

Figure 42 — List of patient's blocks

Earlier in the thesis the concept of asymmetric cryptography algorithm was introduced. Signing the block with another user's public key, the only user, who will be able to decrypt the information will be the user, who has the corresponding private key - the patient in this case. That is, the corresponding decryption possibility message is displayed. When logging back to the doctor and trying to list the patient's transaction, the message about impossibility of decryption is displayed:

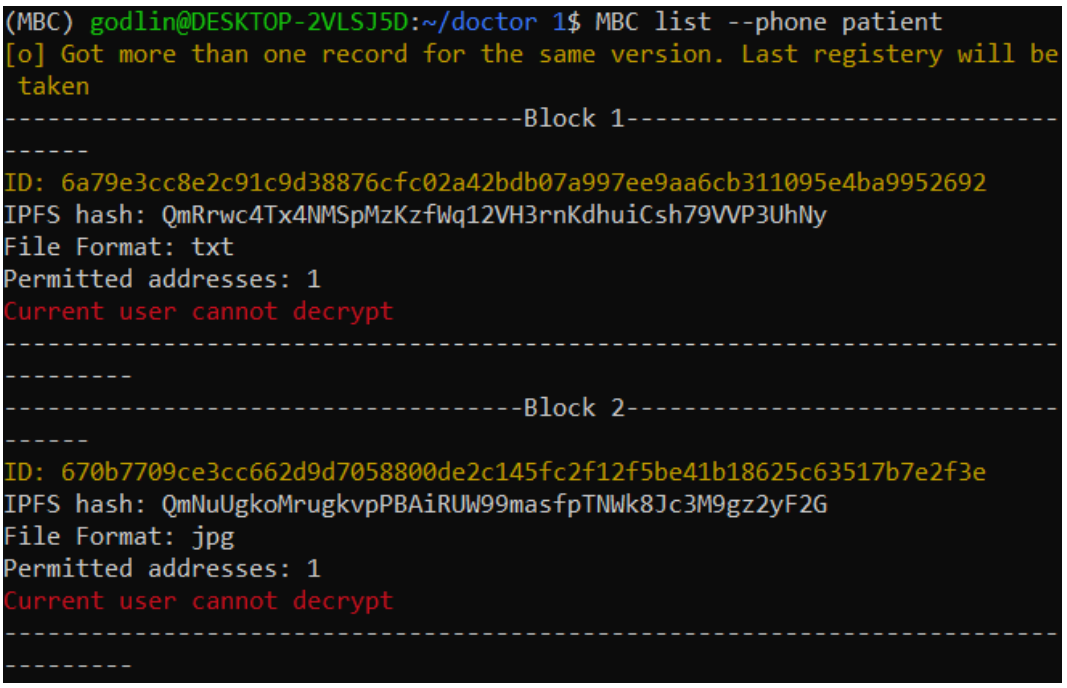

Figure 43 — The restriction to the decryption by doctor 1

As it could be seen, the data is available to be spotted for every user of the network. Even though the ids of user's blocks and the corresponding IPFS file hashes are known, the users without the private key will not be able to decrypt them. The following message appears, when the user without the permissions to view is trying to get the uploaded file:

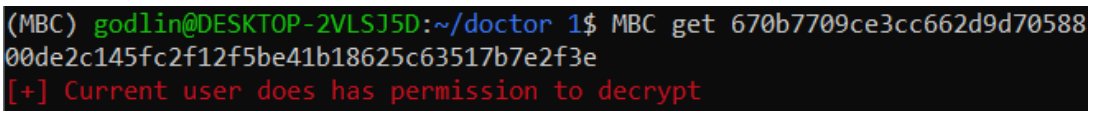

Figure 44 — Attempt to decrypt the file without the appropriate private key

When trying to download the file with the known ID directly from the IPFS, it would be obfuscated - the following image presents, how earlier created .txt file is stored in the IPFS:

