Identity Management in Healthcare Using Blockchain Technology

João Santos and Pedro Salgueiro, Vítor Nogueira

Universidade de Évora, Portugal
m39519@alunos.uevora.pt
pds@di.uevora.pt
vbn@di.uevora.pt

Abstract. Using the Blockchain technology a system can be created to provide several benefits over traditional methods being used in today's Health digital landscape. Costs and risks associated with these systems can be reduced and information can become transparent and trustworthy to all participants. In this article the technological foundations that enable this change are explored and analyzed. The Hyperledger Fabric Network with true private transactions and advanced security mechanisms was used to serve as the basis for this system. An application was created that uses smart contracts to manipulate the ledger. This system will be presented and its impact in Healthcare discussed.

Keywords: Blockchain, Health, Identity, Big Data

1 Introduction

Health is becoming more digital thanks to the widespread availability of computing devices. More and more medical records are stored on a digital format. For storing patient clinical data and their identity in a medical context, the Electronic Health Record (EHR) was created.

While all this information should benefit both patient and health professionals alike, it is not being handled in an effective manner due to problems caused, in part, due to the fragmentation of the patients identity that naturally occurs in today's Health Information Systems.

Health is an important topic, for everyone. Healthcare should strive to provide the best service it can for everyone and everyone should have access to a quality service. EHR are being generated at an ever increasing rate but most of the data is not used in a way that puts the patient's privacy and trust at the forefront.

The purpose of the work presented in this paper is to create and implement a Blockchain based system for Identity Management in the Healthcare domain. The patient will be able to manage his data and control its access. Such a system would be suited to handle the patient's identity, for example, in hospitals

or clinics and would be able to solve many problems in how data is traditionally handled in the Information Systems (IS) available in a regular medical environment.

Blockchain is known as the technology behind the Bitcoin Cryptocurrency, altough nowadays it is being used for many more purposes that are explored in the following sections, and its main design goal is to provide security and immutability to an agreed upon list of records.

A blockchain runs on a network of computers and the list of records is replicated in some manner depending on the blockchain implementation. The first blockchain was conceptualized as the public ledger for the Bitcoin cryptocurrency in 2008 by Satoshi Nakamoto, a pen name of, a still unknown to this day, individual or organization of individuals. The network was implemented in 2009 and many are now finding it has a much broader potential across many fields, with some implementations even resembling a programming platform to execute code in an autonomous manner. [Nak08]

A single universal way to identify a person in a given environment is clearly something we should strive towards as seen in, for example, *Cartão de Cidadão*, a portuguese identification document that replaces four other identification documents, streamlining portuguese civilian identification. This also allows many businesses to tailor their services to this document making it easier on both parts and eliminating unnecessary costs and risks.

Electronic Health Records (EHR) have seen some progress made regarding the standards that allow for interoperability between different organizations thanks to the Health Level 7 (HL7) standard. While this standard is growing in use and is represented internationally, Portugal has just started the work required to implement it. [Hea17]

In an effort to make the identity of a patient more secure and transparent a Blockchain can be used to create a system that puts at the forefront of its design the patients, breaking conventions in traditional patient data handling.

In this article different Blockchain implementations are explored and related work in this field is presented. More precisely, in section 2, a brief introduction to Blockchain is made followed by an introduction to its most prominent implementations. Then a number of real-world use cases of this technology in the healthcare field are explored. In section 3 technical details of the system will be presented. Finally, in section 4, some conclusions are observed regarding the change enabled by these advances.

2 Background

While Blockchain is not a new concept at this point, it is an evolving technology that is being used to solve old problems with new approaches. This section

will explore the Blockchain technology origins and history, some of its different implementations and a brief history to the identity problem is presented.

2.1 Blockchain Technology

A Blockchain can be many things, it can refer to the Bitcoin blockchain, alternative implementations or forks of the Bitcoin Blockchain called Altchains or even platforms that allow execution of code in an autonomous manner, exactly as it was programmed, with no human intervention. Is is a continuously growing list of records, written in the ledger, a structure where records are written, that is being replicated across a network of devices in opposition to having a single central record history, making it a good example of a distributed database. [Woo17]

The main design goal of the Blockchain is security and to fulfill this purpose it uses techniques such as cryptography and digital signatures to not only verify the authenticity of records but also read or write access to the network.

