Computer Science and Information Systems 18(3):927–955 https://doi.org/10.2298/CSIS200426017D

Real Time Availability And Consistency Of Health-Related Information Across Multiple Stakeholders: A Blockchain Based Approach

Zlate Dodevski[1], Sonja Filiposka[2], Anastas Mishev[2], and Vladimir Trajkovik[2]

[1] iBorn, Skopje, Republic of North Macedonia
zlated@iborn.net
[2] Faculty of Computer Science and Engineering,
Ss. Cyril and Methodious University,
Skopje, Republic of North Macedonia
{sonja.filiposka, anastas.mishev, vladimir.trajkovikj}@finki.ukim.mk

Abstract. Sensitivity of the health-related data and the focus on compliance and security has traditionally emphasized the need for centralized approach while implementing Electronic Health Records (EHR) systems. These one-institutional architectural designs are leading to fragmented and scattered pieces of valuable data across various data warehouses and silos. Interoperability challenges arise due to the absence of unified data management and exchange mechanisms making the social need for fundamental design changes bigger.

The capability of a distributed ledger technology and blockchain to offer immutable, decentralized and cryptographically secured record of transactions throughout a peer-to-peer network can facilitate better collaboration and increased interoperability in the field of health and insurance information exchange processes. The paper examines different approaches and application of blockchain technology and identifies which implementations of components are more suitable and beneficial for the specific eco-system analyzed in the paper.

This paper presents alternative way of dealing with information exchange across multiple stakeholders by justifying the use of decentralized approach, distributed access and solution how to comprehensively track and assemble health related data. We propose an architectural design and overview of a specific use case with focus on information exchange processes between health insurance providers and health care organizations, by using blockchain as an underlying technology.

The architectural overview and data flows, backed up by sequence diagrams from specific use cases offered in this paper, can serve as a guide to the blockchain technology adoption and initial setup.

Keywords: blockchain, health-related data, health information exchange, health insurance, decentralization

1. Introduction

The process of improving the efficiency and quality of the health information exchange is a hot topic in the last period in the field of health informatics. HIE (Health Information Exchange) represents electronic transfer of clinical and / or administrative information between different (mostly competitive) healthcare organizations [2]. When talking about the actors in this ecosystem, they can be of different size and form, including clinical centers, hospitals, laboratories, insurance companies, pharmacies, emergency centers, nursing homes, public health centers, etc. The data exchanged can differ and can be part of a wide range, from a summary of medical examinations, referrals, to laboratory results, and even medical history of specific patient. However, the data that is subject to transfer can be structured in different formats and different terminologies can be used, making the interfaces and integration layers which are part of the HIE process more complex and with high cost. Additionally, the data that is subject to a transfer is scattered across the storages of the organizations that are involved in the process, which often leads to inconsistent data handling processes and erroneous and incomplete medical history records.

Technologists and participants in the e-health industry in the recent period are seeing the blockchain technology as innovation in the attempt to improve the data sharing processes. They are seeing opportunity of using the blockchain infrastructure to create a powerful catalog of health records that references different data sources and connect the patients, healthcare providers, laboratories, researchers, health insurance organizations and many other participants in the eco-system [24].

One of the main goals of this research is to emphasize the need for improving the HIE process and investigate the benefits that HIE systems will have with adopting the blockchain technology.

Blockchain in its essence is a distributed system that stores records for specific transactions. It is a distributed ledger of peer-to-peer transactions, which are grouped in blocks that are connected between themselves. Well-defined cryptographic techniques are fundamental pieces which enable this technology and their efficiency is proven by the first application of blockchain technology in Bitcoin cryptocurrency system presented by Sathoshi Nakamoto [27]. They are the core principles that enable decentralized interactions (processes of storing, exchanging and accessing data) between each participant in the network, bypassing the need for intermediaries and regulatory bodies to acquire trust. In this distributed system, there is no need for central authority, instead of that we have records of transactions which are stored and shared between the involved participants in the network. This characteristic is a foundation for offering innovative solutions in different business use cases [26]. In the first application of blockchain technology, the Bitcoin cryptocurrency system, every participant must be familiar with every interaction in the network and every transaction needs to be verified by all participants to be successful and valid. The verification of the interactions and the distributed state of the network are the principles that enable the collaboration in system in absence of trust between members, while the global log of transactions is immutable. Other approaches that rely on distributed ledger technology and blockchain were introduced in the last period, all of them trying to solve the challenge of achieving consensus in a decentralized environment. At the same time, Blockchain is an emerging technology with unanticipated challenges and the promise of unrealized potential in healthcare [29].

During recent years, blockchain becomes emerging technology offering alternative ways of solving challenges in numerous fields, such as the finance, supply chain management, law and many more [32]. There is a trend towards patient-driven interoperability, in which health data exchange is patient-mediated and patient-driven [16]. Many research works are focusing on exploiting the possibility of decentralization offered by the blockchain as technology in real-life use cases [17].

When it comes to the healthcare and the health-related data, blockchain can help to simplify the way how the parties involved in the health care industry exchange the data and collaborate between themselves. Many research papers and practical application were introduced, with blockchain as foundation technology. All of them are trying to overcome the data sharing challenges and the friction caused by highly sensitive data scattered across different centralized infrastructures [17]. Smart contracts, as an intelligent protocol in the blockchain technology, can be exploited to automatically achieve system confidentiality, integrity, and authenticity [36]

The researchers at the MIT Media Lab have introduced MedRec as prototype system to exploit the benefits of blockchain in the healthcare. The content-management prototype has improved permission mechanism for tracking which organization is able to see which medical records and, in that way, simplify the health information exchange. MedRec utilize the blockchain infrastructure to create an immutable chain of content, supported by decentralized network. They also included the concept called “smart contract” to execute business logic on the distributed layer and to program the representation that connects patients and providers [12].

Iryo Network are trying to consolidate the electronic health records and enrich the patient experience with unified health record system. They are moving towards standardizing health-data and supporting the AI & Big Data research performed on the collected health-related data [28].

A mobile healthcare system for personal health data collection, sharing and collaboration between individuals and healthcare providers, as well as insurance companies is presented in [21]. The presented system enables user to share data with healthcare providers to seek healthcare services, and with insurance companies to get a quote for the insurance policy and to be insured.

These systems reveal the possibility for practical implementation of decentralization in the field of electronic health records systems and they are justifying the decision to incorporate distributed layer and blockchain technology.

From technical point of view, the systems are built in different ways exploiting the technologies that the creators considered to be beneficial for their use cases.

Still, there is a practical need for general analysis of the components of the blockchain technology and the approach for adopting the technology by the participants in the ecosystem. In this paper, we try to explain the technical decisions that need to be considered when this approach is incorporated, by disseminating the components and analyzing their effect. Blockchain solutions must also be adaptive to opportunities and barriers unique to different national health and innovation policy, and regulatory systems [22]. It is crucial to study how blockchain technology can support and challenge the healthcare domain for all interrelated actors (patients, physicians, insurance companies, regulators) and involved assets [19].

The paper proposes an architectural overview of decentralized information exchange system. The focus is put on the information exchange between the healthcare providers and health insurance organization. We analyze different approaches in order to offer health-related data integrity and confidentiality, authentication and permission control mechanism, flexible access control of data by different stakeholders and enriched consent mechanisms. The approach that we present in this paper leads to automatization of different processes in health insurance organizations, related to using and accessing health-related data. With the introduction of “smart contracts”, many of those processes can be regulated and put in place without a human interaction, which can significantly reduce the cost, time and friction.

The paper presents a strategy to address the benefits coming from the distributed layer and blockchain technology and shows how this approach will improve the HIE processes, with focus of sharing health and insurance data between healthcare and insurance organizations.

The paper is organized in several sections. In section 2 we introduce specific health information exchange ecosystem and the challenges that it has, where we are expressing the need for overcoming specific challenges, such as the need for unified medical history records system and better cooperation between stakeholders. In the section 3 we introduce blockchain as a technology and explain how blockchain can help to overcome challenges present in health information exchange ecosystem. In order to analyze different approaches of distributed ledger and blockchain technology and discuss which are more beneficial for our eco-system, in section 4 we present the components of the blockchain approach. In the section 5 we focus on the decision to use Hyperledger Fabric as a specific blockchain platform and in the section 6, we describe the architecture of the blockchain-based approach. This paper should be used as a guide for adopting the blockchain technology, so in section 7 we present the first steps and initial setup that need to be performed by the stakeholders in the eco-system and what they need to perform in order the approach to be useful and beneficial for them. Use case analysis of the approach is offered in the section 8, and section 9 and 10 are dealing with the challenges of the blockchain approach.

