Blockchain technology in healthcare systems

CAS Big Data and Machine Learning
16.06.2019

by Lukas Studer

Supervisor:
Bruno Bastos Rodrigues
University of Zurich, Department of Informatics – Communication Systems Group

University of Zurich[UZH]

Content

Abstract

Over recent years, the development in healthcare has become one of the central topics on governments' agendas. Constantly growing costs, a lack of transparency, misguided incentives and counterfeit medicines are just some of the challenges that must be dealt with in order to guarantee a sustainable future healthcare system. Blockchain technology has the potential to develop suitable solutions for many of these challenges. In recent years, an increasing number of blockchain-based solutions have been developed and implemented in the healthcare sector. Interoperability in the system currently trends towards blockchain data silos and this creates a major challenge which must be dealt with. Beside the technological challenges, modern healthcare systems also need reforms to ensure the necessary systematic basis to best utilise new technologies and ensure the ability to adapt to on-going changes.

Keywords: Healthcare, drug, Blockchain, clouds, big data

1. Introduction

The healthcare industry has become one of the largest industries among developed countries in recent decades and, nowadays, accounts for 10% of gross domestic product [1]. This has led to more and more individual healthcare spending and healthcare costs rising in general, [2] which creates sustainability problems within the system. Reforms and changes of current structures are needed. One reason for this development is the technological progress, which lifted the way of treating diseases to a new level. By using, for example, the "Clustered Regularly Interspaced Short Palindromic Repeats" (CRISPR) technology, genomes can be encoded and modified much faster and more easily [3]. Not only new genomic information but also data coming from devices from the internet of things in combination with powerful algorithms, allows us to predict and treat diseases individually in a way that was not possible in earlier days. However, those applications are only possible if appropriate, trusted data is available. In healthcare, unfortunately, data is currently spread among different stakeholders or private companies and can therefore often be hard to access[4]. Thus, not only are reforms required, but an entire reshape of the current healthcare environment, including data collection and regulations, to ensure a sustainable system offering efficient and high-quality treatments.

A possible tech solution to catalyse this evolution could be blockchain. Almost ten years ago, it was originally developed as an electronic peer-to-peer cash system known as Bitcoin [5]. However, for experts it was quite obvious that blockchain, with its immutable, decentralized architecture, had more applications than just acting as a cryptocurrency [6]. The perception of blockchain has also changed in society within the last ten years, from an internet currency to an alternative technology with advantages that can be implemented into the industry [6].

On the one hand, there is an eco-social construct, the healthcare system, which urgently needs to evolve to deal with the latest health trends and the digital world. On the other hand, a rather new technology with big potential, which is permanently looking for new, appropriate application fields. There are indeed some promising aspects of blockchain identifying it as the ideal technology to deal with today's healthcare challenges. However, different concerns on a technological, regulatory but also socio-economic level should be evaluated in the implementation.

This thesis provides an overview of the challenges in the healthcare sector, introduces the Blockchain technology and its characteristics and provides an overview about applications of Blockchain in the healthcare sector. In Chapter 2, basic information about blockchain technology is provided: how it works, how it developed within the last ten years and the different types of chains with their characteristics. Afterwards, an introduction of the healthcare industry and its challenges is shown in Chapter 3 to evaluate the possible value of blockchain technology in the healthcare sector. Different successfully implemented use cases are shown and possible new use cases in precision medicine evaluated. Finally, the potential and challenges of blockchain in healthcare is evaluated in Chapter 4 from a technical and socio-economical point of view, concluding with a short outlook provided in Chapter 5.

2. Blockchain

2.1 What is a Blockchain?

In spring 2008, a whitepaper with the title "Bitcoin: A Peer-to-Peer Electronic cash system" was published under the pseudonym Satoshi Nakamoto [5]. The pioneering idea was to have a peer-to-peer system, in which you can do online payments without a financial institution being involved [5]. This revolutionary idea of not having a trusted intermediary anymore remains as one of the key elements of the blockchain technology [6].
Nakamoto suggest to hash the network transaction timestamps into an ongoing chain, in which records cannot be changed without doing a Proof-of Work (PoW) [5]. All the records are stored in a distributed database and all the data and transactions are public and transparent, visible to all participants of the network [7]. There is no longer a central control institution present since the validation is done through all the nodes in the network by specific consensus algorithms [6]. Due to its constitutions, blockchains are immutable, traceable and prevent double spending which are new advantages compared to former known networks [6]. As reported in [8], blockchain is the most fascinating and profound innovation since the invention of the internet [8].

2.2 How does a Blockchain work?

A blockchain can be seen as a distributed network which allows secure transfer and storing of data or programs [8]. Such a distributed network is built up by many computers (nodes) which write in a public register, the so-called ledger, and all transactions between the users. All those transactions are stored securely, comprehensible and, most importantly, immutable [8].

A blockchain is made from connected blocks where each block contains a header, one or more transactions and a list of uncle blocks which have the same parents [8]. Each header itself contains a timestamp, a hash of the following brick, a difficulty level, a nonce as well as the hash of the following block [8]. In order to add a new block with its transactions to the blockchain [8], the block and its transactions have to be validated by solving a crypto puzzle [6] the so called proof of work (PoW). The first miner who can solve the crypto puzzle receives an incentive in the form of crypto currency which is offered by the ledger [8]. Since each block contains a proof of work, every node can validate the block by checking the proof of work [8]. If an attempt is made to alter a block, the hash and block itself are no longer valid, therefore giving a blockchain its immutable characteristic.

2.3 Blockchain specific terms and concepts

2.3.1 Mining

Mining is the confirmation of blocks or, in other words, the solving of crypto puzzles [6]. Mining is a resource consuming task (once it is necessary to find a partial hash-collision satisfying a target) and difficult to sustain the number of added blocks to the network constant in order to counteract spam attacks [8]. The mining process can follow different concepts, the first one introduced by Bitcoin was the Proof-of-Work (PoW) [8]. Miners can be seen as the members of the network that solve the crypto puzzles and, therefore, add new blocks to the system. For this intense computing task, miners are getting incentives in the form of tokens or, in other words, cryptocurrency like Bitcoin in the Bitcoin blockchain [6].