Unlike a conventional central data storage, where only a single entity keeps a copy of the underlying database, the ledger of the Blockchain is replicated across any number of nodes. Not every participant has the same ability to interact with the ledger and in this respect a blockchain can be permissionless or permissioned. In a permissionless blockchain every node of the network can write in the blockchain whereas in a permissioned blockchain only a select group of entities have access to writing in the ledger making the permissioned version, by default, secure if the entities themselves are secure and considered trustworthy.

How does a permissionless Blockchain maintain security if every participant has access to writing on it, including potentially malicious parties?

Take for example the Bitcoin Blockchain that uses a peer-to-peer network to avoid meddling from a financial institution or a third party in a financial transaction. Given that participating nodes in the network can belong to different and often competing parties, there is no implied trust between them, so the Blockchain needs a mechanism to ensure the integrity of the ledger and prevent malicious meddling from interested parties or to avoid a central authority.[Bar17]

To solve this problem, consensus mechanisms are used differently, depending on its implementation, but having, at its core, a solution to create immutable records and ensure security. In Bitcoin Blockchain's case, consensus is reached by the longest chain rule where the longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of computing power.[Baa16]

While the first blockchain was conceptualized as the public ledger for the Bitcoin cryptocurrency in 2008 by Satoshi Nakamoto and implemented in 2009, many are now using it as a foundation across many application areas such as identity management, traceability and asset management. Thanks to the roaring

success of Bitcoin and the increasingly apparent use cases that the Blockchain can provide, the public awareness of it is rising and it is quickly becoming a technological foundation in our economic and social systems.

2.1.1 Ethereum

Bitcoin is getting media coverage almost everyday and public awareness in cryptocurrencies in general is rising. Some people are considering cryptocurrencies and the Blockchain, to be essentially the same technology and, while that may have been somewhat true not so long ago, Blockchain technology is starting to be used in a plethora of ways.

Ethereum is an open-source platform based on the Blockchain technology that enables developers to build and deploy Decentralized Applications (*DAPPs*). Ethereum is being developed by the Ethereum Foundation and was first discussed by Buterin [2013]. Ethereum intends to provide a blockchain with a built-in programming language that is used to create *"Smart contracts"*. [Woo17]

These contracts are used to describe the logic of any system that developers can imagine and, when created, can then be deployed to the blockchain where they execute as "autonomous agents". Thanks to these tools it is safe to say that long gone are the days where building Blockchain applications required a complex background in coding cryptography, mathematics as well as significant resources.[Woo17,Blo17a]

Ethereum Blockchain is a permissionless Blockchain, and thus, it must have a consensus mechanism to ensure the validation process of every record and, in turn, ensure security and immutability. While other implementations of the blockchain have different consensus mechanics, in Ethereum's case, all participants have to reach consensus over the order of all transactions that have taken place, if a definitive order cannot be established then a double-spend might have occurred.

2.1.2 Fabric

Hyperledger Fabric (HLF) is part of the Hyperledger project started in December 2015 by the Linux Foundation, and is an open-source developer-focused community of communities focused on the development of enterprise-grade, open-source Blockchain-based solutions. Fabric is an implementation of a Distributed Ledger Platform (DLP) under the Hyperledger umbrella. [Cac16]

HLF's initial commit was contributed by IBM and written in Go language. It is a permissioned blockchain and its main design goal was to surpass previous Blockchain implementation limitations, such as, lack of true private transactions and confidential contracts.

This is achieved thanks to assigning peers in the network three distinct roles: endorser, committer and consenter and by offering the ability to create channels, where a group of participants in the network create a separate ledger. HLF is intended as a foundation for developing applications in a modular fashion, opting for a plug-and-play approach to various components. [Hyp17b]

HLF, as discussed, also allows the creation of smart contracts which can be written in Chaincode. As this Blockchain's key operational requirement is privacy, true private transactions and confidential contracts can exist and are a great asset for a business environment where sensitive information is necessary and disclosed often. Thanks to its modular approach consensus protocols are no longer hard-coded and trust models can be repurposed.