2. Health Information Exchange Eco System

The wider ecosystem based on the interchange of health-related data is spreading into multiple sectors that need constant gathering and exchange of data to successfully cope with different problems that arise due to uninformed decisions or fraud attempts [15]. The stakeholders participating in the system include all parties related to creating, storing, or using any health-related data. On the highest level these actors are divided into:

- Individual
  - Service requester and service user, the ultimate beneficiary of the provided services;
  - Personal health information provider, including information from wearable devices such as fitness trackers.
- Healthcare organizations
  - Primary, secondary, tertiary healthcare institutions;
  - Auxiliary health institutions such as laboratories;
  - Emergency healthcare;
- Medication suppliers
  - Pharmacies;
- Health Insurance Organizations
  - Social health plan;
  - Work related insurance plan;

- Life insurance plan;
- Travel insurance plan.

The process of exchanging health information refers to the secure electronic transportation of clinical health information in form which is understandable and usable to both the sender and the receiver. If we try to structure and categorize the transactions, we will ?nd up with two transaction types. The first one is sending information to some registry or other system, and the other one is requesting for and receiving data from other providers and data holders. The goal of the processes can be also divided into two categories, enriching and expanding the patient?s health record and exchanging information between well known healthcare related entities with established business collaboration. The table offers a short overview of the different transactions and processes that one can find in the exchange of health information.

Table 1. Comparison of blockchain categories.

	Goal	**Outbound transactions**	**Inbound transactions**	**Inbound transactions**
Expanding and consolidating patients health record	The goal of this process is to locate scattered patients records, enrich the medical record, aggregate with existing records in the institution and keep them for longer use.	Providers of healthcare, (primary care providers) can broadcast a summary of examination to relevant EHR systems.(if any)	Retrieving a summary of a patient's current conditions from another care provider. Retrieving medication history of patients. Retrieving information from other EHR systems or countrywide registry.	Transfer of care from one primary to another primary healthcare provider.
Exchanging information between relevant healthcare institutions	These processes are initiated by the institution and they are intended to ask for or order some activity or service from another institution. If there is an already established EHR system, the institution can expand the patient?s record with the data of inbound transactions.	Sending referrals to specialists. Ordering tests to the laboratory. Sending prescriptions to medical supplier	Retrieving reports from secondary or tertiary healthcare providers. Retrieving laboratory test results. Retrieving reports of used medical supplies	Patient is referred from a primary care provider to see a specialist.

To be able to use any health service, the individual needs to have the appropriate type of health insurance plan. Multiple health insurance plans can be issued for the individual by different health insurance providers, covering different spectrum of health services. Each health insurance plan is defined using a health insurance policy that defines the terms and conditions including the types of health services covered, the cap expenses covered, and the right to any damage premiums. These health insurance policies may overlap in some areas, in which case the claim should be covered by multiple policies simultaneously. For an example, if the individual was injured during working, the insurance claims activated should be social health, work and life insurance. On the other hand, if the health issue happened while traveling, the medical expenses should be covered by the travel and life insurance plans. The available health insurance plans define the health services that can be received from the health service providers. Based on the treatment defined by the health service providers, the individual may need additional services offered from other medication suppliers, such as pharmacies that work with or without prescriptions depending on the medication necessary.

The actual type of medication that can be acquired is not only dependent on the issued therapy, but also on the active health policy, since some drugs may be covered while others are not covered by the insurance. On the other hand, the health policies are defined based on the overall health history of the individual including all services obtained from the health service providers and medication suppliers, but also individual health data recorded by personal devices such as diet and fitness trackers, blood sugar level and heart-rate monitors.

Since the ecosystem spans over several different institutions that are relatively sparsely interconnected both horizontally and vertically, the exchange of trusted data becomes an issue of high importance.

Normally the individual is tasked with the complete process of information transfer from one institution to the other, usually in the form of printed documentation that is issued by one institution per request and provided in another to obtain the service. This process is not only error prone and tedious for execution, it is also subject to several different fraudulent activities such as false insurance claims, intentional hiding of medical records or failure to provide the most appropriate treatment due to incomplete information.

A system that can support the transparent, yet trustful and confidential, interchange of data between the institutions can help overcome a wide variety of issues.

3. How Can Blockhain Help

To discuss the novelties that the blockchain technology brings into our use case and how we can substitute the centralized model and architecture of implementation of Electronic Health Records (EHR) and Health Information Exchange (HIE) systems we need to fully understand the challenges that those systems have.

The biggest challenge is the complex nature of the health-related data. The reason why this type of data is so special is because they are valuable personal information and subject to numerous security regulations and authorization policies. The systems which are dealing with health-related data must be aware of the consequences of their abuse and that strong access and authorization management mechanism must be applied. Basically, that justifies the reason why systems that electronically manage health related data, are trying to overcome the challenge by putting the data in isolated state on physical storage that is part of the infrastructure of the organization where many security policies and authorization control processes are applied [8]. They are following the centralized approach with keeping the data secured on one place behind firewalls and strong security. Blockchain relies on strong cryptographic techniques and strong security is embedded by default when this implementation approach is used. Blockchain can help in establishing authentication, authorization and membership services through a decentralized network, improving any process that requires permission-control and security mechanisms.

Interoperability is arising as another problem, since there are many different implementations of EHR systems [23]. The process of making systems which are built and implemented differently without unified concept in mind to communicate and collaborate with each other is a difficult and complex task. The process demands the need to build integration layer and put communication protocols in place. Even then, the challenge of portability and secure transfer still exists. Distributed peer-to-peer network is the backbone of the blockchain technology. The EHR systems can have their representative peer included in the eco-system and in that way, they can easily connect and collaborate with the rest of the participants.

Bringing decentralization as a concept close to HIE and EHR systems can sound controversial [9], the appearance of the blockchain as a technology can unlock the true value of this concept. Friction that exists when data with great sensitivity as health-related data is transferred from one place to another, can be significantly reduced and eliminated when decentralization is incorporated in the solution. By putting references to health-related data on the blockchain infrastructure, all participants in the network are able to access and use them with proper permissions and in secure manner. On the other side, the owners of the health-related data can track the changes and have control of which entities should have access to those references by participating in the consensus that proves the validity of the transactions.

The blockchain technology is enabling the use of distributed ledger. The ledger of transactions, in our case the references of health-related data to different data storages, is not stored on centralized server, instead each of the participants holds a copy of the ledger. By owning a synchronized copy of the ledger, the participants in the eco-system are involved in the decision-making processes. Only with their consent, valid transaction in terms of updating or using the references of health-related data can be stored on the ledger. While the control of the centralized databases and storages are task for their owners, in a distributed network implemented by using blockchain, all the interactions to the ledger are synchronized and approved by the participants in the eco-system, eliminating the need for authority that will take care of the integrity and validity.

Blockchain, along with the decentralization concept, brings technological solutions to consolidate the context of transfer and easy access of the data. It can connect widespread particles of data, stored in the storage infrastructure of some centralized implementation and significantly reduce the cost of intermediation. When it comes to our use case, health insurance plans and coverage can be improved and automatized and taken to whole another level. Blockchain can transform the patient records into rich and expanded health history by connecting the different data storages. That rich and easily accessible data portfolio can be used as reference for insurance organizations.

Health insurance organizations can secure accurate claim coverage, they can reduce the effort of coordination between the parties involved and they can apply business logic and policies to reduce the human resource involvement.

4. Components Of The Blockchain Approach

The theoretical definitions of the blockchain, the discussions and research about the potential and opportunity of this technology and the applications in the other fields, such as financial industry, are increasing the awareness of the benefits and the impact. However, to justify the decision to use the blockchain technology we need a general basis of understanding how the infrastructure works underneath. We analyze and cover the fundamental principles and components behind the technology in order to discuss the impacts they will have on the information exchange processes between healthcare providers and insurance organizations. In the following part of the paper, we address the key components of the blockchain approach, that will serve as a reference and lead us to better understanding of the approach to our use case and eco-system.