2.3.2 Consensus

Consensus is one of the central concepts to understand in a blockchain. Since there is no single leader in a blockchain (no trusted third party) one has to come up with an appropriate mechanism to agree on consensus in order to make decisions [6]. Consensus therefore can be described as the state when the majority of the network agrees with the mining output - in other words, they agree on the validity [6]. There are many different consensus mechanisms and new concepts can rise every time. The first one implemented in Bitcoin was the concept of PoW [5] and lately, a more popular one is the Proof-of-Stake (PoS) protocol, both of which are described below.

2.3.3 Proof of Work

Proof of work was one of the central concepts implemented with the first blockchain Bitcoin [5]. Before a block is seen as valid, it has be proven through the PoW [8]. Transactions are stored in a transaction pool awaiting for minors to get collected and append to a new build block [6] [8]. In order to fulfil this process, miners have to solve a crypto puzzle defining a number of zeros as the input of the target hash, meaning that miners would need to find any hash that satisfies the condition of "N" zeros as input [6]. This is, in general, a computationally intensive task, becoming even more intensive depending on the number of zeroes required at the input [6].

As soon as the first miner solves the puzzle or finds the target hash, it is broadcast to the entire network, validated and the new block added to the BC [8]. The winner receives an incentive, cryptocurrency, which is provided by the protocol [8]. This concept is, among other things, highly resource intensive, since everyone is mining (solving the puzzle) like in a race where the fastest wins.

2.3.4 Proof of Stake

PoW consensus models need a lot of resources and time, therefore an alternative block validation model was developed, the Proof of Stake (PoS) concept. In this model, the blockchain is still based on an election process, in which participants entitled to validate transactions [8] need to present a number of tokens at stake. In a deterministic way, it is decided by the amount of tokens (wealth) who can mine a block [6]. In other words, there is a linear relationship between the number of tokens at stake and the mining power [6]. There are several frameworks using PoS like Ripple, Hyperledger or Corda [8]. Also, there are PoS variations, such as the Proof of Authority (PoA). PoA is a modified form of PoS where the role of the stake is replaced by the validator's identity [8]. Unlike the PoW system, not everyone is mining in the PoS system making it much less energy consuming. For example, Ethereum claims to have reduced energy consumption by up to 99% by replacing PoW with PoS [9].

2.3.5 Smart Contracts

The idea of Smart Contracts (SC) goes back years before the blockchain technology rise. The computer scientist Nick Szabo first mentioned the term in the 1990s in reference to computer programs which are executed without any central authority involved [7]. However, smart contracts without appropriate technology are not smart [6]. Thus, a smart contract has to be implemented in the right technological environment and a blockchain provides the ideal basis [6]. Within an SC the inputs and outputs are sometimes defined - also referred to as "if – then" rules [7]. Thus, as soon as the input is triggered the program code is running and delivering its specific output [7]. One has to consider that once a SC is set up it cannot be changed, it is immutable. Bugs in the program code can therefore not be fixed and one has to be sure that there is no mistake in the smart contract before implementing it [7]. SC in combination with BC's rise presented totally new opportunities and fields of application in which automated processes can be implemented in a trustworthy way [7].

2.4 Public perception: from a currency to a useful business solution

It is more than ten years ago when the first Bitcoin block "Genesis" was mined on January 3rd 2009 [6]. Although the technology is just ten years old, it has already had quite a rapid development over that time. When it was first practised as a peer-to-peer cash system [5], there were not many other capabilities seen in crypto currencies [6]. This perception started to change with the implementation of smart contracts, promising much more potential and opportunities [6]. Today the technology is already implemented in the industry and many more applications are due to be implemented in the next few years [6]. Generally, there are four areas to be distinguished in the development of blockchain until today.

- **Blockchain 1.0**: From the release of the Bitcoin whitepaper in 2008 until mid-2013, blockchain was mainly used for digital currency [6]. Bitcoin has been recognized as this new, mighty digital currency without much awareness of the use of blockchain in other areas. The PoW consensus concept was introduced in the first blockchain application and praised as the most significant idea behind Bitcoin since it provides contributed consensus [5].

- **Blockchain 2.0**: With the announcement of Ethereum in late 2013, the next era started [6]. Within three years, Ethereum and its implemented smart contracts brought the blockchain potential to the next level [6]. Different organizations are now recognizing the potential of blockchain technology in a variety of different fields and in 2016 the National Institute of Standards and Technology (NIST) held the first workshop about blockchain on healthcare [6].

- **Blockchain 3.0**: In this era, a large number of decentralized applications (DApps) were rising [6]. The public recognized blockchain technology as more than just a crypto currency and one Bitcoin reached its highest value to date at almost 20K USD [6]. However, new issues regarding scalability and performance came up which have still to be solved [6].

- **Blockchain 4.0**: As of today: In this latest stage, the blockchain technology is jumping into the industry, replacing disused systems or being added as new ones. Blockchains are nowadays customized to vendor specific claims [6].

2.5 General types of Blockchains

In general, one can distinguish two main types of blockchains: public blockchains and private blockchains. However, through the read/write and permissioned/permission-less characteristics, there are four different possible combinations.

2.5.1 Public blockchains

Public or permission-less blockchains are open [6]. In fact, anyone with a computer and internet access can join the network [7]. However, two types of write and read access can be distinguished: permission-less public blockchains and permissioned public blockchains. In a permission-less public BC, everyone can write and read [6]. In a permissioned public BC, every user is allowed to read but only selected members have the power to write [6].
The ledger which contains all transactions is transparent and visible to the public, which means everyone in the network [7]. Therefore, public blockchains are on the one hand transparent, since everyone has the ability to read everything, but at the same time it is hard to identify the participants since no prior identification is necessary in order to join the network [6] [7]. Public blockchains are seen as the real and only blockchains by its closest definition [6]. Probably the best-known example of a public blockchain is Bitcoin, another popular example is the Ethereum blockchain.

