Blockchain Technology: A new secured Electronic Health Record System

Lotfi Tamazirt, Farid Alilat, Nazim Agoulmine

 ISBN 978-2-9561129

Blockchain Technology: A new secured Electronic Health Record System

Lotfi Tamazirt[1*], Farid Alilat[1], Nazim Agoulmine[2]
[1] University of Sciences and Technology Houari Boumediene, Algiers, Algeria
[2] University of Evry val-d'essonne, Paris, France.
ltamazirt@usthb.dz, faralilat@yahoo.fr, nazim.agoulmine@ibisc.univ-evry.fr.

Abstract

Nowadays, health systems are looking for effective ways to manage more patients in a shorter time, and to increase the quality of care through better coordination to provide quick, accurate and non-invasive diagnostics to patients. This paper aims to solve the dependence on trusted third parties by proposing a new management strategy, storage and security in a decentralized network through Blockchain technology. The proposed system also aims to offer a solution to help healthcare professionals to be informed of the slightest changes made in a patient's file in order to reduce medical error rates, but also by allowing them to consult them transparently if they are authorized.

1 Introduction

Over the last few decades, revolutionary new technologies such as the Internet have enabled the daily and professional lives of billions of people to cross the world, and have made it possible to overcome the constraints of distance and ubiquity through equal exchanges and an open and free flow of information. However, as soon as an exchange implies a transfer of material or immaterial value, it requires absolute confidence as a guaranty principle incarnated by centralized institutions which are none other than trusted third parties.

This aspect of authenticity and confidentiality of data as well as the security of information transfers once again makes its full sense in the medical and health care field in which the slightest error in the writing or reading of a medical record can be fatal. Certainly, there are now several electronic systems for the indexation and the storage of patient records, nevertheless, the latter do not always consensus in terms of reliability or legitimacy, hence the need to supervise them. However, the supervision of these trusted third parties is not without risk, which explains the fact that patients and professionals are gradually losing confidence in those systems.

The current problem is therefore how to have solutions allowing to trust these systems, and having the opportunity to solve the intrinsic problems to the functioning of these entities in order to be able to

reform the current system through innovative alternatives to the current schemes, and thus to dispense with a third party in charge of the verification, validation and listing of the history of medical records.

Among those promising technologies that are unambiguous and revolutionizing in many aspects, a permanent, transparent, secured and non-centralized control solution, relying on its own security system has emerged. It is none other than the Blockchain technology.

This paper focuses mainly on the investigation of the applicability and the implementation of an Electronic Health Record (EHR) system (Friend, T. H. et al. (2017). Communication Patterns in the Perioperative Environment During Epic Electronic Health Record System Implementation. *Journal of medical systems*, *41*(2), 22.) based on blockchain technology on the top of an E-health communication architecture. The rest of this paper is organized as follows. The first part of this article is devoted to presenting the fundamentals of Blockchain technology. The second focusses in the technical part of the EHR Blockchain system, and explains in detail its functional aspect and its protocols as well as the steps necessary for the development of this system. Finally, we will end this paper with a discussion of the potential of the Blockchain in such an application and will end with a conclusion.

2 Fundamental of Blockchain technology

The Blockchain literally means a chain of blocks. It is perceived as a system or a computer protocol for managing digital data of all kinds: transactions, contracts, medical data, etc. All this information is housed in digital containers as chronologically chained blocks from hence the name Blockchain.

In other words, the Blockchain is a sort of gigantic register with an almost unlimited storage capacity, transparent, secured and decentralized. It contains the history of all the exchanges made by the users since the system is created. The latter can of course be consulted in a transparent manner. The Blockchain can be described as a register on which everyone can write, but cannot erase and/or destroy.

The confidentiality of data shared by users requires a high level of security. As a result, the system requires the sharing of copies of this register on the various computers known as "network nodes". The robustness of this technology is demonstrated not only by the use of a sophisticated security system, which is asymmetric cryptography, but also by sharing data and information in a “peer-to-peer” (Gaffney, T. (2016). The Peer-to-Peer Blockchain Mortgage Recording System: Scraping the Mortgage Electronic Registration System and Replacing It with a System Built off a Blockchain. *Wake Forest J. Bus. & Intell. Prop. L.*, *17*, 349.) i.e. from one user to another without passing through a third party.