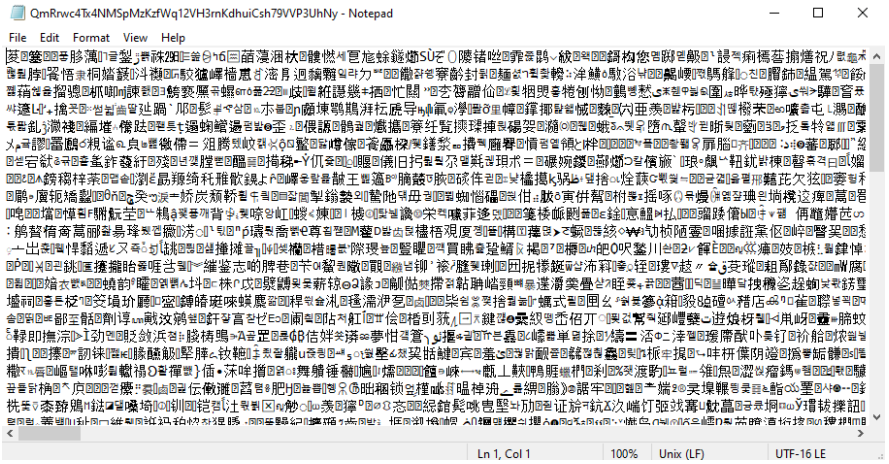

Figure 45 — Encrypted file downloaded directly from the IPFS

When trying to download the file logged as a patient (the owner of a relevant private key), the block may be downloaded:

```
(MBC) godlin@DESKTOP-2VLSJ5D:~/patient$ MBC get 6a79e3cc8e2c91c9d38876cfc0
2a42bdb07a997ee9aa6cb311095e4ba9952692
[+] Current user has permission to decrypt
[+] Decrypting AES key
[+] Retrtriving file from IPFS
[+] Connected to local IPFS node
[+] Decrypting file
[+] File decrypted
Length: 2943
...Head display...
Medical Specialty:
Ophthalmology

Sample Name: Eye Examination - H&P

Description: Complete eye examination - Normal eye and vision exam.
(Medical Transcription Sample Report)
CHIEF COMPLAINT: This 26-year-old male presents today for a complete eye e
xamination.

ALLERGIES: Patient admits allergies to aspirin resulting in disorientation
, GI upset.

MEDICATION HISTORY: Patient is currently taking amoxicillin-clavulanate 12
5 mg-31.25 mg tablet, chewable medication was prescribed by A. General Pra
ctitioner MD, Adrenocot 0.5 mg tablet medication was prescribed by A. Gene
ral Practitioner MD, Vioxx 1

[+] Writing to 6a79e3cc8e2c91c9d38876cfc02a42bdb07a997ee9aa6cb311095e4ba99
52692.txt
[+] Done!
```

Figure 46 — Downloaded files by the patient

The file that was initially added by the doctor is now saved on the patient computer.

Now the patient appeared in another medical organisation and is about to have an appointment with a new doctor - doctor 2. Doctor 2 does not have the access to the patient's previous medical records:

```
(MBC) godlin@DESKTOP-2VLSJ5D:~/doctor 2$ MBC list --phone patient
[o] Got more than one record for the same version. Last registery will be taken
----------------------------------Block 1-----------------------------------
ID: 6a79e3cc8e2c91c9d38876cfc02a42bdb07a997ee9aa6cb311095e4ba9952692
IPFS hash: QmRrwc4Tx4NMSpMzKzfWq12VH3rnKdhuiCsh79VVP3UhNy
File Format: txt
Permitted addresses: 1
Current user cannot decrypt
------------------------------------------------------------------------------
--
----------------------------------Block 2-----------------------------------
ID: 670b7709ce3cc662d9d7058800de2c145fc2f12f5be41b18625c63517b7e2f3e
IPFS hash: QmNuUgkoMrugkvpPBAiRUW99masfpTNWk8Jc3M9gz2yF2G
File Format: jpg
Permitted addresses: 1
Current user cannot decrypt
------------------------------------------------------------------------------
--
```