2.5.2 Private or permissioned blockchains

Private blockchains or distributed ledgers are, in comparison to public blockchains, not accessible to the public (or only through permission) [6]. The chain access permission is only given to known stakeholders before they can join the network [6]. Like in public Blockchains, one can distinguish among two types of read/write privileges: private permission-less BC and private permissioned BC. In a permission-less private network, all the pre-selected members have the power to read and write [6]. In a permissioned private network only a further selection of the pre-defined members can write or even read [6].
To become member of a private blockchain, one must receive an invite to join [7]. Since such networks have a member-only character, the access, processing and validation of transactions within the blockchain is reserved to stakeholders, who are known by the BC owner or creator [6]. A common example of a private blockchain is the Hyperledger Fabric. Although private blockchains are not really seen as “real” blockchains in a narrow view [6], they have their advantages [7]. In a private blockchain one knows all the participants, which can be both an advantage or a disadvantage, and such networks are in general faster compared to public blockchains [7]. Hyperledger is, at the moment, probably the most popular representative of a private BC.

2.6 Main Blockchain Implementations

2.6.1 Bitcoin

The first Bitcoin was issued in 2009 [6] by a group of people under the pseudonym Satoshi Nakamoto [8]- the real initiator is still unknown [6]. Bitcoin came at the start of the era of blockchain technology. This public blockchain is, as pre-defined by its initiator, limited to 21 million BTC [6]. The block size is limited to 1MB, an average time of 10 minutes is needed to create a block and not more than 3-7 transactions per second can be processed [6]. The validation is based on the proof-of-work concept which can be seen as one of the revolutionary ideas behind the Bitcoin concept [5]. PoW has two big advantages, first it is difficult to fake PoW and second double-spending can be avoided [6]. Due to the peculiarities of a BC, there is no control by a single unit or, in others words, Bitcoin offered the first cash system without any central authority such as a bank [6].

2.6.2 Ethereum

Ethereum was announced in December 2013 by Vitalik Buterin as another big public blockchain beside Bitcoin [6]. Compared to Bitcoin, it is not just a cryptocurrency but also a programming environment [8]. An important concept behind Ethereum are smart contracts on a blockchain [6], which makes Ethereum the most common framework for general purpose blockchain applications [8]. The key element is the Ethereum Virtual Machine (EVM), a consensus based virtual machine that decodes and runs the contracts on the nodes [8]. These smart contracts can generally be written in three different languages, but solidity in Ethereum is the most common one [8]. The concept of "rewarding" is slightly different compared to Bitcoin. A trading value "gas" has to be provided to the miner in order to execute a smart contract [6]. Since gas is a statistical evaluation of the calculation costs [8], it is obvious the more complex the transaction/SC is, the more gas is needed and has to be provided to the miner [6]. In comparison to Bitcoin, Ethereum has an unlimited supply, needs an average of 14 seconds to create a new block and can therefore provide up to 25 transactions per seconds [6]. In other words, Ethereum is more versatile and faster in comparison to Bitcoin.

2.6.3 Hyperledger

In comparison to Bitcoin and Ethereum, which are both public blockchains, Hyperledger is a representative of a private blockchain [6]. It was released in December 2015, two years after Ethereum [6]. The Hyperledger umbrella project was built by a cooperation of different market leaders to advance blockchain technology and create a cross-industry standard platform [10]. Unlike public BCs, there is no currency available in Hyperledger and the architecture is a private distributed ledger [6].
As mentioned, one key element of blockchains is the decentralized consensus. Consensus mechanism in Hyperledger is different from the PoW in Ethereum and Bitcoin [8]. In Hyperledger, consensus is based on the Practical Byzantine Failure Tolerance (BFT) [6] which means that consensus is given based on the decisions made by the nodes in the system [6]. Compared to the PoW, this concept is much less energy consuming and faster, which makes private blockchains more efficient and allows more transactions per second compared to public blockchains [7].

2.7 Why should one use a Blockchain?

As described by Rodrigues *et al*. it is not so easy to determine whether to use a blockchain or not and there is no general formula for when the use of blockchain is appropriate [11]. It is important to analyse in detail the characteristics, challenges and goals of the planned application as well as to evaluate the different type of blockchains and their properties [11]. Even though there is no final formula, there are some basic rules available that should help in the decision making [12] [13]. Greenspan defines five compelling conditions and three optional conditions that should be fulfilled in order to use blockchain technology for a specific case [12].

The compelling conditions and rules are [12]:

- The database: Data that has to be stored must be involved.
- Multiple writers: Blockchain technology is made for databases with multiple writers
- Absence of trust: Some degree of mistrust among the writers must be present. Blockchain technology fits for databases with multiple untrusted writers.
- Disintermediation: This point might be one of the most crucial one for blockchains. The need for a trusted intermediary is no longer present, databases with multiple untrusted users are enabled to edit. The general question here is whether disintermediation is wanted, needed or unavoidable?
- Transaction interaction: There must be some interactions between the transactions present. This means that transactions by different writers depend on each other.

Those five points have to be fulfilled in order to think about using blockchain technology accordingly to Greenspan. Additionally, the author recommend three further points [12]:

- Set the rules: There must be rules embedded to restrict the transactions performed. Every transaction is checked by each node against these rules.
- Pick your validators: One must choose the right validators and come up with a suitable consensus mechanism.
- Back your assets: The blockchain must be translated into the real world.

In addition to the above summarized requirements by Greenspan, Rodrigues et al claims that sequential transactions are also necessary [11]. This means that the order of transactions have to impact further transactions [11]. All these mentioned conditions should be fulfilled in order to use a blockchain in a specific case. However, these conditions only show you a possible use of blockchain - the use case requirements should also be taken into consideration [11]. Rodrigues et all summarizes the following requirements [11]:

- Performance: blockchains are slower than centralized databases and not tested as much - is performance important?
- Distributed or centralized control: this core element of blockchain has to be evaluated to see if it is really needed in the specific case.
- Privacy and confidentiality: In blockchains, all data is visible and transactions are transparent to everyone. If privacy and confidentiality are needed and there is a trusted third party, BCs have no advantage over centralized databases.