Figure 1 shows a part of the architecture of a Blockchain.

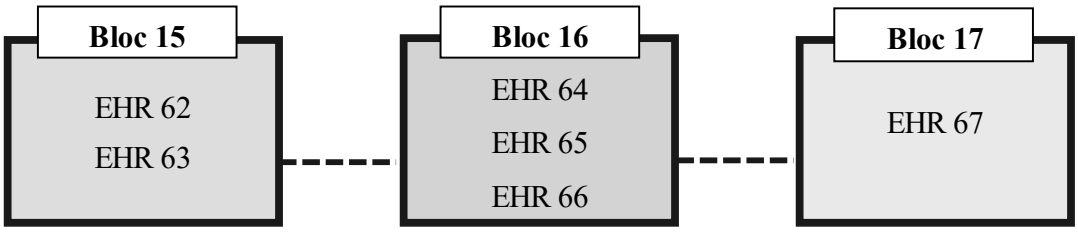

Figure 1: EHR Blockchain architecture.

3 Types of Blockchain systems

The Blockchain technology is adaptable to its degree of openness, if the latter is limited, the Blockchain created is called "private" or "consortium", on the other hand if it is open, it is called "public".

• **Public Blockchain:** The Public Blockchain is a fully decentralized and open-ended block chain in terms of use, reading, and participation in the management of operations within the network. The main element favoring this model is the assured protection of the users of an application against the developers of this same application.

• **Consortium Blockchain:** The Consortium Blockchain is a partially decentralized semi-private chain, where the consensus process, i.e., the management of the operation, is controlled by a set of pre-selected nodes. Depending on the application, access and consultation of the registry may be public or restricted.

• **Private Blockchain**: The private Blockchain is a chain of blocks whose writing is dedicated to a centralized organization, contrary to the right of reading which can be public or private, which reinforces the confidentiality of the users and reduces the costs of operations; its strength lies in the possibility of drafting, modifying and sealing all the rules of the Blockchain network.

The optimum solution for a particular industry depends greatly on the exact area of activity of the industry in question. In some cases, the public model is clearly more appropriate, in others a certain degree of private control is simply necessary.

4 Functional aspect of Blockchains

The functional aspect of a Blockchain system is based on three pillars:

1. Peer-to-Peer network that offers decentralization of the system.
2. Cryptography, which ensures the anonymity or, more precisely, the pseudonymy of users and the electronic authentication, thanks to asymmetric algorithms such as RSA (Somani, U., et al. (2010, October). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on* (pp. 211-216). IEEE.), which can provide encryption as well as electronic signatures. Its security is based on the intra-capacity of the factorization problem of large integers.
3. A programmed consensus, distributed on all the nodes of the network, which ensures the construction of a chain of identical blocks for all the nodes of the Blockchain even if it is built independently.

The combination of these three concepts gives rise to a digital data management system, transparent, secure and decentralized, which allows a breakthrough in computing.

5 Electronic Health Records Blockchain

As mentioned before, the type of Blockchain to use depends heavily on the application. In the case of EHR, the most judicious choice to consider is the Consortium Blockchains. Because medical records

of a particular patient should offer the opportunity for many practitioners to view the history of their patients while not letting anyone add facts if some pre-selected nodes do not allow them to.

So, in order to enhance the security of EHR, we propose to implement a Consortium Blockchain dedicated to medical records. Thus, when recording a fact for example, the user writes in the register or in the database using his own private key. This is called the creation of facts. The attending physician as well as all the members of the network - if they are authorized - can then decrypt and read the medical file with complete transparency. Moreover, the accounts cannot be modified or repudiated because only the user who has the encryption key who is actually the private key. This process is called the electronic signature or authentication.