4.1. Consensus as a Group Decision-making Process

When we are dealing with system that has an absence of central authority, particularly noteworthy is to discuss about how the involved entities can agree on validity of information and how they can agree on the decision to put that information in the distributed ledger and use them as single source of truth. In our case, with the blockchain based approach, it is necessary for the participants which are affected by the process of adding new information to evaluate and agree about the correctness of the information before that information become incorporated and immutable. In other words, there must be some dynamic way of reaching an agreement between the affected participants. They must make a decision based on different parameters, that transaction between two peers in the system is in the best interest for all participants. That general agreement and group decision-making process is defined as a consensus. The process of achieving consensus is important in the blockchain approach and will be subject of discussion in different parts of this paper.

4.2. Categories of Blockchain Approach

With the introduction of blockchain as revolutionary technology and its first real implementation in face of Bitcoin cryptocurrency system, many prototypes are trying to exploit the possibility to gain trust between participants in the system, without the special need for them to know each other. Since the blockchain technology offers a way how to overcome drawbacks of centralized approach in health-related systems, mentioned previously, we must discuss the level of decentralization that is needed [18]. Following the context of this research paper and the use case, before we start analyzing how far should we go with the decentralization approach, we need to define the categories and types of blockchain networks [6].

- The public blockchain as the name implies is shared among anyone in the world and it's open for everyone to join. They are proud representative of the idealistic way that the blockchain brings as concept and in the literature are generally considered as "fully decentralized.";

- Consortium blockchains are modification of the public blockchain, and the main difference is that pre-selected set of nodes/participants are chosen to be carriers of the consensus process instead of having every node to participate in the consensus process as in the case of public blockchains;
- The private blockchain is a blockchain where we can find entity which grants and stores permission to be part of the network. As opposite of the public blockchains these blockchains are only accessible to individuals who has the rights to use it.

Table 2. Comparison of blockchain categories.

	Main Characteristic	**Main advantage in our use case**	**Main disadvantage in our use case**
Public blockchain	Fully decentralized Permission-less peer-to-peer network Representative of the true concept of blockchain	Easy access for any participant to join the community.	Revealing valuable data to the public. There is no built-in component for managing permissions to manipulate with assets. They should be implemented by programming. High and unpredictable transaction fees Performance
Private blockchain	Presence of issuing authority that grants and stores rights of using assets	Permissioned ecosystem suitable for enterprise use cases of blockchain. Restriction on who can participate in the network. Increased performance than public scope, due to centralizing the trust authority	The approach moves away from the decentralized characteristics that blockchain offers.
Consortium blockchain	Pre-selected nodes are carriers of consensus process	Different nodes run by different stakeholders can be part of the decision making and consensus process. Offer more decentralized approach than the private blockchains	Complex hybrid approach with highly trusted entity in the private and power-consuming consensus in the public blockchain.

To explain the decision which of these categories of blockchain are more suitable for our use case, we will depict the characteristics in Table 2. To summarize, each of the categories brings certain advantages and disadvantages when incorporated in the context of our use-case, but this paper intention is to pick only the most suitable one. The decision should consider several main challenges that affect the health information exchange process [11]:

- The performance of the process;
- authorization and permission-to-use the assets due to the nature of the health information;
- involvement of different peers (but under the umbrella of specific organization) in the process of verification and validation
- the subtle closeness of the system due to the need of tightly controlled environment.

Having these challenges in mind, one blockchain scope that is most promising for fulfilling our experiment is the consortium blockchain category. It has increased performance when compared to the public blockchains, and tightly controlled permission environment which consists of multiple organizational authorities [37].

4.3. Channels of Communication and Collaboration

Channels components are responsible for defining collaboration in terms of transactions with privacy and confidentiality and their purpose is to achieve common ground for manipulating with assets provided by the participants in the network. Within the channel of collaboration, each of the participants has proven belonging to specific organization, rights and privileges to act on specific asset. Participants use the collaboration channel for updating the ledger and read or modify the assets in accordance to their rights and permissions. In our specific use case, to simplify the access management and authorization control, and additionally to establish separation of concerns, there will be two channels defined, one for the insurance assets and the other for health-related assets. The participants depending on their intention will be using both channels with different flows. The participant will still be part of the same eco-system, but the separation of channels will reduce the complexity of the data flow and allow us to build business logic tied only to specific channel.

4.4. Ledger

The ledger is component of the system, which is responsible for recording all transactions submitted by the participants in the ecosystem. The ledger consists of immutable sequenced blocks and each block contains multiple transactions. The ledger has these two characteristics in the system that we are analyzing:

- Each participant maintains a copy of the ledger.
- Each channel has only one ledger, which is used to update some asset produced by the participants in the network.

In our approach, to separate the concepts and the data flow, we have two channels of communication and collaboration, one for the insurance assets, the other one for health-related assets. Therefore, there will be two ledgers for each channel. The health-related ledger will be used for assets provided by the individuals (related to diet and valuable information from wearable or other sensor devices), health-care organizations and the medical suppliers. The insurance ledger will be used from the insurance organizations, but it will contain partial health related data and access by healthcare organizations as well. In this way, we can increase the performance of the transactions verification, since the ledgers will have as much amount of data as needed to satisfy the endorsement policy when achieving consensus.

4.5. Participation of Peers

Before we discuss about how participants can join the network and gain better overview of which blockchain category (public, private or consortium) should bring more benefits to the use case let's first analyze some of the main actors.

1. Health insurance organizations with different types of personas (multiple types of participants coming from same organization with/without the same permissions to use the distributed ledger). Different assets can be produced from the insurance organization such as, terms and conditions for specific insurance plan, the coverage options and duration of insurance plan, etc. The insurance organization will use the channel for accessing health-related ledger to query the health condition assets related to potential insurer and define the price of the insurance plans. On the other side, the healthcare organizations can collaborate with the insurance organizations for justifying or initiating claim coverage for their patients.
2. Healthcare Organizations with different types of personas (multiple types of participants coming from same organization with/without the same permissions to use the channel). Different assets can be produced from the healthcare organization such as, medical history of the patient, referrals, lab results, scanning results, diagnosis, prescriptions, etc. The healthcare organization will use the distributed ledger to consolidate all health-related data for the patients from different places and to provide seamless interoperability with other healthcare providers.
3. Individuals can benefit from this eco-system in two ways. First as patients. Blockchain based approach can bring enriched medical history and can transform the health records owned by the healthcare organization with given consent by the patient. Information can be gathered from multiple places, validated and used to make better diagnosis and analysis. Health records can be easily shared and transferred to third parties and guarantee the patient decreased friction in providing details to another healthcare organization. Another role that they can take is the health insurer. If they have active insurance coverage from a health insurance organization that is part of the system, the claim coverage can be taken to another level. The individuals can propose claim coverage and refunding based on the health-related data and insurance plan and if the parties involved agree on the validity, the process is performed automatically.
4. Medical Suppliers such as pharmacies can use the system to override the paper prescriptions (that can be easily altered and subject of a fraud) and communicate directly with the healthcare organization about the validity of the prescriptions. They can plan better, attack the forgery and fraud processes with goal to significantly reduce the cost of medical supplies.

4.6. Permission Management

In the world of electronic health information, health data is not just private secure piece of data, but also personal data related to specific patient's medical history. That's the main reason why the health-related data need to be protected against unauthorized access or corruption. Participants in the HIE process that generate health data can have confidence in the infrastructure of the blockchain system because one of the things it brings as a revolutionary technology is the automation of the data integrity. In addition, giving the possession of personal data should also define the decision-making power of who can manipulate with it. The membership management layer is a component which is responsible for defining the members of specific domain, organization and channel of collaboration and to communicate with other membership providers in order to clarify the ownership of the data. They are also responsible for access privileges, roles and permissions in regards of the context of the network and the channel of collaboration. Specific rights and membership allowance are revoked and handled by specific authorities. In our case:

1. Health Care Institution Authority
2. Health Insurance Institution Authority

Each channel of collaboration is a subject to authorization policy which is using the identity of the participant in order to establish the rights and privileges based on the membership providers. Each of the providers certificate the participant in order to gain appropriate access to the resources.

When it comes to the scope of the blockchain and how the participants can access the ecosystem, accent was put on the need for controlled permission environment and restricted accesses. Each of the organization that can produce assets in some way that are necessary for the functioning of the blockchain based approach, should provide entity or authority that can issue policies for using the assets (in any form, reading, writing or changing). When the peer that is participant in the system, has the security policy and permission to manage the assets, it automatically becomes endorser in the process of verification of validity of specific transaction and carrier of the consensus process. The consensus is important due to the fact that it must be reached in order to initiate update of the change. In our use case, one individual can bring assets to the network in form of health-related documents or personal health information data streams, only if consensus is reached with the other stakeholders, such as healthcare institutions representatives, medical suppliers, etc. One healthcare institution can see health-related information owned by other healthcare institution, only if it has permission to join the system and to read those specific assets.

