Pursuing Health Automatization

The issue with health systems optimization

1st Stéphane Monteiro  
*IT Department*  
Polytechnic of Viseu

Viseu, Portugal

estgv16842@alunos.estgv.ipv.pt  
  
2nd Diogo Oliveira  
*IT Department*  
Polytechnic of Viseu

Viseu, Portugal

estgv15577@alunos.estgv.ipv.pt

3rd João António  
*IT Department*  
Polytechnic of Viseu

Viseu, Portugal

estgv17440@alunos.estgv.ipv.pt

Abstract — Health optimization is a core concept to help citizens in their time of need. So, if the professionals are good at what they do so must be the infrastructures supporting them. But from that some problems appear, first the complexity of the information behind each citizen and then the most effective way to secure a client health history to make him feel safe and secure at any point. With the evolution of technology some solutions came upon the needs, one of them is blockchain. Blockchain can create an abstract system that will allow the user to have its information shared only with the people that require it.

1. Introduction

With the growth of technology, private and public health systems were greatly improved. Many health entities understood that to offer a good service to its clients the presence of technology was vital. From prescribing medications to even detect certain diseases, technology has become an integral part of the health systems. However, many entities still don´t use technology to its full capacity, so many citizens are being offered a tedious and not descriptive service.

With that, one of the integral parts of private or public health systems is the capacity to prescribe medication to its clients. One of the problems with that information is the presence of data that shows to anyone that read it the disease that the client suffers from, to solve that development of a system that allows the access of the medication recipes by all actors participating using a Web Service API, backed up with multiple security features and encrypted transactional data, provided by blockchain, in this case within the Ethereum network, and smart contracts, could be a major player on the health systems of the entities that use it.

Blockchain an old term with modern applications, it has been increasing in popularity on the last few years, mostly because of the creation of cryptocurrencies like Bitcoin. It works as a peer-to-peer network, allowing the creation of a block inside a network. Each block contains a block header and a block transaction. Block headers, contain mostly data that can identify the validity of a block, maintaining in that way a secure system. In the case of a block transaction, it will contain data regarding the transaction object. Since every time that a transaction happens on an already existing block the hashed identifier is updated, then the blocks moving forward should be invalidated. There are ways to calculate the hash for each block from one point forward, that’s why concepts like proof of work, that allows the slowing down of the calculation of the next blocks hashes are being implemented as a safe mechanism to beat tampering. [1]

Ethereum, like Bitcoin, is a decentralized public blockchain network. Inclusive to all users, it aims to offer smart contract functionalities. It was created to solve some of the Bitcoin limitations. Ethereum, allows the creation and deployment of applications that offer immutable and decentralized services. It aims to provide financial services without having the need of third parties involved in a transaction between users. [1]

To have a consent in terms of ruling regarding the content inside a block on the network, a program must be in place to enforce those rules. So, with that on mind, smart contracts are created, chained into a block, they allow the automatization of an agreement between all participants to fulfill a transaction. [2]

A web service, acts like an interface, allowing clients to create, read, update, or delete (CRUD) data from a specified web server. Web services are important systems in modern development, allowing multiple information systems to communicate uniformly with each other. [3]

1. State Of Art
   1. Blockchain

Blockchain acts as a public peer-to-peer network described by blocks. While being mainly used for the creation of crypto currencies such as Bitcoin, the core mission of blockchain is to allow the storage of data in a secured environment while offering a transparency on each transaction.

Every block aims to have its data immutable, data stored in a block should not be updated.

Uma imagem com mesa

Descrição gerada automaticamente

Figure - Blockchain Block

As stated on *Figure 1 - Blockchain Block*, each block can be summarized by a block header and a block transaction. Block headers, contain mostly data that can identify the validity of a block. [4]

In the case of a block transaction, it will contain data regarding the transaction object.

