Towards Using Blockchain Technology for eHealth Data Access Management

[1,2]Nabil Rifi, [1]Elie Rachkidi, [1]Nazim Agoulmine, [2]Nada Chendeb Taher
[1]COSMO, IBISC Laboratory, University of Evry, France
[2]Lebanese University, Faculty of Engineering and Azm Center for Researches, Tripoli, Lebanon

***Abstract*—eHealth is a technology that is growing in importance over time, varying from remote access to Medical Records, such as Electronic Health Records (EHR), or Electronic Medical Records (EMR), to real-time data exchange from different on-body sensors coming from different patients. With this huge amount of critical data being exchanged, problems and challenges arise. Privacy and confidentiality of this critical medical data are of high concern to the patients and authorized persons to use this data. On the other hand, scalability and interoperability are also important problems that should be considered in the final solution. This paper illustrates the specific problems and highlights the benefits of the blockchain technology for the deployment of a secure and a scalable solution for medical data exchange in order to have the best performance possible.**

I. Introduction

The concept of eHealth is very important nowadays. It can have different meanings and definitions, either Healthcare and EMR, or health informatics, to Telemedicine. It is the practice of healthcare which is delivered or enhanced through the internet and related technologies. The importance of eHealth lies within its ability to give patients, all over the world, an access to their medical data and a real-time monitoring of their health with the evolution of IoT and connected objects. It has a huge impact on different aspects of life, and studies need to take place in order to get the best results [1]. mHealth, or mobile Health, which is becoming the most popular form of eHealth can be used in treating patients, and conducting research along with health education and maintaining public health by tracking diseases [2]. On the other hand, it improves the communication between patients and healthcare professionals, thus effectiveness in treatments and health monitoring, wider access to medical care, and less pressure on public healthcare budgets. This is why maintaining the access security to the medical data that is shared in this domain is of high interest.
Blockchain is an emerging technology, first introduced with bitcoin [3], the famous crypto-currency. At the beginning, it was a solution for double spending and only used as a financial application. However, it turns out that Blockchain technology can have many other applications, and it might be the ultimate solution for the problems we face today in eHealth and the Internet of Things (IoT). In fact, Blockchain is a decentralized, peer to peer technology where no third parties are needed. Before settling and choosing blockchain technology as a solution, Deloitte [4] did a study on when and why to choose it, and it was made clear that for blockchain to be considered as an application, it should have some defined characteristics; *”enhanced security is needed to ensure integrity of the system”*. They also provide steps towards building a successful blockchain based solution. After research, we have got to the conclusion that in order to apply blockchain technology to eHealth, it should be public, and has three main keys: scalability, secure access to medical data, and data privacy.
This paper is structured as follows; after this brief introduction, we will discuss the state of the art, regarding blockchain, and previous works that integrate blockchain in eHealth. In the third section, we will present problems facing this integration. The last sections will include our proposed model, a conclusion and some ideas for our works perspectives.

II. State of the Art

A. Preliminaries

1) Blockchain: Blockchain is a Peer-to-Peer decentralized technology. The important thing to know about blockchain is its main characteristic: Transparency, no need for third parties and instant access to data since it is replicated on all nodes. It is a series of linked blocks of transferred data between different connected nodes that form the network of the blockchain.
There exists many types of blockchain, either private or public, and the most popular are Bitcoin and Ethereum. The first one is the infrastructure for the well known cryptocurrency Bitcoin. The other, Ethereum, is very similar to Bitcoin but differs however in several aspects. For instance, it has a very flexible programming language for Smart Contracts, which we will define later, and there is a difference in what the blocks contain, and how each block is validated [5].

2) IPFS: The InterPlanetary File System, is a peer-to-peer distributed file system that is based on different older technologies, especially BitTorrent. It is ”similar to a single BitTorrent swarm exchanging git objects”. IPFS is very similar to Blockchain in terms of the way it functions, however IPFS is seen as the storage system since one of the most drawbacks of Blockchain is its inability to maintain a huge amount of data on it [6]. We believe that IPFS is the best candidate for Off-Chain database in a fully distributed system.