4.7. Smart Contracts

The smart contracts are carriers of the business logic of the solution. They run on the peers (nodes) in an isolated environment (docker containers) and manage the assets which are hosted on the ledger (world state and blockchain part). Smart Contracts are the executors of the rules and the policies initially accepted by all the participants in the ecosystem.

The power of the blockchain solution is in the fact that each of the participants contains copy of the smart contracts and they can run them on their own ledger and after that compare the result with the results of other peers via the collaboration channel, to achieve consensus. The outcome of executing the smart contract on the ledger must be endorsed by the key participants (every participant executes it successfully in its local world state, signs the proposal and returns it back) in order to be accepted as ledger update. In our use case, the smart contracts will be used in many cases, from read-only medical history queries to decision if one claim proposal should be refunded or not. The endorsement policy which is part of the consensus mechanism is closely related to smart contracts. Every smart contract (chain code) works in concert with its endorsement policy which is specified at the time smart contract (chain code) is instanted.

5. Using Hyperledger Fabric as Blockchain Platform

The first step in designing the architecture of the decentralized platform is to select the blockchain platform which will serve as underlying technology to implement all the components that were discussed previously. The blockchain platform should satisfy the initial requirements of our use case, in most complete manner.

In Table 3, we can see the main characteristics of some of the blockchain platforms that are popular now and which effects should they bring if we are using them as platform for developing our use case [10], [34], [31], [1].

Additionally, there is an information about which consensus algorithm is used by each of the platform and in Table 4 we can notice short explanation about them and some of the crucial features that bring those algorithms to the use cases when they are applied [25], [20], [14], [35].

5.1. Performance and Scalability

As we already mentioned, due to real-time availability of information and health related data included in the system, performance is a requirement that we must consider in our use case. When it comes to Ethereum with the combination of Proof-Of-Work algorithm used for achieving consensus, we stumble upon performance problems due to heavy work and power consumption needed to sustain the permissionless and public network. The price paid in terms of performance drop for permissionless and public characteristics of the potential network is not worth in our use case, since we don't need to apply them. The performance of platform intended for private networks such as Hyperledger Fabric, with pre-defined set of carriers of consensus process, is on satisfactory level for our use case. The disadvantages of consensus algorithm that is used by Hyperledger Fabric are related to its semi-trusted environment, due to existence of permission system and the private nature of the blockchain. Performance decrease will happen if more than 20 peers are included in the consensus achieving process. [30] But, considering the initial requirements, these drawbacks of the platform and consensus algorithms are not playing huge role in our experiment.

5.2. Authorization and permission-to-use the network and assets

The Hyperledger Fabric is intended for building networks where the assets are owned and managed by a group of identifiable and verifiable institutions [26]. In our case, those institutions are healthcare and health insurance companies, as well pharmacies and medical suppliers. The reason why Hyperledger Fabric is better choice than Ethereum for our use-case is the infrastructure of permissioned network that it offers, where all the organization and peers are verified before executing transactions. They can operate in specific collaboration channel if, and only if, they have certificate issued by a membership authority. On the other-side, in Ethereum and public networks, permissions to participate don't exist, everyone can join the network [7]. By using Ethereum source code to implement network, Etherium can be used in a controlled setting as well (this is a rather common approach for Ethereum based start-ups focusing on B2B).

Table 3. Comparison of blockchain platforms

	Main Characteristic	**Smart Contract Code**	**Consensus Algorithm**	**Effects of using in our use case**
Ethereum	Built by Ethereum developers Most mature and first blockchain platform that introduce the smart contracts Permission less approach	Solidity	Proof-of-Work	Mature smart contract programming language that offers smooth development with strong community and broad documentation. Main disadvantage is the use of brute-force look-a-like consensus algorithm that is intended more for public blockchains. The performance and scalability will be the main challenges. The public scope of the platform moves away from our initial idea of closed and controlled private blockchain.
Hyperledger Fabric	Built by Linux foundation Consensus is achieved on transaction level Less mature than Ethereum Complex permission module	Go, Java	Proof-of-Stake based mechanisms Byzantine fault tolerance	The endorsement and consensus are achieved on transaction level meaning that all parties that have permissions and participate in the collaboration channel are responsible for the validity and achieving the trust. Increased focus on permissions system and membership service providers More layers of abstractions in the development process and modular architecture can be easily applied to our use case. Solves performance scalability and privacy issues, perfect for health-related systems.
R3 Corda	Permission based network with strong control on communication points Specialized for financial industry	Kotlin, Java	Transaction level consensus between the participants	Similar and complement to Hyperledger Fabric but more simplified with possibility of easy implementations of out-of-the-box functionalities. It has many unnecessary features that are not part of our initial considerations.
Sawtooth	Supports both permissioned and permission-less networks.	Supports different programming languages	Proof-of-Elapsed Time	The consensus algorithm that is introduced by this platform is not mature and not properly implemented yet. When it comes to security Sawtooth has approach based on roles and permissions
EOS.IS	Built by Block.One and came into the market as a competitor to the Etherium ecosystem. The platform raised 4 billion dollars in the initial coin offerings.	WebAssembly languages like C++, Java and Python was the	Delegated proof-of-stake model	The smart contracts can be written in C++, Java or Python. The platform does not require learning a new programming language. The platform solves a lot of issues that the other platforms experience such as problems with scalability and transaction fees. Main disadvantage is the centralized model of decision-making and achieving consensus. Same as Ethereum, the public scope of the platform moves away from our initial idea of closed and controlled private blockchain.

Table 4. Comparison of some of the most popular consensus algorithms

	Main Characteristic	**Blockchain category (permissioned/ permissionless)**	**Achieving consensus**	**Effects of increasing participants in the consensus**
Proof-Of-Work (PoW)	Fully distributed consensus mechanism The original consensus algorithm introduced by Satoshi Nakamoto. Each of 'the participants that have the job to secure the network needs to prove their intent by doing some work (to solve a complex mathematical problem that requires huge computational power) in order to mine new blocks of transaction Huge computational power required	Permissionless	Slow	None
Proof-Of-Stake (PoS)	Opposite in the manner of exploiting computational power due to alternative approach. The algorithm is based on coin stakes that node holds to the network as a proof for creating new blocks.	Both	Fast	None
Proof-Of-Elapsed Time (PoET)	The process behind is related to waiting specific amount of time from each participant in order to mine new block The first participant that finish the waiting process is chosen to be the leader	Both	Medium	None
Byzantine Fault Tolerance	Few pre-selected nodes that forms the consortium and they are communicating with each-others to achieve consensus. Hoch transaction throughput	Permissioned	Fast	Decreased performance
Ripple Consensus Algorithm	Byzantine Fault Tolerance based Each channel has its own federated validator that sorts the messages in order to achieve trust	Permissioned	Fast	None

5.3. Achieving Consensus by Using Hyperledger Fabric

Consensus process in Hyperledger technologies, consists of three phases. First phase is called endorsement and it is closely related to "smart contract" component (called chaincode). Before the network is built and put in operating state, endorsement policy must be configured and defined. With other words, by using this endorsement policy we define which peers have rights to execute which transaction. This phase is also called the execution phase, because transactions are executed by using the smart contract layer. Depending on the endorsement policy, in this phase, transaction proposal is sent to some of the peers which are defined as endorsing peers and the channel is waiting for their response. There can be a case, as part of the separation of concerns, that peers even though are part of the blockchain network are not included in the endorsement process and specific business rules (smart contracts) are kept hidden and private from them. In our use case, that can happen when two healthcare organizations are exchanging information. In that case, all of the insurance organizations that participate in the network will not be included in the endorsement process.

The second phase of the consensus process is called ordering phase, because it involves the so-called orderer entity. The responsibility of the orderer as part of the consensus mechanism affects the order of the transactions. It's a keeper of the order and its functionality is related to making sure that each of the participant has the same order of the list of transactions on its ledger. This phase happens only if all endorsement peers signed the transaction.

The third phase comes right after the ordering of the transactions and it's called validation phase. In this phase, all the peers participate in the process because the process involves updating the ledger with new transaction. They validate the results and apply the changes in their copy of the ledger.