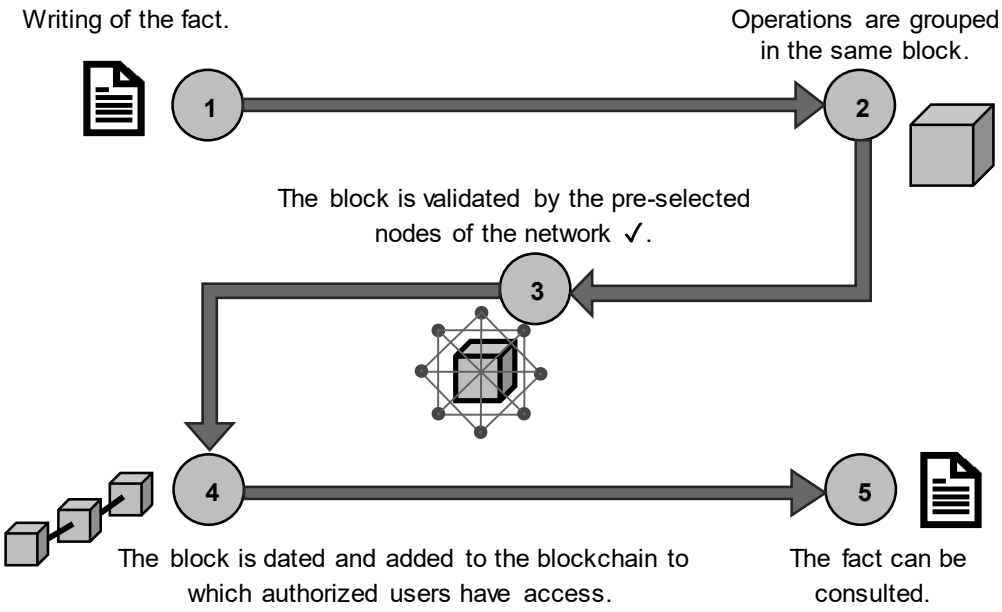

Figure 2: Validation process of the EHR Blockchain.

In the proposed EHR Blockchain, adding a fact is carried out by the establishment of a process ensuring the start of the various steps which are explained as follows: (the figure 2 summarizes the process).

- A doctor proceeds to write a fact on the Blockchain account.
- The fact is recorded and timestamped in a block using arithmetic operations.
- The block is subsequently validated by network pre-selected nodes of the network through cryptographic techniques, this is called Hashing.
- The block is dated and added to the block chain at the end of a vital element that is the consensus mechanism, so that all users can have access to the same chain since each node builds its own exemplary independently.

- Finally, another doctor or other users can access to EHR of a specific patient added by the first doctor.

6 Development of the EHR Blockchain System

The development of an EHR block goes through an extremely important function in the generation process of the EHR Blockchain (figure 3), the hash function. The latter converts a digital input value to another compressed numerical value called a fingerprint. The input of this hash function has an arbitrary length, its output as for it is part has a fixed length.

The properties of this function are given as follows:

- Any data size always gives the same hash length.
- Slight changes in the input data give totally different hashes.
- Hash are unidirectional.

Otherwise, this function has two essential characteristics:

- The slightest change in the input chain causes a big change in the output chain and therefore a different footprint.
- Building a document that can provide a given footprint is deemed to be extremely difficult.

A footprint can therefore be at the same time an identifier, a guarantee of integrity, a proof of existence or even serve as a basic function in the production of proof of work. The footprint of a block is not integrated into n + 1 block, making it impossible to modify the block n, without having to modify also the block n + 1, then n + 2, n + 3, etc.

To find an identifier for each block of our EHR Blockchain, we must build a file that contains all the validated facts of the block and the identifier of the previous block, and to strengthen the security of this chain of blocks, a random number named Nonce (Kishigami, J., et al. (2015, August). The Blockchain-based digital content distribution system. In *Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on* (pp. 187-190). IEEE.) is added.

This file will go through a Hash function (Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using Blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE* (pp. 180-184). IEEE.), and the result is a sequence of characters that will be used as an identifier of the next block, then the blocks will be chained one after the other, where the identifier of a block is used to process the next block.