3) Smart Contracts: The idea of Smart Contracts was first introduced by NickSzabo in 1997 [7]. He then defined it as contractual clauses, such as collateral, bonding, property, etc., that can be embedded in hardware and software. Based on this definition, Smart Contracts are the most interesting components of the Blockchain. In [8], Smart Contracts are

978-1-5386-1642-0/17/$31.00 ©2017 IEEE

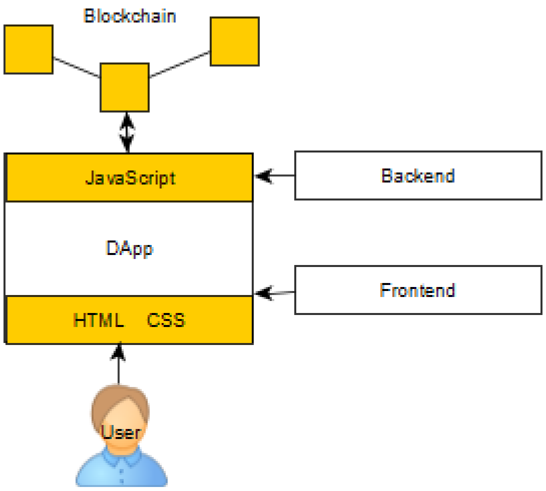

Fig. 1. Decentralized Applications: Frontend, Backend and link to Blockchain

explained in details in an IoT context. For simplification, Smart Contracts are scripts, or codes, that are written and deployed on the blockchain, waiting for some condition to be true or false, in order to trigger an action, or a specific transaction. Thus, Smart Contracts are the ”brains” of the blockchain.

4) DApps: DApps, or Decentralized Applications, are very similar to a normal application from a user’s point of view, however, they are very different. A Decentralized Application is similar to a normal application by its Frontend, which is the code that is behind the user interface, such as HTML in case of web application. The difference is that in the case of DApps, the backend is a distributed peer-to-peer network where the backend in a normal application is a server. Figure 1 explains the architecture.

The approach of a DApp is very interesting in the case of an eHealth application, since the users need to interact with a distributed peer-to-peer network in a standard and common way, and this is a great advantage in DApps.

5) Mining: Mining is the process of validating a block in the blockchain, it varies between different types of blockchain. What’s important is the fact that a lot of computational power is needed for becoming a ”Miner” in the blockchain. Miners are usually rewarded, for example in bitcoin, they are rewarded with actual crypto-currency. Mining might affect the whole performance of the system, it is a critical concept that needs to be taken into consideration.

B. Related Works

We have conducted an intensive research to analyze the state of the art by crawling the Internet searching for works with these two keywords: eHealth and Blockchain. Searching these keywords using IEEEXplore generated only four responses. The analysis of these results shows that there have been few, yet different approaches to apply blockchain technology on eHealth, especially Healthcare. For instance, it is possible to distinguish different areas regarding this subject: Data Access, Data Sharing and Permission Management. Another way to look at these works is if they considered its either static Data such as EMR/EHR, or dynamic Data such as Sensory data from on body sensors.

In [9], the authors provide a general discussion about how Blockchain can be used in Healthcare, and how other previous and present projects are actually being developed in a converging Blockchain Healthcare combination. They focus on the ease of medical data access using blockchain, the use of this data for research matters, and the advantage of using this technology to prevent medical products counterfeit and fraud, along with some Blockchain applications for healthcare.

If we dig deeper, we can realize that few protocols, data models, architectures and some studies are being developed in this domain. It is clear in [10], that blockchain is becoming a tool that is used to build new protocols, as they proposed a fully detailed protocol and architecture to organize data access, and focusing on making it more and more user-centric. This approach is very interesting since it is directly built on smart contracts, that play a very important role in how the whole system is supposed to work. The main idea was deploying contracts that organize the relationship between patients and providers, and gives the patient complete control of their medical data, and who can access the data, along with an off-chain database. However, all this data is static, EMR and EHR files.