2.1.3 Burrow

Hyperledger Burrow (HLB) is also part of the Hyperledger project and its development started in 2014 by Monax and sponsored by Intel. It is a permissionable smart contract machine written in Go and offers a modular blockchain client with a permissioned smart contract interpreter built, in part, to the specification of the Ethereum Virtual Machine (EVM) and the client has, essentially, three main components, the consensus engine, the permissioned EVM and the Remote Procedure Call (RPC) gateway. [KMBD17,Hyp17a]

HLB has its own Consensus Engine, the Byzantine fault-tolerant Tendermint protocol. The Tendermint protocol is an open-source effort that allows high performance in solving the consensus problem and also has a flexible interface for building arbitrary applications above the consensus, as well as, a suite of tools for deployments and their management. [Buc16]

2.2 Identity in Healthcare

Originally records of a patient were stored in a physical format. Thanks to the advent of the computers more and more records are stored on a digital format and the Electronic Health Record (EHR) was created. This benefits handling of information between the patient and the medical professionals and medical institutions.

Standards for EHRs were created and many failed to bring the much needed consensus that was required for interoperability between different Information Systems in different institutions. Health Level 7 has done much work to be recognized in many countries and is quickly being implemented in many countries to allow for joint efforts between organizations.

However due to the decentralized nature of many health organizations the identity of a person has become a very cumbersome, costly and risky affair to handle. Security in a connected age, where internet is easily available, is lagging behind

and presenting some problems. There is also the question of transparent use of information by the organizations that store it.

2.3 Blockchain for Identity Management in Healthcare: Use Cases

Some companies started to see Blockchain applications in the Healthcare field and established some key partnerships however many of those are still very early on development or deployment. Guardtime has fully deployed their system in 2008, started cooperating in 2011 and in 2016 announced a partnership with the Estonian Government, where a million patient records are now secured by the strategy and, until today, still proves the resilience of the Blockchain technology thanks to other advances in cryptography. Now other companies like Verizon are becoming interested in this technology for their own purposes. [Gua18,Est16]

Another company, Gem, is collaborating with Phillips Healthcare to explore options in this area, and is opting to solve the interoperability problem with an additional layer of abstraction they call GemOS. Factom, another Blockchain-based service, has also announced a partnership with a major US medical services provider HealthNautica.[Blo17b,Fac17]

The use of the Blockchain technology in the health field is expanding. Just recently a new platform appeared, called Medichain that allows patients to store their own data in a secure way and give anonymized access to this data to specialists. Giving data allows for users to gain tokens that represent value. [Med18]

3 A HLF Network for Healthcare

After analyzing the different blockchain implementations the Fabric network was chosen as the foundation for this system. First we will discuss the tools provided to configure the network, and then discuss the system architecture.

3.1 Fabric Network Configuration Tools

Hyperledger Fabric (HLF) does not use a centralized ledger where every record is available to every participant in the network. Instead it opts to allow multiple ledgers in a network to achieve different goals of a greater purpose. This allows the creation of channels of information between trusted parties, for example, a channel of secure and private information between the clinical staff of an hospital and a patient.

A HLF network is comprised by the *"cryptogen"*, *"configtxgen"*, *"configtxlator"* and *"peer"* tools that are used to configure the network.

The *"cryptogen"* tool generates cryptographic data consuming the file *"crypto-config.yaml"*. HLF uses an abstraction layer for certification and authority called Membership Service Provider (MSP) that defines the rules by which entities are governed and authenticated and it must be unique for every participating entity.

The *"configtxgen"* tool generates the genesis block for the orderer services and the initial transactions. This tool consumes the file *"configtx.yaml"* that defines configuration parameters for channels, the genesis block and the orderer service.

The *"configtxlator"* tool is also used to generate channel configurations. Finally the *"peer"* tool is used to manage the participating peers in the HLF network.

These tools are used to create and maintain the topology of the network and are invoked when a change to the network is made, for example, when permissions to certain records are changed or a new user is enrolled in the network and are very much intertwined with the Certificate Authority (CA) server system to maintain the security that is needed in a sensitive subject that deals with private information.

3.2 Identity Representation in Hyperledger

HLF allows information to be written and read in a distributed manner with security and privacy at the forefront. Using smart contracts, a record is created to represent the concept of identity in this network.

The information that defines the patients identity is a key requirement to build a system that recognizes patients across the Healthcare environment. To this end, the identity of a patient is recorded on the ledger of the HLF network as a structure via a smart contract deployed to the network that interacts directly with the ledger. This structure contains the necessary fields to identify the patient such as its name and birth date, for example, as well as some other information necessary to manage this data.

To aid in interoperability with other systems the Fast Healthcare Interoperability Resources (FHIR) standard by the Health Level 7 organization was used as basis for the representation of a patient. Each field of the structure that represents the patients identity, defined in the smart contract, is linked to a field of the patient structure as presented in the FHIR standard.

