Identity Management in Healthcare Using Blockchain Technology

João Santos

Universidade de Évora, Portugal
February 18, 2018
m39519@alunos.uevora.pt

Abstract. Nowadays Health is becoming more digital. Thanks to the widespread availability of computing devices more and more records are stored on a digital format. For patients clinical data, 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, thanks to the fragmentation of a patient's identity inherent in today's Health Information Systems. 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 system will be presented and its impact in Healthcare discussed.

Key words: Blockchain, Health, Identity, Big Health

1 Introduction

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 many times 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 access to it. Such a system would be suited to handle the patient's identity, for example, in hospitals or clinics and solving many problems that are inherent to how data is traditionally handled with the information systems available in a regular medical environment.

Blockchain is the technology behind the Bitcoin Cryptocurrency, altough nowadays it is being used for many more purposes which are explored in section 2, 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 thanks to the inherent characteristics of this technology.

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 a proposed 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, alternate 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, that is replicated across a network of devices in opposition to having a single central copy, making it an example of a distributed data structure. [Woo17]

The main design goal of blockchain is security and to this effect it uses techniques such as cryptography and digital signatures to verify the authenticity and read or write access to the blockchain.

Unlike a conventional central data storage, where only a single entity keeps a copy of the underlying database, the blockchain is replicated across any number of nodes. Not everyone 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.

But then, how does a permissionless blockchain maintain security if everyone 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.

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.

Hyperledger 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 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.

Hyperledger 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 Ethereum virtual machine 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 allows for easier handling of information and benefits the patient and the medical professionals.

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. One exception is Guardtime that has fully deployed their system for the Estonian Government in 2008 where a million patient records are secured by the strategy and, until today, still proves the resilience of the Blockchain technology thanks to other advances in the cryptography side.

Another interesting company to mention is Gem, which 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]

It is safe to assume that more and more companies will try to fill this void and try to solve the identity problem we face.

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

HLF does not use a centralized ledger where every record would be available to every participant in the network. Instead it spans multiple ledgers in a network. This allows, as discussed, the creation of channels of information between trusted parties, for example, a channel between the clinical staff of a hospital and a patient.

After obtaining the fabric binaries there are four tools that can be used to configure and manage a HLF 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.

3.2 Identity Representation Proposal

To manage the data of the patient they must be identified by the blockchain. To this purpose it is proposed that the identity of a patient is recorded on the ledger of the fabric network.

To aid in interoperability with other systems the FHIR standard for Health Level 7 was used as basis for the representation of a patient.

3.3 Aplication and Smart Contracts

To create an interactive system an application will be built that the end-user will interact with. This application will interface with smart contracts through Hyperledger Fabric Software Development Kit built using the Hyperledger Fabric Shim for node.js.

The application will handle the user input and commands will be presented for the user to handle the application flow. The smart contract will handle the assets part of the system. A smart contract to represent and manipulate identity will be built and interface with the network to write records to the appropriate ledger.

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.

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].

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.

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.