6. Architectural Overview

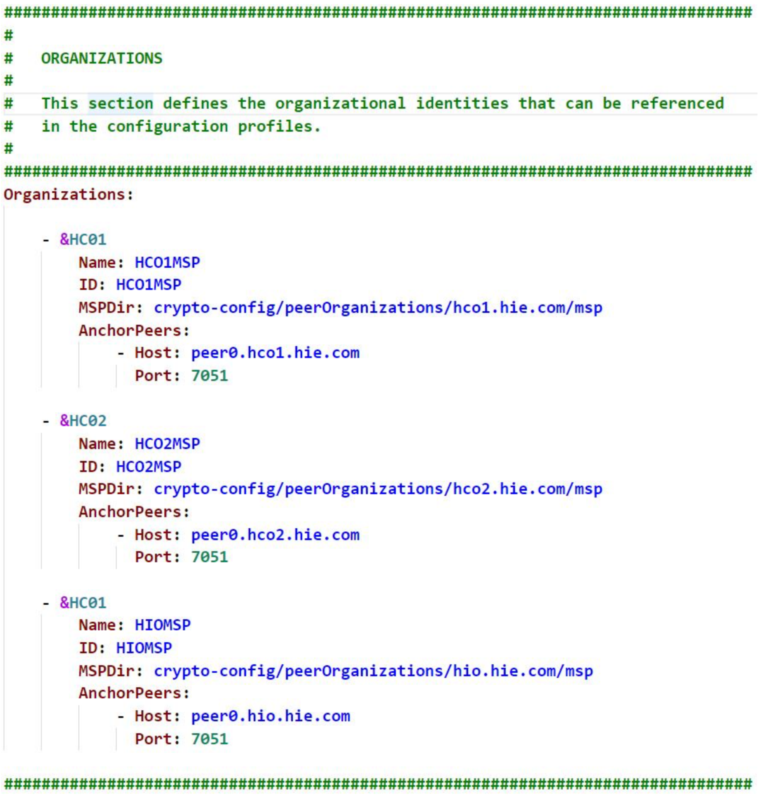
Each participant, defined as node in the network, has two layers included in the architecture. The first one is the blockchain layer, which consists of many components that we already discussed, and this layer serves as trust-less network that can provide agreements and consensus through endorsement of smart contract outcomes [28]. The second layer is the application layer and this layer is responsible for all application logic and data that is not needed to be subject to verification of validity. The application layer can interact with the blockchain through transactions. Defining the components of both layers is crucial for the architectural design [38].

6.1. Defining the Assets, Peers, Organizations and Channels

The starting point of configuring the blockchain based approach is to define the assets, peers, organizations and channels. Hyperledger Fabric technology offers possibility to configure these components with different software tools, scripts and configuration files. After initializing our network, our experiment should consist of:

- healthcare organization 1 with one peer – HCO1;
- healthcare organization 2 with one peer – HCO2;
- health insurance organization with one peer HIO
- individual represented by one peer.

After defining the peers and organizations, we need to configure the channels and their endorsement policies (Figure 1). Every participant should communicate with the others on channel that is supported by related ledger. Each of the peers are configured to be registered to certification authority server, which is responsible for granting them specific permission for performing actions in the system.



```
################################################################################
#
#   ORGANIZATIONS
#
#   This section defines the organizational identities that can be referenced
#   in the configuration profiles.
#
################################################################################
Organizations:

    - &HC01
        Name: HCO1MSP
        ID: HCO1MSP
        MSPDir: crypto-config/peerOrganizations/hco1.hie.com/msp
        AnchorPeers:
            - Host: peer0.hco1.hie.com
              Port: 7051

    - &HC02
        Name: HCO2MSP
        ID: HCO2MSP
        MSPDir: crypto-config/peerOrganizations/hco2.hie.com/msp
        AnchorPeers:
            - Host: peer0.hco2.hie.com
              Port: 7051

    - &HC01
        Name: HIOMSP
        ID: HIOMSP
        MSPDir: crypto-config/peerOrganizations/hio.hie.com/msp
        AnchorPeers:
            - Host: peer0.hio.hie.com
              Port: 7051

################################################################################
```

Fig. 1. Configuration file for organization and peers

6.2. Defining the Data Flow

Considering our eco system, major architectural question that needs to be answered here is the decision which data should be placed on-chain and what should be kept off-chain. That decision will affect performance and flexibility.

Before we present the transaction and data flow, we need to discuss which data are subject to negotiating and verifying by the consensus of the network and should be stored on-chain, meaning that they will be stored in each copy of the ledger of the peers, and which data should be stored off-chain meaning that it will be referenced by the negotiation process. In blockchain approaches, there are two ways how to store the data, the first one is to add data into transactions, like Bitcoin. And the second one is to store it as variables into contract storage as Ethereum. Both ways, store and update data by submitting transactions to the blockchain layer.

What we plan to do in our use case is to find the most suitable way how to connect data stored in traditional relational databases and kept in organizational storage servers to the blockchain network. We designed a way how to establish bridge between the blockchain layer and the off-chain data, by using references, indexes, meta-data, hashes or critical information as on-chain data on the blockchain that will point to the real data needed for achieving consensus. As we mentioned, the real data can be placed somewhere in the infrastructure of the organizations that participate in the blockchain network, no matter if it's cloud solution, physical servers or a public storage.

6.3. Writing the Business Logic

As we mentioned before, the smart contracts, or with the terminology of Hyperledger Fabric, the "chaincode" is responsible for executing the business logic in the blockchain based architecture [30]. As a step towards defining the approach, we should consider developing all the necessary smart contracts that will perform the intended actions in the system. For example, how an injury can be covered by a health insurance organization or how one health care provider can grant permission for using health related data to another health care provider, or how a patient can transfer medical files from one organization to another. All these processes should be covered and implemented by using smart contracts.

6.4. Application and Integration Layer

The blockchain based architecture should contain a layer where the data present at the off-chain storages can be used as a feed to populate the blockchain network with data. Basically, all the assets that can be produced by the participants in the network should be indexed, referenced or hashed and stored to the ledger of the channel as immutable data. This process should be done as initial phase of seeding the blockchain network. The plan in our use case is to build integration layer in form of API calls. That integration layer should serve as a bridge between the organizations and individuals on one side and the web system of our use case together with the blockchain layer on the other side. Individuals can access that integration layer by using distributed application and in that way execute transaction on the blockchain, and organizations can build their own API layer in order to transfer the needed data. The overall architecture and communication can be seen at Figure 2 [39].

7. Initial Setup

After we discussed about what we want to achieve and analyzed how we want to do that and why, the next step is to bring the participants into play and assume their effort to make this blockchain based health information exchange mechanism, feasible and beneficial.

Individuals are the central point of the ecosystem and they are the ultimate beneficiaries from the services, features and functionalities that this decentralized way of health information exchange should provide [4]. Using 2 as reference, we can say that the interaction of the individuals with the blockchain solution is the distributed application. The distributed application offers the individual different types of services, from accessing their health insurance and broad information related to it, to real time access to medical history, lab results, prescriptions, reminders, etc. The distributed application act as a bridge between the individual and the blockchain layer. The individuals can initiate and demand different types of actions, such as claim approval and payment, transfer of data from one institution to another, etc. The system can also detect when specific actions are needed and can initiate them instead of the individual, asking only for a consent.