Figure 47 — The restriction to the decryption by doctor 2

Therefore, in order for a doctor 2 to view the record, the corresponding access has to be given by the patient:

```
(MBC) godlin@DESKTOP-2VLSJ5D:~/patient$ MBC permit --phone doctor2 6a79e3c
c8e2c91c9d38876cfc02a42bdb07a997ee9aa6cb311095e4ba9952692
[+] Found user with mobile number!
[+] Got Public RSA key
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDNMRJjzsjhKv1e/CWu3CetWG3n
81Dj3FOf85B/gPP9Pn96qUi5zuIcJW0FtrVRJXkogAxNMyU6g2TUFGLfseU8+54F
Za/oTh7bRHH71tFX4b3hmU7yfyJXyEdbzojhVV1AzzvrimtiUM01DHF2e16aRYG0
xhe0rF8sMnebaciG2wIDAQAB
-----END PUBLIC KEY-----
[+] Decrypting AES key using private key
[+] Decrypted : b',\xd5>\x17C)UL\x03\xc9\xf2\n1\xa7\xd6\xc4\x04\xee\xac\xb
f@\xc9\x1e\x0f\xd15\xaf\xc7m\xde\xab\xf9'
Press any key to continue ...
[+] Encrypting AES key with RSA public key
[+] Transfering Block to patient: 3awboX1G4vsh43RV7b4zLKKsJzCMYpYm5uSxNgBS
odUv
[+] Preparing TRANSFER transaction with encrypted key
[+] Signing transaction
[+] Asset block confirmed on the blockchain: 66107
[+] send_syncing on the blockchain
[+] Transaction sent: 0508cafbbda5ab6d19c565f782db2c8255e12b0c041024e9ebfd
2f26fd0f3d93
```

Figure 48 — Giving permission to doctor 2 to decrypt the block with certain id

The user permitted the access to one the blocks to a doctor 2. Now doctor 2 is able to decrypt the file in the block:

Figure 49 — Possibility of the block decryption after corresponding access rights given

At any time the patient is able to restrict access to this user.

The developed solution covered the main requirements that were identified during the literary analysis phase. The goal of the developed prototype is to prove the workability of the concept and propose the implementation as a framework for the design of a blockchain service, which was presented in the framework of the reference architecture.

5.3 Discussion

The prototype shows how the basic requirements of the patient and physician system are covered in the case study. Prototype helped to verify that the implementation of the part of the reference architecture is possible. The answer to the **SQ6** is given.

However, the prototype implies certain limitations. First, the logic of not all the modules listed was reflected within the prototype, but only the basic logic covering the scenario under discussion. Second, testing under heavy loads is necessarily required, as a large number of users in the system is implied. Finally, the big limitation to this prototype is the fact that a blockchain network deployed, but the network only had one node.

6 CONCLUSIONS

The section consists of two parts. The first will assess the potential impact of the developed system. The first will look at the impact within the considered process of the organization. This is followed by a final remark. The reflections within this section respond to **SQ7**.

6.1 Implementation impact

The introduction of a blockchain-based electronic health record system can bring significant qualitative improvements for key stakeholders and society as a whole. To begin with, the potential effect on primary stakeholders will be examined. This will be based on the process for which the architecture was previously modeled.

A comparatively recent study was carried out to examine the distribution of working time at the outpatient appointment of a general practitioner in a polyclinic in the city of Moscow (Vechorko, 2016). The results of the analysis of the distribution of working time based on a phototimer survey of the general practitioner at the outpatient consultation indicate irrational use of time for intermediary contact with a patient in connection with the large amount of work performed with the documentation. The therapist spends *46.84%* of his time collecting anamnesis and interviewing the patient as part of his main activity in the office. This is due to the lack of integrity of medical information - the doctor needs to review the patient's records in a "raw" (not aggregated) form in order to form a picture of the state of health.

With a unified medical record with structured information storage, the doctor can immediately get a complete picture of the patient's condition in a human-readable form. This can include automatically generated graphs, conclusions and even predictions for further development of the condition from the current one. This can significantly reduce the time spent on the history of one patient, bringing it closer to about 1 minute or less in trivial cases.

In addition to providing support for making important medical decisions, the developed system on the blockchain architecture will also allow for statistical monitoring of the operational activities of medical organizations. The analysis of statistical data, evaluation of events within medical organizations and relevant conclusions allow to make correct

management decisions and consequently contribute to the improvement of operational activities. Collected data within the medical system allows conducting sample statistical surveys to solve problems at different levels of the health care system.

In addition, the availability of primary information and the availability of tools for its consolidation and analysis will significantly simplify and reduce the staff-organizational structure of medical statistics. Based on the data available in the system, the indicators characterizing the work of each medical institution can be evaluated. For example: staffing levels of doctors, nurses, and junior medical personnel, state of material and technical basis and availability of medical property, compliance of organizational and staff structure of subdivisions with the volume and nature of tasks to be performed, general state of patient health, morbidity, hospitalization, loss of labor, mortality, dispensary work, efficiency of treatment and rehabilitation activities, therapeutic and diagnostic work, etc. Thus the information accumulated in the system will reveal dynamics (positive or negative) of indicators and the reasons for their change as a result of the analysis.