The addition of the random value Nonce aims to reinforce the robustness and security of the Blockchain. A condition on the identifier of the block is then imposed, it is called "The target difficulty", it is the fact of finding an identifier that begins with a number '0' depending on the accuracy of the system.

The aforementioned process requires significant computing power, since it can only be solved by trying random combinations of the Nonce, until finding a value that matches.

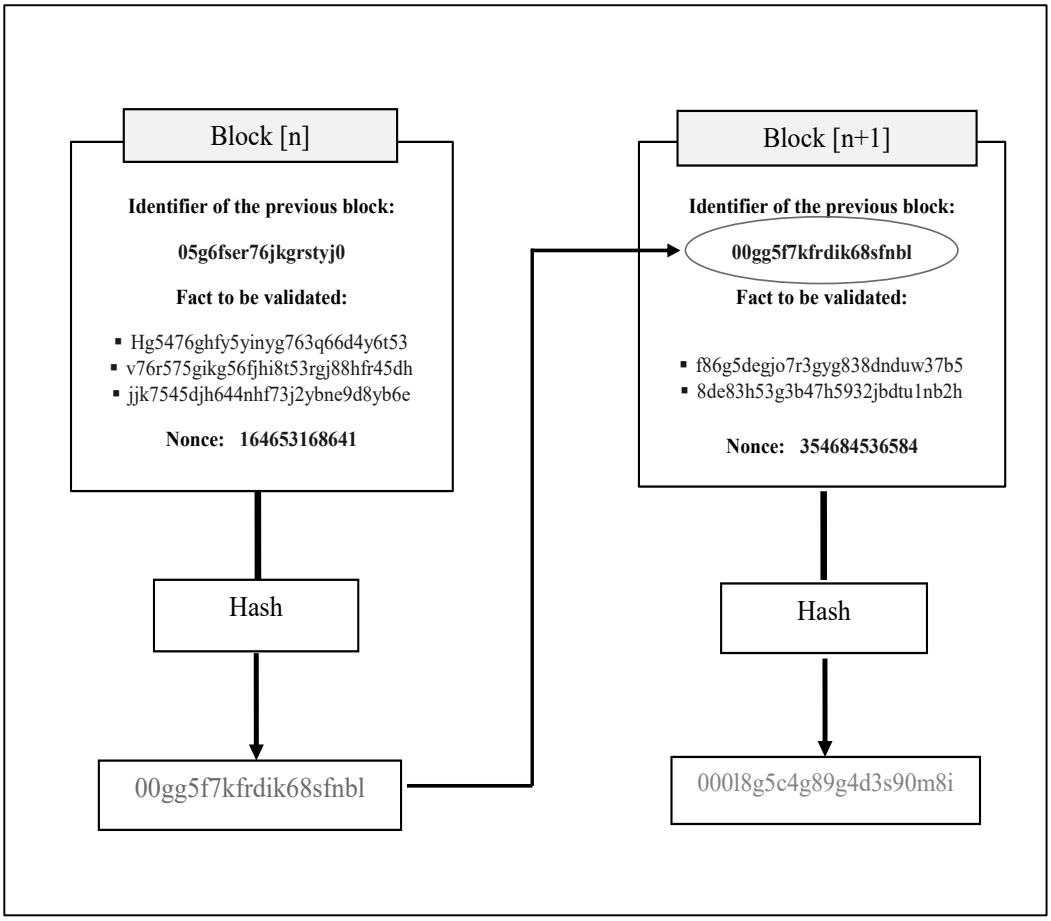

Figure 3: Example of an EHR block construction.

7 Content of an EHR block

A block consists of two essential parts, the block header and the contents of the block.

1. The header of the block is composed of:
    - Technical data, including a Magic ID, a version number that specifies to which set of rules of the protocol, this block is compliant, as well as the size of the block.
    - A Hash corresponding to the identifier of the previous block, it ensures the link that creates the Blockchain.
    - The Merkle root (Kallahalla, M, et al. (2003, March). Plutus: Scalable Secure File Sharing on Untrusted Storage. In *Fast* (Vol. 3, pp. 29-42) that includes a history of all block transactions as a single Hash.