The efforts of the patient in order to keep the prototype alive and beneficial on highest level can be:

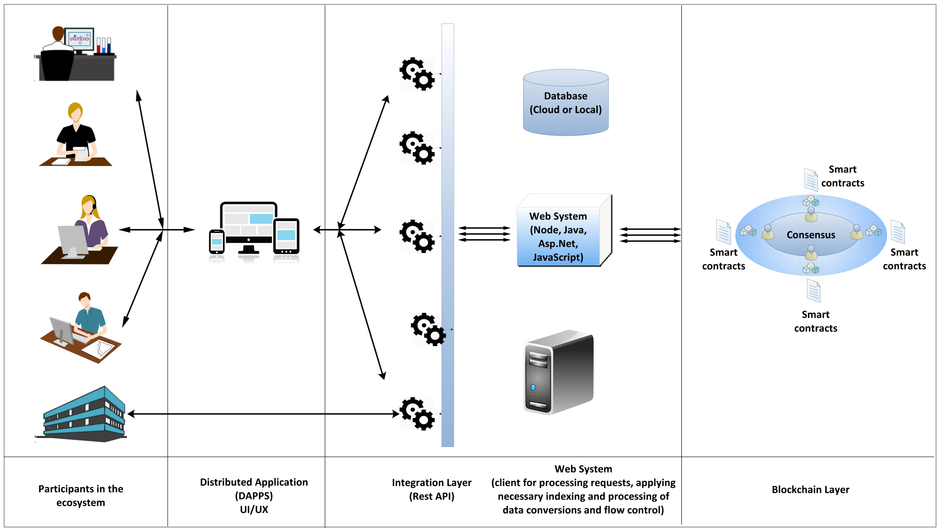


Fig. 2. Blockchain based approach

- Registering an account in the system;
- Feed the network with different types of data. Authorize the prototype to retrieve information from external sources, such as sensors of wearable devices, insert diet and meal plans, period and types of physical activity, etc.
- To seed the blockchain layer with relevant health related data, the healthcare organization that owns the medical records of that specific individual should also be part of the ecosystem. The membership management component of the healthcare organization should authenticate the individual and verify that it is the owner of the health related data. With consent of the individual, that healthcare organization can synchronize the medical records of the individual and feed the blockchain layer with them. From that moment, the individual and the healthcare organization will be always present in the endorsement process and they will always be part of the decision-making process regarding who can control and process the related data stored on the blockchain.
- To seed the blockchain layer with relevant insurance related data, the health insurance organization that owns the insurance policy should also be part of the ecosystem. The membership management component of the insurance organization should authenticate the individual and grant him permission to manipulate with its data. With consent of the individual, that healthcare organization can synchronize the terms and conditions, the duration of the insurance and details about the coverage of the individual and feed the blockchain layer with them.
- After seeding phase, the other actions are related to initiating some service provided by the prototype.

The organizations that are part of the ecosystem, no matter if they are healthcare organizations, health insurance organizations or medical suppliers have two possible ways how to bridge the collaboration gap with the blockchain layer and them. The first way is to access the blockchain layer via the interface of the distributed application. The interaction should be similar as the one which the individual is performing. The actions that can be performed by using the distributed applications are related to registering, setting up membership module and access control mechanism for other participants to ask for permissions to access, adding peers that are part of that organization and feeding the blockchain with relevant data.

To simplify the interoperability between the organizations and the blockchain based solution, the organizations can access the blockchain network directly through the integration layer that is part of the architecture. When it comes to healthcare organization, the Electronic Health Records (EHR) systems can exploit the API calls that are part of the integration layer of the blockchain based solution, to communicate in both directions. Either to retrieve health related data that is not present in the medical record of specific individual, thus enrich the medical history or to feed the blockchain with data that is relevant for the provided services of the blockchain based solution. The same can be done for the other organizations that have software enterprise solution to store and manage health related data.

8. Use Case Analysis

In the previous sections we discussed about the components of the blockchain technology and how can we exploit them in the field of electronic health records. We were considering and evaluating blockchain platforms and consensus algorithms, so we can make the right choice to fulfill the requirements of our use case and satisfy the needs of our eco system. As discussed in section IV, Hyperledger Fabric as a blockchain platform is a good starting point for the practical part of the research. In the next parts, we will analyze two use cases by using sequent diagrams and we will see how the data and the information should move across different components (represented as lifelines) and how the participants can benefit from using this approach. The user scenarios we have chosen to represent the capability of the solution we consider in this paper, focus on the exchange of health data to health insurance institutions and the use of a health insurance plan. The reason for this emphasis comes from the complexity of the workflow, which includes conditions that need to be met and the involvement of multiple actors for a particular request to be approved or a solution to be proposed by the system itself. We should keep in mind that the solution encourages facilitated communication between different entities, if the health insurance companies are not part of that entity set, then the solution will have the same architecture, but with simplified parts of the system in which the conditional logic for decision making is embedded.

8.1. Sequent Diagram for Claim Coverage Proposal Coming From Peer that Represents the Insurer

If the components of the solution described above are initialized and set, the system can execute different types of transaction and data flows, so let's analyze the process of asking for refund of claim covered by insurance plan which is issued by specific health insurance organization insurance. The transaction and data flow is depicted at Figure 3. The process covers proposal for access of health data owned by specific healthcare organization and activating endorsement policy, written in the form of a smart contracts to evaluate the truth about the health conditions and terms and coverages of the insurance plan.

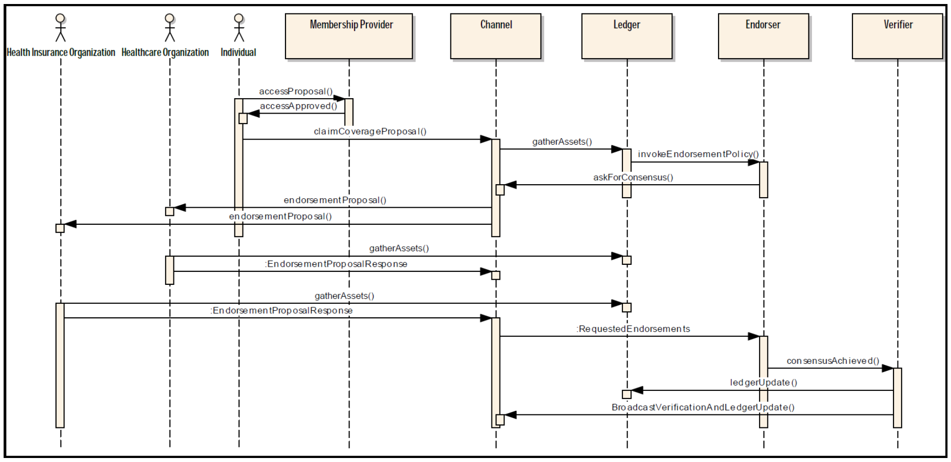


Fig. 3. Sequence diagram of claim coverage proposal

Hyperledger Fabric as a technology platform can help in couple of segments for fulfilling the requirement, as we already discussed in the previous sections. First of all, it's a platform for creating permissioned network of participants. That means that each of the members that participate in the system, should have been pre-configured as valid peers from specific organization and with proven identity. With other words Hyperledger Fabric is a platform that can offer configuration of peers and organizations and permissions that complies with data protection regulations. The healthcare providers, the insurance providers, the patients and the other participants should have their own peers as representatives in the network which will execute their business logic. If satisfying endorsements are given from both parties affected: the healthcare provider owning the health information and health insurance provider owning the insurance plan for the individual, a consensus is made and assets in the ledger are updated, meaning that the claim is reviewed, accepted and refund is approved in a smart and automatic way reducing the need for a human interaction.

When we are talking about endorsement policies, Hyperledger Fabric can offer configuring how many and what kind of combination of endorsers are required for considering one transaction as valid. That is part from the consensus algorithm that is used as a backbone for acquiring distributed trust.

Each of the participant has their own copy of the ledger and own copy of smart contracts, so the process of endorsement is nothing more than executing smart contracts from all parties involved in the process on their ledger and sending the outcome results to the channel in order to verify the truth and achieve consensus.

8.2. Health Information Exchange between Healthcare Providers

In this scenario, shown at Figure 4, an individual that has health information owned by specific healthcare organization asks for health information exchange with other healthcare organization. In other words, this sequence diagram explains the process of adding read permission to healthcare organization which is not an owner of the health information related to the individual. When the individual initiates health information exchange, the channel checks the ownership of the health information and checks which healthcare organization should have permission to read them. Endorsement is given from both parties and the verified proposal is executed as a ledger and membership provider update. From technology aspect, this flow is very similar to the previous one.