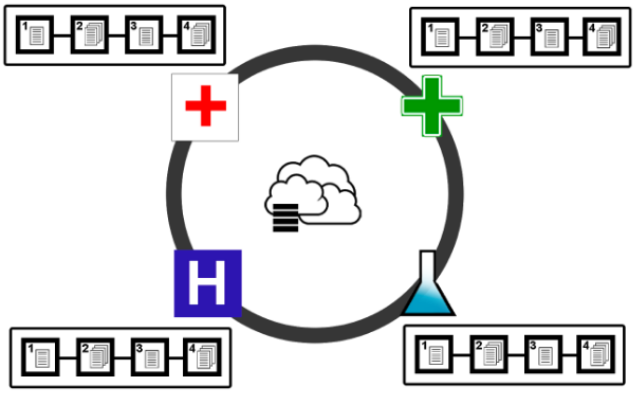

Fig. 1. An Example of Interoperability with the Blockchain Network

3.3 Aplication and Smart Contracts

To create an interactive system that can manage the patients identity in an Healthcare environment an application was built that the user interacts with. This application interfaces with smart contracts through the Hyperledger Fabric Software Development Kit and the chaincode was built using the Hyperledger Fabric Shim for node.js.

The application is accessed by the user and calls upon the smart contract. The smart contract will handle the assets part of the system. A smart contract to represent and manipulate identity was built and interfaces with the network to write and read records to the appropriate ledger. The overview of the architecture for this system is represented on Figure 2

The application allows for user enrollment to create a new identity in the network. When a new user of the application enters in the network the function, in the smart contract, that initializes the creation of the user and writes the user to the ledger as a new participating identity is called. Due to the security mechanisms this specific transaction is automatically signed by the administrator of the network and is verified by the CA servers.

The smart contract also provides the application with several operations to manage the identity object as seen on Figure 3. These operations form an Application Programming Interface (API) that return a payload in JSON format with identity information from the network. This API allows a query to be made to the network that returns the patients information, changing incorrect or outdated information or disabling the identity structure of someone who is not participating in the network actively anymore in order for that information to be read-only from that point on, for example, with more available. Depending on the operation only certain users can access the information or manipulate the already

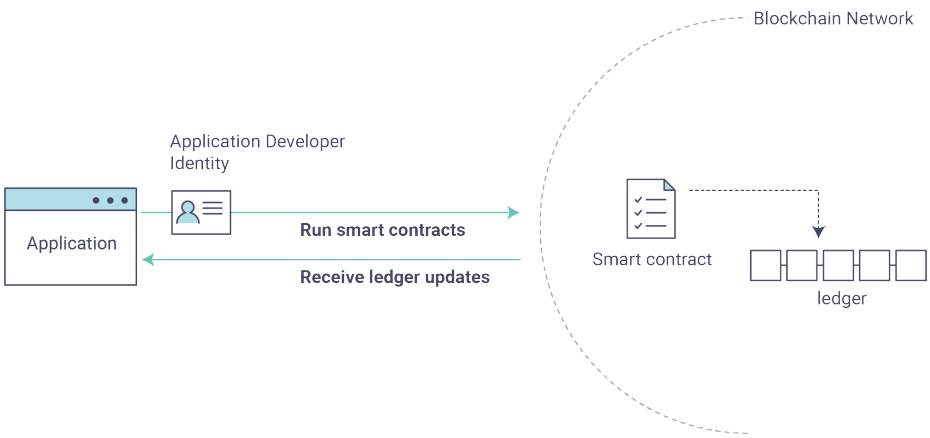

Fig. 2. An Overview of the System Architecture (Source: HLF Fabric Documentation)

existing one. This system architecture leads to a modular as well as extensible approach regarding the availability of new operations that become available as soon as new versions of the smart contract are deployed.

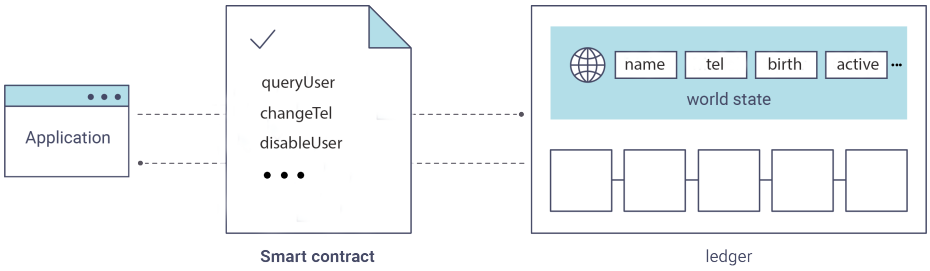

Fig. 3. Smart Contract Operations Example (Original: HLF Fabric Documentation)

4 Conclusion

In this document it was described that the way identity is handled by medical institutions nowadays presents a problem. Blockchain was explored as a tool to solve this problem and some of its different implementations were analyzed. Some practical use cases of this technology also discussed. This research will enable solid foundations for future work.