- Robustness or reliability: Blockchains are by definition fault tolerant because of the built-in redundancy.

It is important that not only are these requirements evaluated, but also the trade-offs between them [11]. At first glance, one would probably not assume intuitively that not all blockchains are meant to store sensitive information [11]. However, by combining blockchains with, for example, off-chain centralized solutions, one can overcome the challenges with sensitive information as well as the huge amount of data [11]. It is furthermore important to also consider and assess any possible combination of these requirements [11].

Similarly, Wüst proposed a flow chart to determine whether blockchain technology in specific cases makes sense and which one should be chosen [13]. The decision making starts with the question: does data need to be stored? It then asks if multiple writers are present and if a trusted third party is present [13]? These three questions are initially used to decide whether to use a blockchain or not. An additional three questions are in the flow chart in order to decide which blockchain is the most suitable. One has to decide if all writers are known, if all writers are trusted and if public verifiability is necessary [13]. With this flow chart one can do a case by case analysis and get the assessment of whether to use a permission-less blockchain, a public permissioned blockchain, a private permissioned blockchain or to not use a blockchain at all [13].

3. The healthcare industry and its challenges

Although healthcare systems are different in each country, developed systems are facing a continuous trend of rising healthcare spend each year [2]. In Europe, the healthcare spending among the OECD countries in 2015 was 6% of the GDP and is predicted to rise to 9% in 2030 and 14% by the year 2060 [2]. In other words, health spending has risen faster among OECD countries than economic growth [2]. When looking for the main challenges driving the cost increase, there is consensus among the western healthcare systems. Demographic development, increase of chronic diseases and medical-technical progress are the most common cost drivers [14] [15]. Life expectancy increased within the last decades enormously, in that people are firstly living longer and secondly there will be (and already are) much more elderly, retired people and a decreasing younger workforce [14]. Since the health spend is increasing disproportionally in the elder years and, at the same time, there is a smaller workforce, the cost misbalance increases [14]. Also, people are not just getting older, they are more often getting old with a disease [14]. Since many diseases can be treated today, but not entirely cured, many people are receiving expensive life-long treatments which leads to enormous health expenditure [14]. Related to this, there was (and still is) a tremendous development in medical and technical progress, which allows us to treat more complex diseases - bringing higher treatment costs [14]. The increased health expenditures are coming half from the demographic development and half due to more chronic diseases in combination with medical-technological progress [15].

The longer life expectancy and the misbalance between retired people and the workforce are social circumstances which cannot be impacted that easily. Efficiency is one key word to control the other two cost drivers. Since special treatments are expensive, payers will more

often only pay for efficient treatment with a positive effect [15]. Treatments can be successful for a certain group of patients, while there is barely any effect in others.

With the recent technological progress, healthcare treatment is moving towards personalized medicine, earlier diagnosis or long term outcome evaluations, with the aim to make the treatments, and therefore the entire healthcare system, more efficient [15].However, in order to use most of the new technologies properly, good quality health data is needed which is often not yet a given. The context of health records, efficiency and interoperability is discussed below in Section 3.1.

The above challenges mainly occur in well developed countries and healthcare systems. Switching the focus towards a global view, another major issue is counterfeit drugs. A comprehensive report by the World Health Organization (WHO) showed that one out of ten medical products in developing countries is substandard or falsified, leading to tens of thousands of deaths every year [16]. Although this threat is not new, authorities all over the world are struggling with this topic (the WHO even launched a task force in 2006 against counterfeit drugs) [17]. In the drug supply, one must come up with a tracking mechanism for all stakeholders to prove the ingredients of a drug. This is where blockchain might provide a very useful solution [18]. Addressing this challenge, different solutions have been proposed also with blockchain technology being involved [18].

3.1 Interoperability

As mentioned above, good quality health-care data is key to make the right decisions and provide the best treatment to individual patients in order to improve the efficiency of the system. Thus, medical data-sharing is a key element in the healthcare system. In many of today's healthcare systems for the sharing of medical data, a patient has to maintain their own medical records and share it with several providers via physical paper copies or digital copies on a physical storage [19]. This outdated way of data sharing is seen to be inefficient due to four major issues [19].

First, it is slow since a patient has to obtain, deliver and pick up medical records in a physical way [19]. A typical example is the preparation of different x-ray pictures and medical history if someone switches their doctor/hospital. Transferring data in this way is costly and inefficient [11].

Another major issue is the lack of security with patient data [11]. Medical records can easily be lost or stolen while being physically transmitted by the patient to the providers [19]. This does not even require a criminal element to be present, the data can easily be forgotten in a public place (*e.g.* train).

A third issue is seen in the incompleteness of the data. Since there are so many providers and stakeholders involved, the data is stored in different, disparate and soiled systems [19]. Without a single source containing all the information, each patient has to keep track of what information was sent to the different care providers in order to be able to get a copy of the record [19]. The fragmented data itself has to be maintained by each institution or entity individually [11]. This makes it hard to use the data in a proper way for diagnosis and health analysis.

In such a fragmented, provider-centric system, the provider has furthermore unfettered access to the records [20] which might not fulfil modern data protection regulations. Zhang et al. even describes patient-centred care as one of the major pressing issues in the healthcare industry [19]. In an ideal healthcare system, all contributors would notify the patient immediately when new data is available (*e.g.* lab results entered) [19]. In contrast to today's rather provider-centric system, a patient-centric system would be necessary [19]. In today's healthcare system, the provider is permanently in possession of the patient's data once access is granted [19].

3.1.2 The patient centric healthcare system

In contrast to the above, in a patient-centred system, patients are in full control of their data instead of the providers. They can decide when, what and to whom they want to share their data [19]. However, the implementation of a patient-centric system is not straightforward [20]. On the one hand, there is a technical challenge since all service providers would need some sort of unique access key to all the medical records. On the other hand, such an implementation might create a lot of administrative work [20]. As Zhang et al. describes there are barriers in the current healthcare technical infrastructure which can be summarized as information security privacy concerns, a lack of trust between providers and scalability concerns [19].