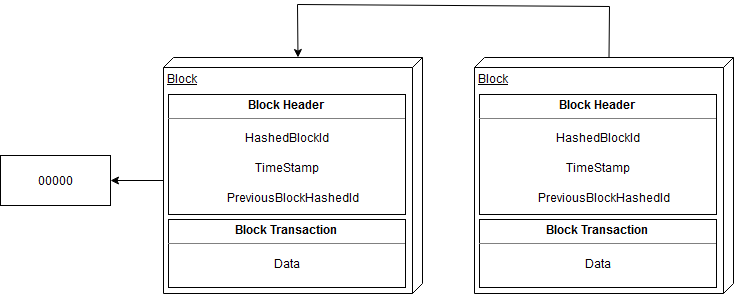


Figure - Blockchain

When one block is created, it´s added to the chain, and it will store the previous block hashed identifier, creating in that way a continuity of linked blocks that maintain the security of the data, an example can be seen in *Figure 2 - Blockchain*.

Although blockchains aims for immutability, as processing power increases, the data on a block can be tampered with.

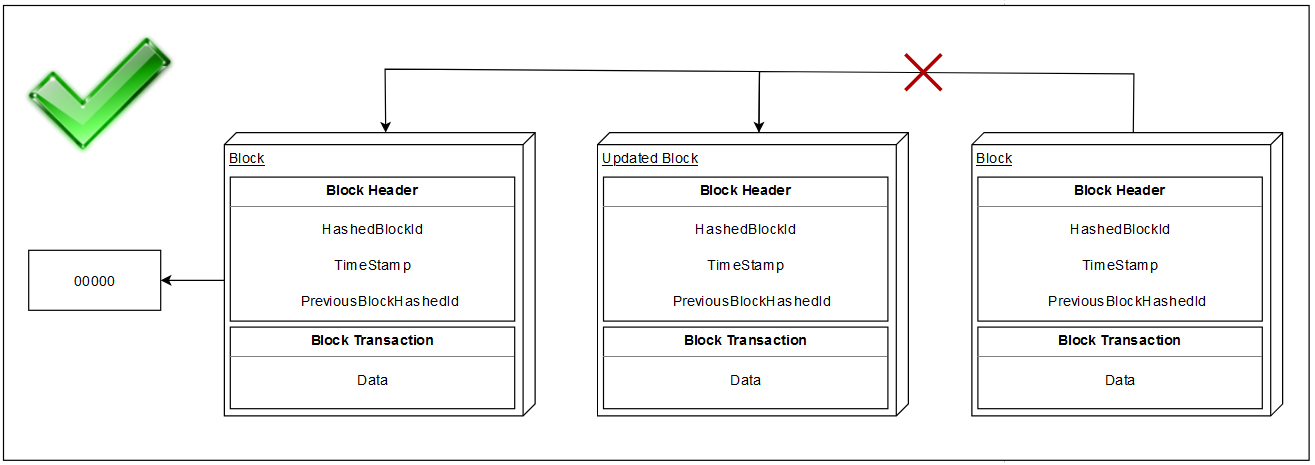


Figure - Blockchain Block Update

Normally, when a block is updated, the subsequent blocks are considered invalid, since the previous hashed identifier on the next block is not existent anymore, this can be seen on *Figure 3 - Blockchain Block Update*.