The available in blockchain information from each medical institution will allow to adequately compare patient diagnoses made at the time of referral for hospitalization with the diagnoses established in the hospital, as well as clinical (lifetime) and pathologic anatomic diagnosis, based on which a conclusion can be made about the defects of treatment work (brief observation of the patient, incompleteness and inaccuracy of examination, underestimation and overestimation of anamnestic data, lack of necessary hardware and laboratory tests, the absence, underestimation or overestimation of the consultant's opinion) and organizational defects in the work of polyclinics and hospitals (late hospitalization of a patient, understaffing of medical and nursing personnel of medical and diagnostic departments, shortcomings in the work of individual hospital services (admission department, diagnostic rooms, etc.), improper and negligent staffing. In this case, it may turn out that the correct final diagnosis is only the last stage of many incorrect, mutually exclusive diagnostic assumptions of the doctor during the entire period of observation of the patient.

6.2 Summary

Master thesis is made on a currently relevant topic, as it affects the most important area having a direct relation to the quality of human life - healthcare. This work considers the possibilities of applying blockchain technology in healthcare. In the paper several feasible applications of the technology in healthcare are analyzed, but ultimately the main focus is

on the implementation of electronic medical records, suggesting that this is the most critical area, as it affects a wide range of stakeholders - from patients and doctors themselves to research centers. In terms of the storage and management of electronic health records, the healthcare industry has long needed to innovate and there is now enough track record of integrating blockchain technology for the healthcare industry to lead the transformation.

The thesis begins by outlining that one of the key problems the healthcare industry currently faces is the lack of a unified patient medical record. The corresponding problem is highlighted because of the highest frequency of its potential occurrence in various scenarios, as well as the potential damage to both the patient and other participants in the scenario. Then, the current typical organization of the information components of medical organizations are being discussed, pointing out the local storage of fragments of medical records in various organizations, and reflecting on why the corresponding architecture was initially built in the first place. After pointing out the problem of medical data fragmentation, the paper reflects on potential problems - security, privacy, and lack of infrastructure for aggregating medical data between organizations being the most key.

The paper hypothesizes that blockchain technology has potential in the implementation of electronic health records. The research question and the corresponding sub-questions are posed. Design science research method is chosen as a research methodology, describing the preferences for choosing this particular methodology. Since the methodology process involves sequential processes, according to each process the corresponding content in the subsequent parts of the paper is presented. In such a way the paper allows the reader to relate the scientific approach to the content of the paper.

In order to build the reader's understanding of the technology itself, it is briefly described. Definitions have been given, the main characteristics, types, working mechanisms have been described, and the main difficulties of blockchain projects implementation, which are faced by developers, have been given. The final part of this chapter is a breakdown of blockchain applications in healthcare. Three main directions are given. In this way, the thesis implies the multidirectionality of potential implementation.

In the next chapter, a systematic analysis of current proposed solutions is conducted. As sources of information, scientific articles and real-world projects with descriptions on the Internet are being usd. The purpose of the analysis is to form the potential stakeholders of

the system in order to identify the requirements. Regarding the potential goals of using the stakeholder system, a list of requirements is clearly formed. For relevant requirements, the implementation on blockchain is based and potential problems of alternative implementations are highlighted.

The goal of the next chapter was to present a reference model of a medical organization architecture based on storing patient medical records in blockchain. One of the most popular patient-doctor interaction scenarios is taken as a business process. For the process in question,an architectural approach is used to demonstrate problems in the current architecture of a typical medical organization information solution, proposes a reference architecture model based on the requirements formed earlier, and cites the advantages of implementing an architecture based on the reference model. Further, the migration steps of the necessary steps for transition from the current architecture to the target architecture, which is based on the reference model are highlighted. At the end of the chapter, the thesis demonstrates the target enterprise architecture.

The next stage of the thesis was the development of the prototype. The purpose of this stage was to give the reader a visual representation of the logic of patient-doctor interaction in the scenario under consideration, given in the earlier chapters of the work. In the manner of storytelling, the theis visually and clearly describes the sequence of actions of each of the users, pointing out the peculiarities of the technical implementation in the prototype and attaching the corresponding screenshots.