As described in this section, there are several challenges that healthcare systems are facing which depend also on the development stage of the individual system. In general, one could summarize the most common institutional challenges from above as [2][14] - [20]:

- Multiple stakeholders with different interests involved (interoperability).
- Fragmented data, sub-data sets and data security (interoperability).
- Lack of trust among the stakeholders (interoperability, security).
- Demographic changes, chronic diseases.
- Medical-Technological progress leading to new, more specific treatments.
- Provider-centric view - patients are steered by provider.
- New dimension of fraudulent drugs being available over the internet (drug traceability).

In other research, the categorization was done on a higher level, where interoperability, drug traceability and data security have been found to be the most urgent issues in healthcare [1]

In order to face those challenges, several changes and trends are apparent [14-20]:

- Comprehensive medical records and datasets.
- Regulation reforms among the stakeholders.
- Progress towards patient-centric systems.
- Movement from general to personalized medicine.

There seems to be some benefits that blockchain can bring to the healthcare industry in order to overcome the challenges above. The main benefits of blockchain are seen in transparency and trust [11] which could, for example, help in building up comprehensive medical records or support the progress towards a patient-centric system.

But as Rodrigues *et al.* state, it is important to mention that, the presence of blockchain alone, does not mean healthcare systems should be completely rebuilt [11].

4. Use cases in the healthcare industry

There are different fields with use cases in the healthcare industry. Examples are medical records or patient dossiers, insurance reimbursement management, medical supply chains or prescription billing [7]. The healthcare industry faces several challenges where the interest of more use cases is present. However, the most urgent fields can be summarized as interoperability, drug traceability and data security [1]. In the following section, some different use cases from different fields in healthcare are described. Also, it is worth noting that use cases discussed here were selected from a wider range of uses cases. In section 4.5, there is further analysis provided for a possible use case in combination with AI for personalized medicine.

4.1 Healthcare data management

Improving healthcare data management is an approach for dealing with interoperability as well as data security.

There are several projects dealing with the recording, management and sharing of healthcare data [18], in this section the focus is on MedRec. MedRec is a decentralized record managing system implemented in 2016, which uses blockchain technology to allow patients to manage their Electronic Health Records (HER)[21]. MedRec manages authentication, confidentiality, accountability as well as data sharing [21] which were previously managed by different healthcare providers, with and sharing or accessing records laborious process for patients. Based on a Etherum blockchain, a decentralised record management system has been created which provides patients with easy access to their data [21]. The network consensus is provided via Proof of Work and all the embedded stakeholders receive access to aggregated, anonymized data as a mining incentive [21]. Through smart contracts the patient-provider relationship is logged and provides the instruction to execute on external data in order to access the data [21]. There are three types of contracts being implemented: register contracts, patient-provider relationship contracts and summary contracts [21].

Register contracts are used to map the patient's identification to its corresponding Ethereum address [21]. These forms of contracts are executed for registering new identities or to change the mapping of existing ones [5].

Patient-provider relationship contracts are used when nodes are managing medical records of or for each other [21]. Providers can easily select the desired data by using a simple SQL SELECT query, while a simple tool was designed for patients to control and check their records [21].

The third type of contracts are summary contracts which are used to locate the patient's medical record history [21]. Patients can see all the providers they were engaged with and providers

can see all the patients they are serving as well as the third parties with whom the patients are sharing information [21]. MedRec demonstrates how to orchestrate medical data in a decentralized blockchain to provide patients with comprehensive record review as well as empowering research through anonymized, comprehensive medical data [21].

Since several mistrusting stakeholders (writers) are storing medical data, blockchain might indeed be a useful way to share medical information. There are many different interests among these stakeholders where trust in the system cannot be fully given. In the healthcare system there is no trusted intermediary acting as a controlling institution, rather the different stakeholders just own and manage the individual data. Such a third party might indeed not even be needed since each patient should have the ability to manage their own data. Using an Ethereum blockchain to provide patients access and control over their medical records seems to be a useful solution. It also allows easier sharing of medical data between healthcare providers (e.g. when a patient is moving) which makes the entire system more efficient and therefore helps to get the rising healthcare expenditure under control.

4.2 Fighting counterfeit medications

Fighting counterfeit medications by using blockchain technology can be assigned to drug traceability as well as data security, as seen in Section 3. After the enaction of the Drug Supply Chain Security Act by the FDA, with the idea of having an electronic interoperable system to trace drugs [22], the need for new technology arose.
The MediLedger project and FarmaTrust are two examples of use cases where blockchain technology is applied to fight counterfeit drugs. The MediLedger project was initiated in 2017 by several big pharmaceutical companies like Pfizer or Genentech as well as global wholesalers [23]. With MediLedger, the team wanted to explore the possibility and feasibility of using blockchain technology in the drug supply chain [23]. The focus was to evaluate a solution in compliance with the Drug Supply Chain Security Act (DSCSA) but the conclusions can also be used for further use cases [23]. It is based on an open network which is accessible to the entire pharma supply chain [24]. The basic technology is a permissioned Ethereum setup [24] with a client/node interaction with a specific form of consensus, the zero-knowledge-proof (ZKP) [23]. The client stores the private data (also transaction data), receives transactions and prepares them by calculation of the hashes [23]. The node, at the same time, maintains the blockchain security by participating in the consensus process and also hosts the smart contract [23]. In the zero-knowledge-proof method, the verifier provides the receiver only the information that a statement is true but not any additional information about the transaction [23] [25]. This has some specific advantages in this use case. If all transactions are accessible for everyone, there would be a conflict of interests. It would create a competitive disadvantage to join the network if the pharma companies and wholesalers can see all the transactions among each other [26]. Another advantage is that ZKP is more efficient in that MediLedger is faster compared to the public Ethereum [24].