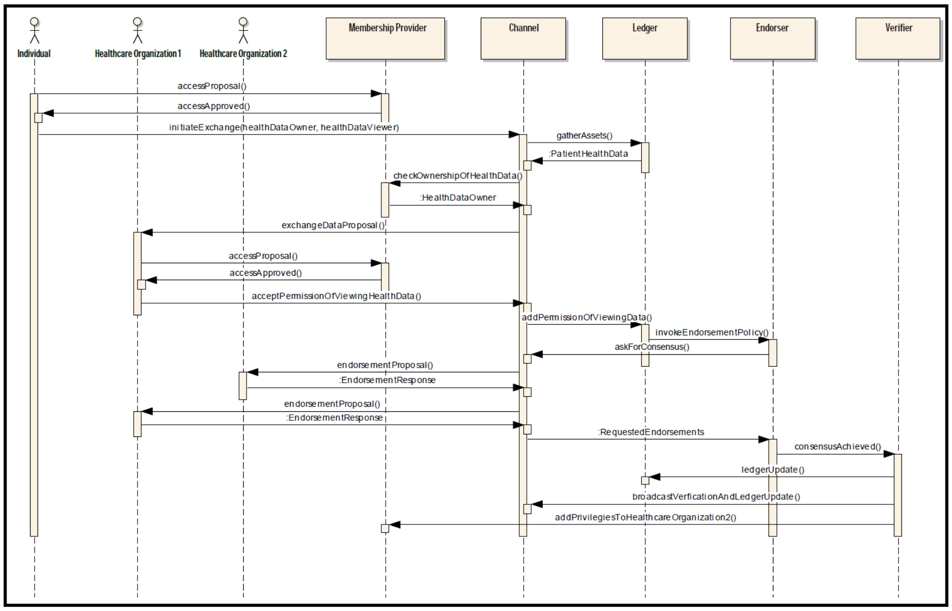


Fig. 4. Sequence diagram of adding read permission to another healthcare provider

Hyperledger Fabric offers configuration of peers and organizations and a channel where they can communicate with each other. The consensus algorithm that includes endorsement policy is helping the process to validate that one peer can have read permissions on some specific data in the blockchain.

9. GDPR

Main topic of this technical paper is the process of exchanging health-related data. When we are discussing about systems where personal data are being processed, then we must consider the compliance with the General Data Protection Regulation (GDPR) [5]. GDPR comes into play when there is some kind of "processing" of personal data. Every information that can identify, directly or indirectly, a data subject which is identifiable natural person, is considered to be personal data. The personal data that can be in form of an identification number, location data, name of the data subject, etc. The "processing" of personal data is defined as operation or set of operations, that can be automated or not, such as storing, structuring, organization, adaptation or alteration, retrieval of data, etc.

There are two very important terms that needs to be mentioned and discussed, the role of the data controller and the role of the data processor in the GDPR. The controller of the data is some entity which states the purpose and the means of the processing of personal data and that statement is determined by legal legislation or laws defined by the legal authority in the country. When there is some entity which process the personal data on behalf of the controller, then that entity is considered to be the data processor.

In the blockchain based approach of defining a system for exchanging health related data, there is no hierarchy, instead every participant is equally responsible for processing of data. In the blockchain system, each of the participant is data controller and it is obligated to comply with the GDP regulation.

One of the main principles that will come into effect with the GDPR is the demanded transparency for the processing, storing and exchanging personal information. With other words, the individual (data subject), can demand the controller of the data, information about all kind of details regarding their personal data. As we are already aware, there is an absence of central authority, so that is certainly a challenge that the blockchain based systems will face to become GDPR compliant. However, the structure of Blockchain technology brings unique possibilities to overcome these challenges and bring transparence and extended logs regarding the access to the distributed data. The transparency and tracing can be achieved by using the characteristics of the blockchain network.

The blockchain network can be used to log every access of the data by the participants in the network. That logging mechanism can serve as an immutable record of health-related data exchanges between parties and the data subject can always control and monitor where their personal information is used, and by whom.

The combination between GDPR and blockchain systems can be a subject to a lot of discussion and probably they do not fit together, keeping in mind the fact that personal information is scattered across peer-to-peer network as a part of blockchain solution. Blockchain is a distributed database with strong encryption and security mechanisms, but still individuals don't know where data is stored (distributed environment) and they don't know who manage their data. On the other side, in many ways the blockchain can be used as an ally and a partner when it comes to overcoming some of the challenges of GDPR obligations.

What blockchain can offer when GDPR comes into play is ways how to solve transparency in data portability, traceability of data usage and many other details related to the use of personal data, improved consent mechanism and management, etc. However, there are many challenges that appear because of the characteristic of the blockchain. Right to be forgotten is one of them. The Table 5 shows details about some of the GDPR obligations that affect the blockchain systems and how can be solved.

One of the most promising thing that can be done in blockchain systems regarding the GDPR compliance is removing the personal identifiable information from the stored data. That can be easily done by encrypting the indicators that identify the data subject and in that way the controller shall not be obliged to maintain, acquire or process additional information [13].

Table 5. Some of GDPR obligations seen through eyes of blockchain solution

GDPR obligations	**Main characteristics**	**Blockchain based systems**	**How can be solved**
Right to be forgotten	The data subject has the right to obtain from the controller the erasure of personal data concerning him.	Key characteristic of blockchain is immutability of stored data. It is the reason why this obligation is a challenge in the blockchain based systems.	Smart contract containing all the data subjects which triggered the right to be forgotten should forbid processing of data related to forgotten subjects. Instead of erasing the data, encrypting the personal data and erase the key used.
Transparent information and data traceability	The controller shall take appropriate measures to provide information about any form of transfer and communication relating to processing to the data subject.	One of the key characteristics of blockchain is absence of central authority which makes difficulty to track details about the controller, propose and the details of the data processing.	Implementing logging mechanism that will utilize the immutability and transparency of the blockchain network. When the personal data is used by specific controller or processor, the access is logged together with all sorts of details. That log can serve as a place for satisfying the needs for information regarding the data flow.
Consent management	Also called lawfulness of processing. The data processing is considered to be lawful if the data subject has given consent for the processing.	In the permissioned blockchain networks, such as those implemented by Hyperledger Fabric platform organizational authorities exist that grant permissions and right to access.	Smart contract can be trigged to forbid the use of data processing that is not lawful. Certification authorities in the permissioned blockchain networks can solve this problem as a condition peer to join the network.

10. Performance

The experiment that we are going to perform, as a result of this research paper, will be implemented by using the Hyperledger Fabric platform. The reason for choosing this platform is already discussed in the previous sections, so it is noteworthy to discuss the performance part since it's important for the final prototype. Hyperledger Fabric is a complex distributed system, so determining the performance will be difficult task, since many parameters can come into play. The performance can vary depending on the type of the distributed application, transaction size, implementation of the ordering service, the network, hardware on which the participant run, number of participants in the system, number of participants that are part of the consensus process, number of channels of collaboration etc [33].

Though there are tools that can measure the performance of the blockchain solution, such as Hyperledger Caliper and some measures that are present in the technical documentations such as 3500 transactions per second with latency less than one second, in this section we are going to focus more on the parameters which affect the performance [30].

When it comes to the performance, since Hyperledger Fabric offers permissioned business blockchain solution, the speed of executing the transactions and validating them through all the participants in the process of achieving consensus can be drastically better than the other implementations of blockchain technology [3]. As we already described, Fabric is using the paradigm execute-order-validate in the transaction flow, where the endorsers are separated from the ordering service giving the possibility transactions to be executed in parallel. Just for comparison, in many other blockchain platforms, such as Ethereum, the nodes must execute transaction sequentially and, in such way, decreasing the performance. Another gain from the platform is the separation of concerns by splitting the blockchain on separate channels of collaboration. Each channel has its own ledger and its own chaincode, giving a huge performance increase, since only specific nodes should involve in executing some business rule.

The constraints that affects the performance can be different and on the highest level can be separated in:

- Block size – measurement for how many transactions can be grouped in a batch which is sent to the peers to form the new block in the blockchain. To maximize the throughput, the blockchain platforms offer possibility to configure the size of the blocks. Block size should be optimized in order the prototype to have the best transaction per second trend. Some experiments with predefined hardware and network parameters, assumes that 2 MB of block size can bring to 3000 transactions per second and latency less than one second [30].
- Number of endorsers – the endorsers are the peers which are defined in the endorsement policy as the special ones which are responsible for the process of achieving consensus. They are responsible for executing process, so logically the performance should drop if the number of endorsers increase.
- Transaction size – we already mention couple of time the importance to include as less amount of data in the transaction as possible, because they affect the performance directly. Additionally, transaction in Fabric are larger because they carry identity and certification data.

11. Conclusion

In this paper, we present a use case analysis in which stakeholders related to healthcare and insurance can distribute health related data in a secure, multi-institutional and multinational way. We analyzed the components of blockchain based architecture that are crucial in prototyping such mechanism for transferring information. After thorough analysis, examination and comparison of the current trends and platforms, we are presenting a combination of approaches related to blockchain technology, that are suitable and we can incorporate it in the overall architecture. The combination consists of development platform that will create private network which is satisfying the needs of our scope, execute-order-validate endorsement policy for enforcing the business rules of the use case, consensus algorithm that offers satisfying performance and scalability to the architecture and membership mechanism that will control the access to the network.