The other approach, is based on pervasive social network based healthcare [11], where the focus is on the data generated by the WBAN (wireless body area network), in other words, on body sensors. This is more of a cryptography point of view approach, where the real problem treated is the energy and computational power of the on-body sensors, by adding a ”Coordinator”, and a scheme on how to use blockchain in such applications. They also presented experiments and interesting results.

It is also interesting to understand a more general approach, in [12], where a full protocol, with different levels of functionality was proposed to manage, store and share data based on blockchain technology in an IoT context.

III. The Problem with the Blockchain Approach

So far, Blockchain seems to be a very good solution for eHealth security problems. In fact, it provides transparency, trust-less environment, security protocol that has not yet been broken, and a technology that might change the future of the Internet. But implementing blockchain in applications like eHealth, demands a lot of resources. Some authors were confronted with this challenge, like already mentioned in the previous section [10], [11]. One of our first research objectives is to first answer this question: Is it possible to design a blockchain based architecture, a model, that can scale and provide enough security for eHealth applications?

In this paper, we propose such an architecture. Based on blockchain knowledge and previous works, we were able to combine the flexibility and importance of smart contracts, alongside with the scaling of off-chain database and the security and privacy of the blockchain for future eHealth

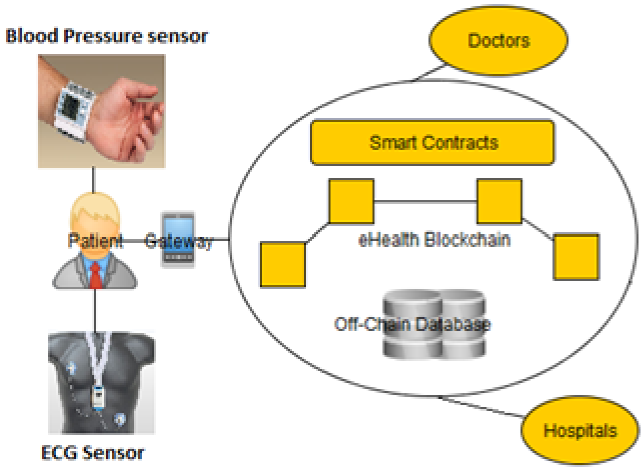

Fig. 2. Our proposed architecture, Patients with a data gateway to the Blockchain and medical sensors, Doctors and Hospitals are nodes connected to the eHealth Blockchain with deployed Smart Contracts along with an off-chain database

DApps. The application of these technologies in eHealth domain answers the challenges and solves the problems in a standard architecture.

IV. Model and Proposed Solution

Our proposed approach in building our model is to use blockchain technology as a solution to address eHealth applications challenges. We give attention to data exchange security and sensors' low computational power. First, it is infeasible and provokes very poor performance to store all the data on the blockchain, so the blockchain will be used as a tool to transfer only part of the data, or a pointer to where the data actually is, and thus, Off-Chain database. IPFS is a tool that has been already discussed in Section II. This will be used in our architecture as Off-Chain database to store medical data [13].

In figure 2, patients, doctors, and hospitals are connected to the eHealth blockchain, which provides security and privacy of the medical data. The off-chain database provides the solution for the blockchain storage that causes downgrading performance. This model describes the implementation of a standard eHealth application in a Blockchain environment. Patients may have sensors that are generating data, the data generated by the sensors will trigger a smart contract deployed on the blockchain which will then trigger a notification to certain interested parties, like doctors or research centers. To be able to completely describe this model, a simple use case scenario will justify how every component of this architecture works. Let us suppose that a patient with heart disease is being monitored in real time by some doctor, a smart contract linking the patient to the doctor, along with some terms to determine the communication between the two parties, after all, smart contracts are like any contract. Because of the issues we already discussed, regarding the computational power needed being a node on the blockchain, the sensors cannot be directly connected to the blockchain, thus the importance of the gateway. The gateway can be any device with sufficient energy and power to be node. Mobile phones or laptops can be used as gateways. All the data generated by the sensors will be handled by the gateway, and then stored in the off-chain database IPFS. A notification, along with a hash describing the location of the data will be communicated through the blockchain via a client; in the case of Ethereum, many clients exist like geth or PyEth. In order to maintain access security and privacy of the data, smart contracts need to be deployed on the blockchain in order to secure the patient-doctor relation. This can go beyond, by allowing the patients to choose themselves who has the right in viewing their data, from research centers to multiple doctors. We suppose that in order for the doctor to well monitor the patient, he needs samples of ECG data every period of time. After the data from the ECG sensor is stored, and the doctor is notified, using the hash sent with the notification, the doctor can access the ECG data in the IPFS database. This will provide greater data privacy. Using this model, along with cloud computing, opens up a way of solving the mining high computational power problem, when it comes to patients nodes. Even thought this will remove the complete decentralization characteristic from the model, but it will provide greater performance for future applications. In the case of cloud computing, the gateway might become a cloud server, which will create further issues since it is a remote server and connecting to it will jeopardize the data privacy. In the next section we give a detailed description of how this model is implemented and validated in an eHealth environment.