FarmaTrust is another pharma tracking system designed to fight counterfeit medicine by pairing blockchain technology with artificial intelligence [27]. By integrating data from warehouses, manufacturers, shipping and logistics, counterfeit drugs are eliminated from the supply chain [27]. All packages are tracked in the blockchain and the end-customer can easily

check the validity of the medicine [27]. A permissioned blockchain network is implemented in which smart contracts among trade partners are evoked (e.g. manufacturer or wholesalers) [27]. Compared to MediLedger, FarmaTrust uses a different blockchain technology called Quorum [28]. A Quorum blockchain provides a combination of public and private transactions, where a transaction can be open (similar to Ethereum) or private (meaning it is confidential and not transparent) [28]. The consensus mechanism is based on a voting system where voting rights are delegated to other members [28].

As mentioned in section 3, counterfeit drugs are an increasing issue worldwide which cannot be controlled with current solutions. Since a drug is passing from the manufacturer to the end-producer through several stakeholders, it is hard to control where the drug originally came from since there is no end-to-end security. With approaches like MediLedger or FarmaTrust, a secure end-to-end supply chain in pharmaceuticals can be achieved. High trace and track regulations can be fulfilled and a safe drug supply guaranteed. This is important in order to fulfil high treatment standards and guarantee quality in medical treatments.

In the current system, the absence of trust can be the biggest challenge offering fraudulent players the opportunity to bring counterfeit drugs into the chain. With its immutable characteristics, blockchains is a proffered solution as it becomes nearly impossible to bring counterfeit drugs into a blockchain system. Since every single drug has to be trackable, it is almost impossible for a third party to check whether all transports were compliant. A blockchain with no need for a trusted intermediary makes it possible to guarantee fully compliant supply. The scalability of the tracking system allows an end-to-end tracking of each drug. MediLedger and FarmaTrust are two good examples that successfully use the advantages of blockchain over current solutions.

4.3 Blockchain & AI, feasibility for precision medicine

As discussed in Section 3, the healthcare system is tending towards a patient-centric system, where personalized medicine becomes more and more important to ensure efficiency and quality of treatment. Precision medicine generally means the treatment and prevention based on individual genomic variety [29]. It is less designing a customized drug for one specific person, but rather clustering individuals into subpopulations [30] to provide the treatment with the best health outcome.

It is almost 20 years since the successful sequencing of the vast majority of the human genome in 2000 [31]. Back then, researchers would assume that this new discovery would influence the prediction of individual risks of diseases and the implementation of personalized drugs (precision medicine) based on the patients individual genome [31]. And indeed, within recent years, several causal relationships between genes and diseases have been discovered [32] and a trend from classical medicine towards precision medicine has developed. However, besides the positive outcomes [32] and promising applications [33], it seems like the full potential for patients in the medical mainstream has not yet been fulfilled. To reach the full potential of precision medicine, not only genomic information but also data from providers and data from

sensors and mobile devices is required. Since there are many different types of data, one needs to provide a reliable data sharing environment. Once all the different data and systems are optimally integrated, it could be possible to know when someone should receive a specific preventive treatment before a severe event happens. Based on individual genomic characteristic, the potential risk of specific diseases can be evaluated. As an example, an individual can be clustered into a specific risk group of having a stroke based on genomic information. Sensors and mobile devices can then further estimate the risk of having a stroke in the nearer future based on the current health condition. A physician therefore, would know before a stroke happens when a specific patient should receive a specific preventive treatment.

Blockchain provides a large open dataset which, in combination with artificial intelligence, could bring precision medicine to the next level. As described in section 2.7, there are five main conditions that must be fulfilled in order to use blockchain technology in a specific case [12]:

- **The database**: Data must be recorded and stored for precision medicine to track when certain conditions are fulfilled. This includes not only the genomic sequence information but also medical records and treatment history as well as data coming from sensors and smart devices (Internet of Things – IoT).

- **Multiple writers**: For precision medicine, several players are involved by nature. On one hand, the hospitals and physicians need to document the patient's conditions and the treatments ideally with the outcomes. On the other hand, Pharma companies should provide information from clinical trials and other relevant information about drugs, their application and treatments. At the next level, specific genome information could be available too which could be provided by an additional player. Lastly, data coming from sensors and devices are also updated and integrated. Looking forward, even stakeholders with information about insurance contracts etc. could be involved to automatically check payment reclaims. One can see that many different stakeholders and therefore writers are involved in precision medicine.

- **Absence of trust**: Although one could expect increased levels of trust in each of the involved stakeholders, there is some degree of mistrust among the writers since the interests of each are so different (e.g. Pharmaceutical company and Payers).

- **Robustness and reliability**: The blockchains ability to replicate transactions and permanently record them is an advantage in this case. If one of the stakeholders updates any data, one can see exactly what was updated, the impact it has and how the historical data. It gives further security benefits since attackers cannot easily change important information, e.g. genomic sequences or clinical trials results, which could lead to possible harmful treatment of a patient.

- **Disintermediation**: No trusted third party is available and is not even required in this example. As mentioned above, there are several stakeholders with different interests present in the system but they would not be controlled by a third party. The controlling party in a healthcare system is usually a governmental institution which controls and

regulates different aspect among the stakeholders. In Switzerland for example, this would be the Federal Office of Public Health (FOPH). However, it seems impossible that one third party can control and evaluate all the individual cases in a system for precision medicine based on patient's health outcome. Furthermore, a centralized management and ownership is not even required since patients should manage their own records. Therefore, one needs to come up with a trustworthy system without a controlling third party.

- **Transaction interaction**: Decisions on what treatment and at which point a physician should implement them depends heavily on the interactions between different transactions. Depending on clinical outcomes and a patient's specific condition, an individual therapy will be applied by the physician.

To summarise, mandatory requirements seem to be fulfilled and blockchain technology could offer great value when used in precision medicine. The collection of all this data offers a powerful instrument and there is a potential risk of misuse and fraud. Blockchain could indeed provide a good solution in dealing with such sensitive personal data. Furthermore, it is not straightforward to hide or delete undesirable outcomes (*e.g.* adverse events) since every change in the system is tracked and transparent. Also, in terms of performance, there is not much contradiction in the use of blockchain. Since there are not so many transactions which need to be done within seconds, the slower performance of blockchain compared to centralized systems is not such a big issue. However, since so much data is involved, one needs to evaluate carefully which data to store on the chain and which off-chain. For example, it would probably make more sense to store the genomic information centralized off-chain and only pointers on the chain as generally described by *Rodrigues et al* [11].