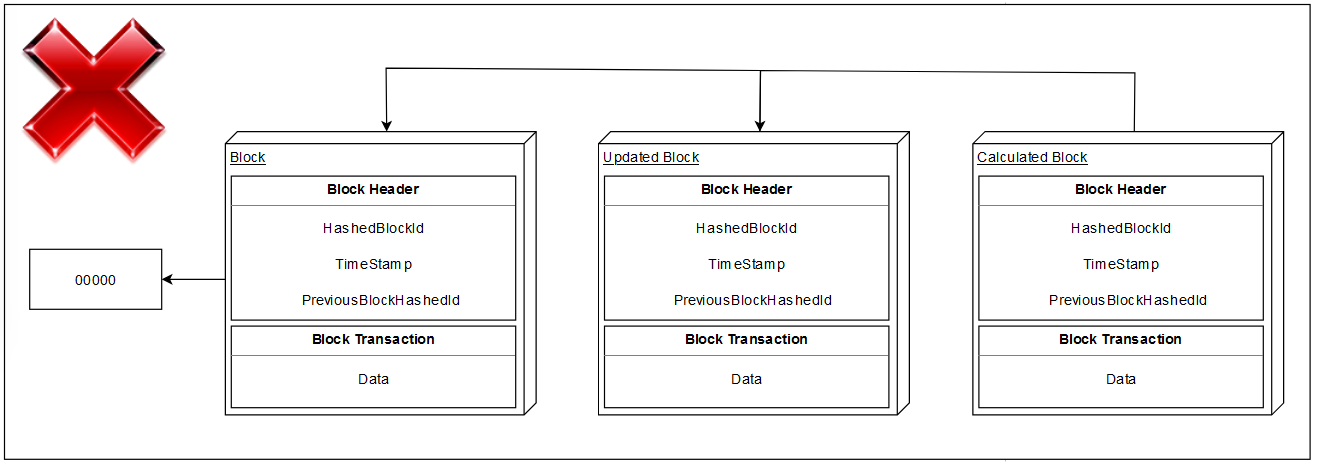


Figure - Blockchain Block Invalid Update

However, as it is exemplified on *Figure 4 - Blockchain Block Invalid Update*, with great processing power a new line of blocks can be calculated, creating a new chain completely valid within seconds.

To solve this problem, the concept of proof of work was created. Whenever a block is updated on the blockchain, there is an amount of effort (time), normally by decrypting encrypted puzzles by using hashed functions, to finish the creation of a new block. If a transaction contains that proof of work, then the blockchain knows that the transaction is verified and valid.

However, proof of work contains a big problem, the energy consumption is massive, for that, proof of stake appeared as an alternative to proof of work. Proof of stake allows a user to be next forger of a block, by having a system of random selection based on entrance price on that selection. So, instead of multiple users trying to forge the next block of a blockchain, only a selected person can forge it. [4]

* 1. Ethereum Network

Ethereum, a public decentralized blockchain network. Created to solve some of the Bitcoin limitations. Ethereum, allows the creation and deployment of applications that offer immutable and decentralized services, most commonly, financial services.

Ethereum takes advantage of Smart Contracts and a pool of cryptographic rules to have the user deciding a combination of ownership rules, transaction states and functions. Those rules are going to only be run when certain conditions are met. [1]

* 1. Smart Contract

To have a consensus between many participant actors, as in any area, a contract must be created and respect by the totality of the participants, and so that’s the main goal of smart contracts. It will store information regarding the pre-define functions that force every actor to fulfil the rules if they want to act on a transaction.

Whenever a smart contract is created and then deployed, the creator will receive an address, that address will be shared for other users to create a transaction. That means that the public blockchain subject to a smart contract will have blocks created if the creator of each block respects the parameters defined by the smart contract. [2]

1. ARCHITECTURE

To work within the bounds that were specified to achieve a decoupled, and scalable system, an architectural solution was designed.