V. Implementation

To implement this model, the core of it is the blockchain. As already mentioned in Section II, there exists multiple types of blockchains, but for reasons of ease of testing and further development, Ethereum blockchain is used. Ethereum is also a public blockchain which has its own characteristics and block parameters, but provides the capability of creating our own private blockchain for studying and testing purposes. We used go-Ethereum (Geth) as the Ethereum client in order to connect to the Ethereum Blockchain, SolidityC language for Smart contracts programming and IPFS as database for file storage. As a frontend, a web application approach was chosen, HTML and javascript languages were used to develop the frontend. A network of nodes was setup on an Ethereum private blockchain. For the purpose of testing EMR, electrocardiogram (ECG) data was stored on IPFS nodes connected to the Ethereum nodes, and generated periodically by a local software. A couple of smart contracts were also deployed for notification generation and nodes organization. For the purpose of testing data from sensors, a future step is using a Raspberry Pi. The Raspberry Pi should be connected to the blockchain as a node, deploy a contract to notify the generation of new data every period of time. Different types of sensors can be connected to the Raspberry Pi, thus different types of Data generated can be tested in the implementation. Figure

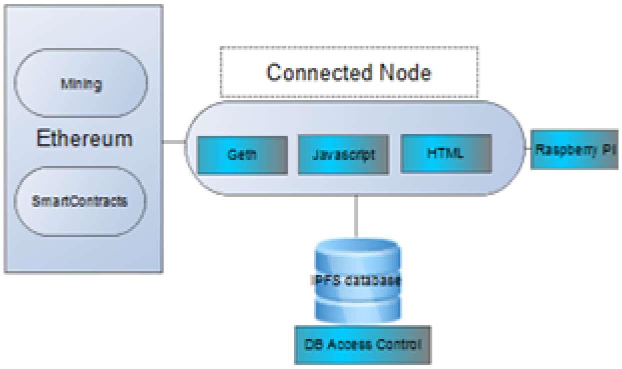

Fig. 3. The implementation of the system with all its components: Ethereum Blockchain, Ethereum Client Geth, IPFS Database, Web HTML and JavaScript, Solidity Smart Contracts

3 describes how the components are linked. The Raspberry Pi creates a node and connects to the Ethereum blockchain, along with an IPFS node connected to the IPFS database, with the DB access control that provides privileges and rights to access the Database. Mining is done on the blockchain by certain powerful nodes, in real life situations these nodes need to be research centers. Smart contracts are deployed on the blockchain, as they become like any other nodes with ethereum addresses. This model can be changed and manipulated in many ways, this will be discussed in the next section along with future works.

VI. Future Works

Implementation of this model and its validation were successful but in a limited environment. A lot of performance metrics and parameters can be studied, and different tools can be used. The author in [14] explains very well the different parameters that can be changed, optimized in order to optimize the performance of the system. Combining this with challenges in [15], that are not scientific but general challenges, a fully functional system for the future may be reached. In [14], the authors focus on the scalability of the decentralized networks, especially blockchain, with experiments on latency, throughput and other parameters. Another important parameter to study is the block itself, from the size of the block, to the time needed for mining a block, in other terms the cost. This is why, one of the major and most influential events in blockchain technology is mining. Many questions arise: Who should be mining? What is the mining cost? What is the mining reward? We are currently working on an implementation of this model combined with cloud computing as already mentioned in the previous section. Our next work will focus on IoT devices data rates, deadlines and block parameters in order to achieve an optimized performance in an eHealth context.