It is safe to say that a system for improving the way a patient can interact with their health data can be built, using this technology, as discussed in previous sections. The system should allow for a transparent handling of personal data and be able to allow for secure management of access to this particular data.

If an advance is made in this regard it is expected that the patients trust in their Healthcare service is increased, and that risks and costs inherent to multiple descentralized information systems, that are not normalized to any standard, be reduced.

References

ACCG17. Daniel Augot, Hervé Chabanne, Olivier Clémot, and William George. Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain. pages 1–10, 2017.

Baa16. Djuri Baars. Towards Self-Sovereign Identity using Blockchain Technology. *University of Twente*, page 90, 2016.

Bar17. Iain Barclay. Innovative Applications of Blockchain Technology in Crime and Security. 2017.

Blo17a. BlockGeeks Ethereum Guide. `https://blockgeeks.com/guides/ethereum/`, 2017. [Online; Accessed November 29, 2017].

Blo17b. Is Blockchain the Answer to Healthcare's Big Data Problems? `https://healthitanalytics.com/news/is-blockchain-the-answer-to-healthcares-big-data-problems`, 2017. [Online; Accessed December 1, 2017].

Buc16. Ethan Buchman. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. 2016.

Cac16. Christian Cachin. Architecture of the hyperledger blockchain fabric. *IBM Research*, July, 2016.

Dre17. Daniel Drescher. *Blockchain Basics*. Apress, Berkeley, CA, 2017.

Est16. Estonian Government Adopts Blockchain To Secure 1 Mln Health Records. `https://cointelegraph.com/news/estonian-government-adopts-blockchain-to-secure-1-mln-health-records`, 2016. [Online; Accessed February 25, 2018].

Fac17. Factom's Latest Partnership Takes on US Healthcare. `https://cointelegraph.com/news/factoms-latest-partnership-takes-on-us-healthcare`, 2017. [Online; Accessed December 1, 2017].

Gua18. Verizon to Use KSI Blockchain Technology Developed for Estonia. `https://www.sdxcentral.com/articles/news/verizon-use-ksi-blockchain-technology-developed-estonia/2018/02/`, 2018. [Online; Accessed February 25, 2018].

Hea17. Health Level 7 Webpage. `https://hl7.org/`, 2017. [Online; Accessed January 15, 2018].

Hyp17a. Hyperledger Burrow Github Page. `https://github.com/hyperledger/burrow`, 2017. [Online; Accessed November 29, 2017].

Hyp17b. Hyperledger Fabric Documentation. `https://hyperledger-fabric.readthedocs.io/en/release/`, 2017. [Online; Accessed November 29, 2017].

KMBD17. Casey Kuhlman, Dan Middleton, Benjamin Bollen, and Silas Davis. Hyperledger Burrow (formerly eris-db). 2017.

Lew15. Antony Lewis. A gentle introduction to blockchain Technology. *Bits On Blocks*, pages 1–13, 2015.

Med18. MEDICHAIN - The Medical Big-Data Platform. `https://medichain.online/`, 2018. [Online; Accessed February 25, 2018].

Nak08. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. *`https://bitcoin.org/bitcoin.pdf`*, page 9, 2008.

SWP16. David Shrier, Weige Wu, and Alex Pentland. Blockchain & Infrastructure (Identity , Data Security). pages 1–18, 2016.

VS17. Martin Valenta and Philipp Sandner. Comparison of Ethereum, Hyperledger Fabric and Corda. (June):1–8, 2017.

Vuk17. Marko Vukolić. Rethinking Permissioned Blockchains. *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC '17*, pages 3–7, 2017.

Woo17. Gavin Wood. Ethereum: a Secure Decentralised Generalised Transaction Ledger. 2017.

YL16. Affan Yasin and Lin Liu. An Online Identity and Smart Contract Management System. *Proceedings - International Computer Software and Applications Conference*, 2:192–198, 2016.