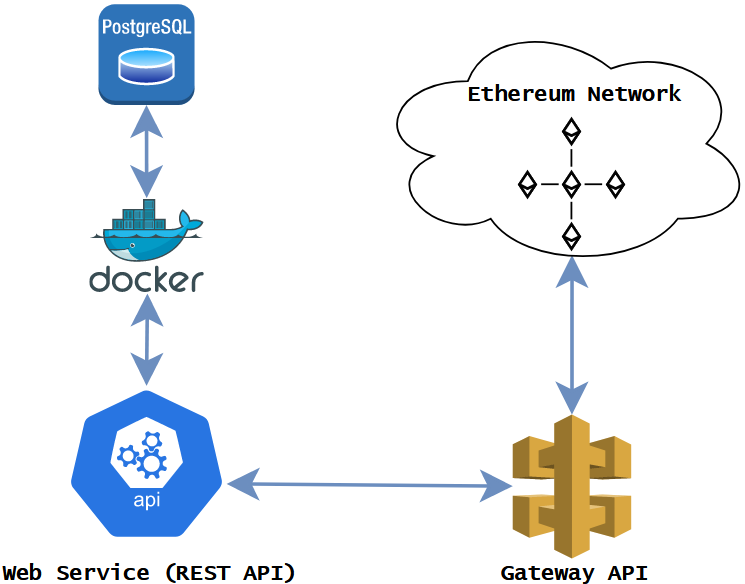


Figure - Architecture

As presented in the *Figure 5 - Architecture*, there are three tiers of support within this system. The first refers to the backend application in charge of storing medication data and authenticating healthcare entities.

The second is a middleware application that sits between the health care application and the Rinkeby Ethereum Testnet. It separates the functionality required to interact with the smart contract from the healthcare application. This application makes use of an Ethereum API supplied by Infura for reading data from the Smart contract. The Infura Ethereum API, as well as a MetaMask wallet linked to the Rinkeby Testnet, are required for data storage in the smart contract.

The smart contract functionality was created using an Ethereum Virtual Machine (EVM) written in Solidity and tested using the Remix IDE. It was then deployed into the Rinkeby Testnet using the MetaMask account, which needs a gas price payment in the form of ETH based on the smart contract code resource efficiency.

The last component represents the Rinkeby Ethereum Testnet which is a test blockchain network that allows the deployment of smart contracts.

1. Results

For the results we will check a medical recipe structure and it will be evaluated the time required to execute each functionality disposed by the smart contract.

Uma imagem com texto

Descrição gerada automaticamente

Figure - Medical Recipe

In the *Figure 6 - Medical Recipe,* we can see multiple SHA256 encryption keys representing each entity for the healthcare entity (userId), the citizen (citizenId) as well as a key for the complete medical recipe structure (recipeId). Each entity ID was encrypted for security purposes before being persisted with the smart contract functionality.

There are three methods which are for creating a medical recipe, retrieving all medical recipes existing and retrieving all medical recipes for a specific patient.

For an exact number of 15 med recipes stored in the Smart Contract we obtain the following execution times for each of the methods available.

1. Table Type Styles

|  |  |  |
| --- | --- | --- |
| **Access** | **Method** | **Execution time** |
| write | create a med recipe | 8496.004ms |
| read | get med recipe by patient | 622.448ms |
| read | get all med recipes | 844.961ms |

It is notable the time difference for creating the medical recipe when compared to retrieving data from the smart contract. It took about 8.5 seconds for creating the med recipe while for retrieving the data for both methods it was less than a second.

1. future work

To future work, there are some limitations to be fixed, currently, the system works on the top of a public Ethereum Network, it causes some extra gas costs, mostly from the Smart Contracts, that could be reduced by having a custom blockchain created for this same system. One other feature that could be done, is using another framework, like Hyperledger instead of a public Ethereum network that is being currently used, to create a private network, having the information secured and only accessible by verified users.

References

|  |  |
| --- | --- |
| [1] | D. Vujičić, D. Jagodić and S. Ranđić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8345547/figures#figures. |
| [2] | F. L. C. G.-G. E. B. &. A. B.-H. Shafaq Naheed Khan, "Blockchain smart contracts: Applications, challenges, and future trends," [Online]. Available: https://link.springer.com/article/10.1007/s12083-021-01127-0#article-info. |
| [3] | S. Islam, R. Kumar and A. R. Dar, "A COMPREHENSIVE STUDY ON WEB SERVICES BASICS," [Online]. Available: https://www.researchgate.net/publication/326477418\_A\_COMPREHENSIVE\_STUDY\_ON\_WEB\_SERVICES\_BASICS. |
| [4] | W. Metcalfe, "Ethereum, Smart Contracts, DApps," [Online]. Available: https://library.oapen.org/bitstream/handle/20.500.12657/37713/2020\_Book\_BlockchainAndCryptCurrency.pdf?sequence=1#page=88. |