It seems to be legitimate to ask whether such a big project is technically feasible. There are many different stakeholders involved, which must be coordinated, and many different forms and sources of data. It could be possible to approach the solution by having several permissioned blockchains (*e.g.* Ethereum) to start with less complexity. It might be useful to first separate the genomic data and access from all the information coming from mobile devices (where further data integration and quality control might occur). However, here one has to take blockchain data silos into consideration which should be avoided. One possible solution could be to have a public blockchain though which all the others are accessible.

In addition, the use of machine learning can bring up powerful algorithms that allow us to find meaningful patterns in genomic data (*e.g.* CT scans). In order to come up with those powerful algorithms, the systems need data - lots of data. This is where blockchain technology comes as an instrument to store, provide and share robust and comprehensive data on an individual level. Therefore, blockchain is just one piece in the precision medicine jigsaw to fulfil the potential for the society by providing a large open dataset.

5. Discussion

As described in Section 2.4, there is an ongoing evolution in BC itself, but also in the perception of the technology. Society is drifting away from BC as just a currency, namely cryptocurrencies, and sees more and more the opportunities for integrating this new technology into daily systems and processes. There is promising potential for BC to add value to current healthcare systems. It is a fact that, around the world, the costs of healthcare systems are growing and this is not a development we are able to stop or reverse. Tremendous changes are needed on a systematic, social but also technological level. New ideas and approaches are therefore more enthusiastically welcomed compared to other industries. Additionally, not many processes relating to data collection and sharing, are well defined or digitalized. As described by *Rodrigues et al*, BC needs to offer a measurable added value over existing systems. If there is not an obvious advantage, it is unlikely that the new technology will even be tested [7]. Since healthcare systems have to change tremendously in the future, new processes and systems (e.g. in data collecting and storing) have to be implemented. As there is often no existing system, it is easier for BC use cases to be implemented (or at least tried out) than in other industry sectors. However, in the healthcare industry, BC must not only deal with technological, but also legal, governmental and eco-social aspects.

Regarding the technological challenges, uses cases in the healthcare sector are obviously facing the same challenges as BC applications in general. One of the general challenges of BC is scalability. Especially when integrating more and more stakeholders of the healthcare sector - this seems to be one of the biggest hurdles. An additional challenge in healthcare are the many different stakeholders with their own devices and data types, which makes the implementation of BC even more difficult. It seems to be valid that in the near future, several semi-permissioned blockchains might be active in the healthcare as described within the use cases in section 4. However, at one point a public BC seems to be necessary in order to integrate all those different networks. (Otherwise, we will end up with several, non-integrated systems which would not be an advantage.)

There are further regulatory aspects in storing all health information on a blockchain that must be considered, mainly relating to the newly implemented General Data Protection Rule (GDPR). Under Art. 17, it states that an individual has the right to erase personal data [34]. However, this is contradictory with BC technology due to the immutable nature of a blockchain. *Katuwal et al* suggests that if health information is stored off-chain (and only pointers such as cryptographic hashes are stored in the chain) the application should be compliant with the GDPR [18]. However, the GDPR must be considered for each use case specifically. There are, in general, many different institutional or regulatory aspects relating to BC and especially in healthcare. Many governments have no general conditions regarding BC. Furthermore, in healthcare, where many different stakeholders are involved, all of them need to be integrated into one system. As discussed, interoperability is one of the biggest challenges in healthcare. Independently of BC, integration into one system must be implemented and regulated by government. BC technology can therefore be a helpful technology in the implementation, but in this case becomes just a tool rather than a comprehensive solution to tackle interoperability issues. Also, the role of the government within a BC with multiple stakeholders with different interests may have to be redefined.

One should also consider the many people working in healthcare. For many of them, the step towards digitalization is not as easy as it sounds since many routine tasks must be adopted with potential increased workload at the beginning of an implementation. However, this seems to be a hurdle that can be overcome with the right coordination and approaches, it just needs some time since human beings tend to have routine in their daily lives.

New technology should bring more efficiency to healthcare and therefore, of course. Save costs. In general, blockchain can simplify and improve processes and, due to new possibilities in healthcare, the saved costs (e.g. through more efficiency) are assumed to be even higher. But it is important to evaluate the impact, and especially the costs, of running and maintaining the blockchain system. Since it is a rather new technology, an accurate cost assessment might not be that easy and could even change due to newer BC technologies. However, a transparent costs assessment is crucial in order to implement BC successfully among the different healthcare stakeholders. In general, it is safe to assume that implementing a blockchain solution will not save costs immediately. Depending on the complexity and the impact, it might take several years in order to see cost saving effects.

Although blockchain is a rather new technology, and the possible fields of applications might not live up to the early hype, there is a promisingly potential of BC in healthcare. Although there are still some technical challenges to deal with, the bigger hurdles might be in the eco-social environment.

6. Conclusion & Outlook

Reforms in the healthcare system are needed in order to deal with modern challenges. Independently of blockchain, there is a need to improve the coordination among the different stakeholders and adopt current processes as well as legal aspects to better meet the new circumstances. The biggest challenge remains the interoperability. In current BC use cases we are faced with off-chain solutions done in different SC languages. It therefore needs effort to come up with a common SC language to make the system consistent. New approaches should be evolved in order to deal with the trend towards blockchain data silos. Currently, there is no gold standard, approaches like side-chains are very complex or notary-schemes re-introduce a centralized party. Future research should focus on how to deal with those silos.

It seems legitimate that the government should take responsibility in the coordination of future development of the system, including technological evolution. The relevant reforms have to be made in order to have the system ready to adopt new technologies and, at the same time, the implementation of those technologies should be coordinated by the government rather than different third parties. A governmental focus group containing experts from the stakeholders, universities and research institutions might be helpful to guarantee the right changes and technological consistency. With a proper approach, blockchain could bring future advantages to reshape the healthcare system, make it more efficient, provide suitable individual treatments and finally save costs for everyone while embedding the interests of all stakeholders involved.