VII. Conclusion

With the present challenges of eHealth, and the advantages of blockchain technology, a revolution in the definition of many areas might take place. The future is towards a distributed Internet, and blockchain technology is the silver bullet for such a future, despite it's multiple difficulties. Patients will be connected to doctors, research centers, EMR providers, Insurance companies, in a trustless-no third party environment. A transparent access to all data, and a sharing of patients' medical data in a private secure way with the patient completely in control of his own data, who can see and who can use his data. This approach will revolutionize future applications, becoming extremely secure, private, and user-centric. eHealth is just the beginning, a peer-to-peer technology like blockchain can be applied in many different applications, from the music industry [16], to the power grid [17], all the way to the simplest buying, selling or data transfer over a decentralized secure network. Our paper proves that with the use of this technology along with the correct tools, models, protocols, and fully functional systems are yet to be implemented. This possibility of avoiding data intermediaries will affect the eHealth and Healthcare market, from providers to users and normal clients.

References

[1] *E-health: the importance of usability and accessibility*, April 2016, [Online] Available: focuscura.com/en/knowledge-development/blog/e-health-importance-usability-and-accessibility

[2] E-health: What is e-health and why is it important?, World Heart Federation, Scientific sessions 2014, Melbourne Australia

[3] S. Nakamoto. (2008). Bitcoin: *A Peer-to-Peer Electronic Cash System.* [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] *Blockchain: Opportunities for Health Care*, August 2016, [Online] Available: deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf

[5] Ethereum Whitepaper, [Online] Available: github.com/ethereum/wiki/wiki/White-Paper

[6] IPFS - Content Addressed, Versioned, P2P File System, [Online], Available: https://ipfs.io/docs/

[7] Nick Szabo, *The Idea of Smart Contracts*, [Online], Available: fon.hum.uva.nl/rob/Courses/InformationInSpeech/

[8] Konstantinos ChrisTidis and Micheal Devetsikiotis, ”Blockchains and Smart Contracts for the Internet of Things”, *IEEE Access (Volume: 4)*, 2016.

[9] Matthias Mettler, M.A. HSG Boydak, ”Blockchain Technology in Healthcare The Revolution Starts Here”, IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016

[10] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman, ”MedRec: Using Blockchain for Medical Data Access and Permission Management”, , International Conference on Open and Big Data (OBD), 2016

[11] Jie Zhang, Nian Xue, and Xin Huang, ”A Secure System For Pervasive Social Network-Based Healthcare”, IEEE Access (Volume: 4), 2016

[12] Sayed Hadi Hashemi, Faraz Faghri, Paul Rauschy and Roy H Campbell, ”World of Empowered IoT Users”, *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2016

[13] Trent McConaghy, Rodolphe Marques, Andreas Muller, Dimitri De Jonghe, T. Troy McConaghy, Greg McMullen, Ryan Henderson, Sylvain Bellemare, and Alberto Granzotto, ”BigchainDB: A Scalable Blockchain Database”, [Online], Available: bigchaindb.com/whitepaper

[14] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi1, Emin Gun Sirer, Dawn Song, and Roger Wattenhofer, ”On Scaling Decentralized Blockchains”, *Initiative for CryptoCurrencies and Contracts (IC3)*, 2016

[15] Deloitte UK, *Blockchain Key Challenges*, [Online], Available: deloitte.com/content/dam/Deloitte/uk/Documents

[16] Ben Dickson, *Blockchain could completely transform the music industry*, TechTalks, [Online], Available: venturebeat.com/2017/01/07/blockchain-could-completely-transform-the-music-industry/

[17] Don Tapscott and Alex Tapscott, *How Blockchain Technology Can Reinvent The Power Grid*, 2016, [Online], Available: http://fortune.com/2016/05/15/blockchain-reinvents-power-grid/