The final chapter of the main part of the paper is a justification of the efficiency of transition of medical organizations to the system of electronic medical records based on blockchain. The effectiveness of implementation both in terms of process optimization for the organization, and more global effects is considered.

All sub-questions were answered as part of the work. Answers to them were required for the completeness of the answer to the main research question. Thus, the study can be considered successful.

6.3 Final remarks

Blockchain technology provides a distributed medical data storage framework. Ownership of the personal data remains with the patients who have the access to the EHRs and give the corresponding permissions to the healthcare providers on request. A blockchain

network provides continuous data availability as it does not have the single point of failure, which centralised systems have. Finally, as well as all centralized systems the service built on top of blockchain technology provides the integration possibilities with the current IT solutions that are used by the medical organisations.

Nowadays, blockchain technology is tried to be "pulled" into everything and its importance is often exaggerated. Technology experts and the experts from the domain warn against excessive use of the technology in healthcare and remind of the problems that may arise if blockchain is actively used in the healthcare market.

Overall, blockchain provides the basis for a qualitative leap in healthcare. The use of blockchain to store medical records will make the transition to personalized medicine possible. With this transition, it will become much easier to analyze the quality of care provided by medical organizations and, most importantly, to form an optimal and more accurate treatment plan. In this way, technology can make a significant difference in the quality of life.

REFERENCES

1. *Survey of the Russian commercial healthcare market*. (n.d.). https://assets.ey.com/content/dam/ey-sites/ey-com/ru_ru/topics/health/healthcare-research-2018-2019-eng-ey.pdf.

2. Kobyakova O.S. and others. STANDARDIZATION OF MEDICAL CARE - LEAN PRODUCTION TOOL AS THE BASIS FOR SYSTEM IMPROVEMENTS // Social Aspects of Population Health. 2020. Т. 66. № 3. С. 2–2.

3. Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

4. Kamoun, F., & Nicho, M. (2014). Human and Organizational Factors of Healthcare Data Breaches. *International Journal of Healthcare Information Systems and Informatics*, *9*(1), 42–60. https://doi.org/10.4018/ijhisi.2014010103

5. Epalm. (2021, April 7). *HIMSS Annual European Digital Health Survey*. HIMSS. https://www.himss.org/resources/himss-annual-european-digital-health-survey.

6. Bevan, N., & Curson, I. (1997). Planning and Implementing User-Centred Design Using ISO 13407. *Human-Computer Interaction INTERACT '97*, 657–658. https://doi.org/10.1007/978-0-387-35175-9_119

7. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/mis0742-1222240302

8. *Bitcoin: A Peer-to-Peer Electronic Cash System*. (2009). https://bitcoin.org/bitcoin.pdf.

9. Baran, P. (1962). *On Distributed Communications Networks*. Defense Technical Information Center.

10. van Steen, M., & Tanenbaum, A. S. (2016). A brief introduction to distributed systems. *Computing*, *98*(10), 967–1009. https://doi.org/10.1007/s00607-016-0508-7

11. Vergne, J. P. (2020). Decentralized vs. Distributed Organization: Blockchain, Machine Learning and the Future of the Digital Platform. *Organization Theory*, *1*(4), 263178772097705. https://doi.org/10.1177/2631787720977052

12. Laurence T. Blockchain. Hoboken, NJ: For Dummies, a Wiley brand, 2019.

13. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2018). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, *22*(S6), 14743–14757. https://doi.org/10.1007/s10586-018-2387-5

14. Chowdhury, N. (2020). *Inside blockchain, Bitcoin, and cryptocurrencies*. CRC Press, Taylor & Francis Group.

15. Battah, A., Iraqi, Y., & Damiani, E. (2021). Blockchain-Based Reputation Systems: Implementation Challenges and Mitigation. *Electronics*, *10*(3), 289. https://doi.org/10.3390/electronics10030289

16. Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital Supply Chain Transformation toward Blockchain Integration. *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*. https://doi.org/10.24251/hicss.2017.506

17. Chatterjee, P. (2010). India combats confusion over counterfeit drugs. *The Lancet*, *375*(9714), 542. https://doi.org/10.1016/s0140-6736(10)60214-0

18. DavaIndia. (2020). https://www.davaindia.com/.

19. Raikwar, M., Mazumdar, S., Ruj, S., Sen Gupta, S., Chattopadhyay, A., & Lam, K.-Y. (2018). A Blockchain Framework for Insurance Processes. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. https://doi.org/10.1109/ntms.2018.8328731

20. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*. https://doi.org/10.1109/obd.2016.11

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

22. Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., Jahangir, M. M., Chowdhry, K., Lachhani, R., Idnani, N., Schumacher, M., Aberer, K., Stoller, S. D., Ryu, S., & Wang, F. (2019). ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care (Preprint). https://doi.org/10.2196/preprints.13598

23. Yang, Y., Li, X., Qamar, N., Liu, P., Ke, W., Shen, B., & Liu, Z. (2018). Medshare: A Novel Hybrid Cloud for Medical Resource Sharing Among Autonomous Healthcare Providers. *IEEE Access*, *6*, 46949–46961. https://doi.org/10.1109/access.2018.2865535

24. Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *Journal of Medical Systems*, *43*(1). https://doi.org/10.1007/s10916-018-1121-4

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

26. Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. (2018). BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. *2018 IEEE Globecom Workshops (GC Wkshps)*. https://doi.org/10.1109/glocomw.2018.8644088

27. *Estonia - We have built a digital society and we can show you how*. e. (2021, February 25). https://e-estonia.com/.

28. Open Longevity. (n.d.). https://openlongevity.org/.

29. Medicalchain. (2016). https://medicalchain.com/.

30. *Research Foundry: blockchain based healthcare data solutions*. BurstIQ. (2021, May 25). https://www.burstiq.com/.

31. blockchainhealth.co. (2017). https://blockchainhealth.co/.

32. Healthcare API Platform. URL: https://pokitdok.com/ (date of access: 07.05.2021).

33. Florence HudsonSpecial Advisor for Next Generation Internet, Hudson, F., Special Advisor for Next Generation Internet, Forbes, & Today, B. in H. (n.d.). *HealthChain - Blockchain For Medical Devices*. HealthChain Blockchain Project. https://healthchain.io/.

34. Ghadamyari, M., & Samet, S. (2020). Decentralized Electronic Health Records (DEHR): A Privacy-preserving Consortium Blockchain Model for Managing Electronic Health Records. *Proceedings of the 6th International Conference on Information and Communication Technologies for Ageing Well and e-Health*. https://doi.org/10.5220/0009398101990204

35. IRYO.NETWORK. (2021). https://iryo.network/.

36. Carex. (2021). https://carex.com/.

37. *Patientory - Healthcare platform for healthcare providers and consumers*. Patientory Inc. (n.d.). https://patientory.com/.

38. *Health Level Seven International*. Health Level Seven International - Homepage. (2021). http://www.hl7.org/.

39. Choque, L., & Bayona-Ore, S. (2020). Entreprise Architecture: Critical Factors and Implementation. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. https://doi.org/10.23919/cisti49556.2020.9141169

40. Desfray, P., & Raymond, G. (2014). TOGAF®. *Modeling Enterprise Architecture with TOGAF*, 1–24. https://doi.org/10.1016/b978-0-12-419984-2.00001-x

41. Syynimaa, N. (2018, November 13). *Essence : Reference Architecture for Software Engineering - Representing Essence in Archimate Notation*. JYX. https://jyx.jyu.fi/handle/123456789/60344.

42. Bean, J. (2010). *Soa and Web services interface design: principles, techniques, and standards*. Morgan Kaufmann/Elsevier.

43. ISO/IEC Standard for Systems and Software Engineering - Recommended Practice for Architectural Description of Software-Intensive Systems. (n.d.). https://doi.org/10.1109/ieeestd.2007.386501

44. ArchiMate® 3.1 Specification. (2021). https://pubs.opengroup.org/architecture/archimate3-doc/.

45. Niemi, E., & Pekkola, S. (2013). Enterprise Architecture Quality Attributes: A Case Study. *2013 46th Hawaii International Conference on System Sciences*. https://doi.org/10.1109/hicss.2013.201

46. *BigchainDB. The blockchain database.* (2021). https://www.bigchaindb.com/.

47. Labs, P. (2019). *IPFS Powers the Distributed Web*. IPFS. https://ipfs.io/.

48. Vechorko, V. I. (2016). DISTRIBUTION OF WORKING HOURS OF PRIMARY CARE PHYSICIAN WITH A NURSE AT A MOSCOW POLYCLINIC (PHOTO and time study). *Social Aspects of Population Health*, *52*(6), 4. https://doi.org/10.21045/2071-5021-2016-52-6-4