References

1. Richa, S.: Blockchain in Healthcare, http://www.fccco.org/uploads/Blockchaininhealthcare_FCCCO_RS.pdf, (2018)
2. OECD: Healthcare costs unsustainable in advanced economies without reform, https://www.oecd.org/health/healthcarecostsunsustainableinadvancedeconomieswithoutreform.htm, (2015)
3. Castillo, A., Castillo, A.: Gene editing using CRISPR-Cas9 for the treatment of lung cancer. Colomb. Médica. 47, 178–180 (2016)
4. Engelhardt, M.: Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technol. Innov. Manag. Rev. 7, 22–34 (2017). doi:http://doi.org/10.22215/timreview/1111
5. Satoshi, N.: Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/en/bitcoin-paper, (2008)
6. Stiller, B., Rodrigues, B., Scheid, E.: Clouds and Blockchains. Lecture in CAS Program big data & machine learning. , University of Zurich (2019)
7. Egloff, P., Turnes, E.: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens. SKV (2019)
8. Mohanty, D.: Blockchain für Manager. FRANZIS Verlag GmbH (2018)
9. T, A.: Inside Ethereum's Plan To Reduce Energy Consumption by 99%, https://www.ccn.com/inside-ethereums-plan-to-reduce-energy-consumption-by-99, (2019)
10. Cachin, C.: Architecture of the Hyperledger Blockchain Fabric, https://pdfs.semanticscholar.org/f852/c5f3fe649f8a17ded391df0796677a59927f.pdf, (2016)
11. Rodrigues, B., Bocek, T., Stiller, B.: The Use of Blockchains: Application-Driven Analysis of Applicability. In: Advances in Computers. pp. 163–198. Elsevier (2018)
12. Greenspan, G.: Avoiding the pointless blockchain project, https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/, (2015)
13. Wust, K., Gervais, A.: Do you need a Blockchain?, https://ieeexplore.ieee.org/document/8525392/, (2018)
14. Hellmann, W., Eble, S.: Gesundheitsnetzwerke initiieren: Kooperationen erfolgreich planen. MWV Medizinisch Wissenschaftliche Vertragsges. (2009)
15. Meyer, P.C., Brauchbar, M.: Trends und Herausforderungen im Gesundheitswesen der Schweiz. Schweiz. Ärzteztg. 99(33), 1072–1075 (2018). doi:https://doi.org/10.4414/saez.2018.06842
16. WHO: 1 in 10 medical products in developing countries is substandard or falsified, https://www.who.int/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified, (2017)
17. WHO: Growing threat from counterfeit medicines. Bull. World Health Organ. 88, 241–320 (2010)
18. Katuwal, G.J., Pandey, S., Hennessey, M., Lamichhane, B.: Applications of Blockchain in Healthcare: Current Landscape & Challenges, https://arxiv.org/abs/1812.02776v1, (2018)
19. Zhang, P., Schmidt, D., White, J., Lenz, G.: Blockchain Technology Use Cases in Healthcare. In: Advances in Computers. pp. 1–41. Elsevier (2018)
20. Zhang, P., White, J., Schmidt, D., Lenz, G.: Design of Blockchain-Based Apps Using Familiar Software Patterns with a Healthcare Focus, https://www.hillside.net/plop/2017/papers/proceedings/papers/19-zhang.pdf, (2017)

21. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: Using Blockchain for Medical Data Access and Permission Management. Presented at the 2nd International Conference on Open and Big Data , Vienna (2016)
22. FDA: Drug Supply Chain Security Act (DSCSA), http://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa, (2019)
23. The MediLedger Project 2017 Progress Report, https://uploads-ssl.webflow.com/59f37d05831e85000160b9b4/5aaadbf85eb6cd21e9f0a73b_MediLedger%202017%20Progress%20Report.pdf, (2018)
24. Morris, N.: MediLedger: Pharmaceutical industry's blockchain network, https://www.ledgerinsights.com/mediledger-pharmaceutical-blockchain/, (2018)
25. Ashish: Introduction to Zero Knowledge Proof: The protocol of next generation Blockchain, https://medium.com/coinmonks/introduction-to-zero-knowledge-proof-the-protocol-of-next-generation-blockchain-305b2fc7f8e5, (2018)
26. Maksym Petkus: Zero-Knowledge Supply Chain Blockchain. Consensus 2018. , New York (2018)
27. FarmaTrust: FarmaTrust Progress Report, https://medium.com/@farmatrust/farmatrust-progress-report-dec-2018-4282442de07b, (2018)
28. Sharma, T.K.: What is Quorum Blockchain?, https://www.blockchain-council.org/blockchain/what-is-quorum-how-is-it-different-from-other-blockchain/, (2018)
29. Genetics Home Reference: Help Me Understand Genetics Precision Medicine, https://ghr.nlm.nih.gov/primer/precisionmedicine.pdf, (2019)
30. Timmerman, L.: What's in a Name? A Lot, When It Comes to "Precision Medicine," https://xconomy.com/national/2013/02/04/whats-in-a-name-a-lot-when-it-comes-to-precision-medicine/, (2013)
31. Collins, F.S., McKusick, V.A.: Implications of the Human Genome Project for medical science. JAMA. 285, 540–544 (2001)
32. Ng, S.B., Turner, E.H., Robertson, P.D., Flygare, S.D., Bigham, A.W., Lee, C., Shaffer, T., Wong, M., Bhattacharjee, A., Eichler, E.E., Bamshad, M., Nickerson, D.A., Shendure, J.: Targeted capture and massively parallel sequencing of 12 human exomes. Nature. 461, 272–276 (2009). doi:10.1038/nature08250
33. Ashley, E.A.: Towards precision medicine. Nat. Rev. Genet. 17, 507–522 (2016). doi:10.1038/nrg.2016.86
34. European Parliament: Art. 17 GDPR – Right to erasure ("right to be forgotten") | General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-17-gdpr/, (2016)