The architecture of the approach depicts and explains how a distributed layer technology can fit into existing Electronic Health Records (EHR) systems or Insurance Content Management systems, bridging the gap between the different implementations and reduce the friction of data distribution and obtaining the best value and performance in such environment.

The paper shows a clear roadmap of the actions and steps that one participant in the system, no matter if it's individual, healthcare provider or insurance company, need to perform to become part of such decentralized health information exchange system. Additionally, it explains the initial setup and efforts that one health care or insurance institution should perform to adopt this alternative approach of health information exchange and the benefits that they will gain from it.

References

1. Ethereum vs Hyperledger. Blockchain Training Alliance (2018), `https://blockchaintrainingalliance.com/blogs/news/ethereum-vs-hyperledger`
2. What is HIE? — HealthIT.gov. Healthit.gov (2018), `https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie`
3. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference. p. 30. ACM (2018)
4. Bell, L., Buchanan, W.J., Cameron, J., Lo, O.: Applications of blockchain within healthcare. Blockchain in Healthcare Today (2018)
5. Boban, M.: Digital single market and eu data protection reform with regard to the processing of personal data as the challenge of the modern world. Economic and social development: book of proceedings p. 191 (2016)
6. Buterin, V.: On public and private blockchains. Ethereum blog 7 (2015)
7. Cachin, C.: Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers. vol. 310 (2016)
8. Cardon, D.: Healthcare Databases: Purpose, Strengths, Weaknesses. Health CatalystURL (2018), `https://downloads.healthcatalyst.com/wp-content/uploads/2014/08/Healthcare-Databases-Purpose-Strengths-Weaknesses.pdf`
9. da Conceição, A.F., da Silva, F.S.C., Rocha, V., Locoro, A., Barguil, J.M.: Eletronic health records using blockchain technology. arXiv preprint arXiv:1804.10078 (2018)
10. Diedrich, H.: Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations. Wildfire Publishing Sydney (2016)
11. Dixon, B.: Health Information Exchange: Navigating and Managing a Network of Health Information Systems. Academic Press (2016)
12. Ekblaw, A., Azaria, A., Halamka, J.D., Lippman, A.: A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data. In: Proceedings of IEEE open & big data conference. vol. 13, p. 13 (2016)

13. Fabiano, N.: Internet of things and blockchain: Legal issues and privacy. the challenge for a privacy standard. In: Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017 IEEE International Conference on. pp. 727–734. IEEE (2017)
14. Gervais, A.: On the Security, Performance and Privacy of Proof of Work Blockchains. Ph.D. thesis, ETH Zurich (2016)
15. Goldschmidt, P.G.: Hit and mis: implications of health information technology and medical information systems. Communications of the ACM 48(10), 68–74 (2005)
16. Gordon, W.J., Catalini, C.: Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and structural biotechnology journal 16, 224–230 (2018)
17. Greenspan, G.: Four genuine blockchain use cases — MultiChain. Multichain.com [Online]. Available (2018), `https://www.multichain.com/blog/2016/05/four-genuine-blockchain-use-cases/`
18. Guegan, D.: Public blockchain versus private blockhain (2017)
19. Kassab, M.H., DeFranco, J., Malas, T., Laplante, P., Neto, V.V.G., et al.: Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Transactions on Emerging Topics in Computing (2019)
20. Krawisz, D.: The proof-of-work concept. Satoshi Nakamoto Institute¡ http://nakamotoinstitute.org/mempool/the-proof-of-work-concept/# selection-17.15-17.19 (2013)
21. Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D.: Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC). pp. 1–5. IEEE (2017)
22. Mackey, T., Bekki, H., Matsuzaki, T., Mizushima, H.: Examining the potential of blockchain technology to meet the needs of 21st-century japanese health care: viewpoint on use cases and policy. Journal of medical Internet research 22(1), e13649 (2020)
23. McDonald, C.J.: The barriers to electronic medical record systems and how to overcome them. Journal of the American Medical Informatics Association 4(3), 213–221 (1997)
24. Mettler, M.: Blockchain technology in healthcare: The revolution starts here. In: 2016 IEEE 18th International Conference on e-Health Networking. Applications and Services (Healthcom (2016)
25. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C.: A review on consensus algorithm of blockchain. In: Systems, Man, and Cybernetics (SMC), 2017 IEEE International Conference on. pp. 2567–2572. IEEE (2017)
26. Mougayar, W.: The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons (2016)
27. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2009)
28. Network, I.: IRYO. Global participatory healthcare ecosystem. URL (2017), `https://iryo.io/iryo_whitepaper.pdf`
29. Ribitzky, R., St Clair, J., Houlding, D.I., McFarlane, C.T., Ahier, B., Gould, M., Flannery, H.L., Pupo, E., Clauson, K.A.: Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. Blockchain in Healthcare Today 1, 1–15 (2018)
30. Scherer, M.: Performance and scalability of blockchain networks and smart contracts (2017)
31. Schueffel, P.: Alternative distributed ledger technologies blockchain vs. tangle vs. hashgraph-a high-level overview and comparison (2017)
32. Swan, M.: Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc." (2015)
33. Thakkar, P., Nathan, S., Vishwanathan, B.: Performance benchmarking and optimizing hyperledger fabric blockchain platform. arXiv preprint arXiv:1805.11390 (2018)
34. Valenta, M., Sandner, P.: Comparison of ethereum, hyperledger fabric and corda. Tech. rep., FSBC Working Paper (2017)

35. Vukolic, M.: The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In: International Workshop on Open Problems in Network Security. pp. 112–125. Springer (2015)
36. Wang, R., Liu, H., Wang, H., Yang, Q., Wu, D.: Distributed security architecture based on blockchain for connected health: Architecture, challenges, and approaches. IEEE Wireless Communications 26(6), 30–36 (2019)
37. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A taxonomy of blockchain-based systems for architecture design. In: Software Architecture (ICSA), 2017 IEEE International Conference on. pp. 243–252. IEEE (2017)
38. Zheng, Z., Xie, S., Dai, H.N., Wang, H.: Blockchain challenges and opportunities: A survey. Work Pap.–2016 (2016)
39. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: Architecture, consensus, and future trends. In: Big Data (BigData Congress), 2017 IEEE International Congress on. pp. 557–564. IEEE (2017)

Zlate Dodevski is the Chief Operations Officer at iborn.net. He received his MSc in Computer Science, in the field of Intelligent Information Systems, in 2019 at the Faculty of Computer Science and Engineering (FCSE), under the Ss. Cyril and Methodius University in Skopje, Macedonia. Zlate has an extensive background in blockchain technologies, decentralization of systems and secure management of Health Information Exchange. His current research interests are focused on topics such as system security, cryptography, and distributed architectures.

Sonja Filiposka is a full professor at the Faculty of Computer Science, Ss. Cyril and Methodius University in Skopje. Since obtaining her PhD in 2009 from the Faculty of Electrical Engineering and Information Technologies she has been actively taking part in a number of research projects related to e-infrastructure, networking and ICT education. During her professional carrier she has authored over 100 research papers published in conference proceedings and journals. Her main research fields of interest include e-services, orchestration of systems, complex networking and security.

Anastas Mishev, PhD, is a professor at the Faculty of Computer Science and Engineering at UKIM. He obtained his PhD in Computer Science in 2009. The focus of his research is infrastructures for collaborative computing and research, primarily Grid and High-Performance Computing systems. His aim is to get these systems closer to all potential users, mainly the research communities, in order to fully use their enormous potential. He researched in the areas of computer architectures and networks, software engineering, Internet technologies and e-learning, and is co-author of over 70 scientific papers published in international journals and proceedings of conferences. He has participated in the implementation of over 30 international projects funded by TEMPUS, PHARE, DAAD and FP programs, targeting the development of IT infrastructure and IT education.

Vladimir Trajkovik received Ph.D. degree in 2003 from Ss. Cyril and Methodius University in Skopje. He joined the Ss. Cyril and Methodius University, Skopje, R N. Macedonia, in December 1997. His current position is a professor at the Faculty of Computer Science and Engineering. He has published in more than 50 respectable journals and more than 150 conference papers. His research interests include: Information Systems Analyses and

Design, Distributed Systems, ICT based Collaboration Systems and Mobile services with special focus on two areas: Connected Health and ICT in Education.

Received: April 26, 2020; Accepted: December 12, 2020.