- A block creation Timestamp that is used to determine whether the network is creating blocks too fast or too slowly.
- The target difficulty related to block checking. This is the condition on which the block identifier is generated.
- The Nonce: A random number added, to make the hash more difficult and create different Hash to find the most suitable.

2. The content of the block consists of a list of all the patients records, as well as the operations performed.

The figure 4 shows a block content of the EHR Blockchain.

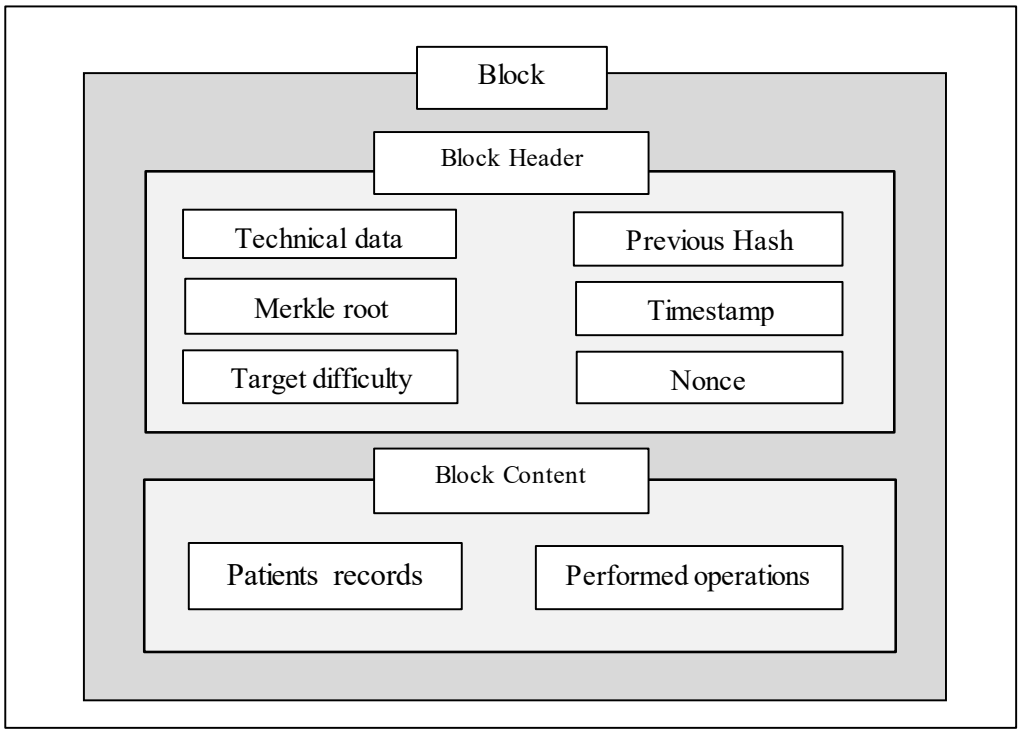

Figure 4: Block content of the EHR Blockchain.

8 Discussion

Through the implementation of our EHR Blockchain system, we truly believe that this technology has the potential to transform health care sector by increasing the level of the privacy and security, and most of all the interoperability of health data, by providing a ubiquitous, and a secured network infrastructure, capable to authenticate and verify the identity people with access to patients' medical records. The use of such a technology will open up new perspectives in the healthcare field by organizing it through the creation of secured and immutable health data and by surpassing the economic

challenges that must be addressed by governments. In (Rifi, N., et al. (2017, October). Towards using Blockchain technology for eHealth data access management), authors 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.

Hence, like any recent technology that is taking its first steps, the Blockchain system will obviously face technical problems, however, the technological research and hardware investments provided have solved some of these major problems such as data storage and the huge computing power needed to validate the blocks, which is currently disciplined by alternative protocols offering other management methods. In addition, an improvement must be made for the duration of the validation of the facts and the integration of the blocks in the chain which is rather long because it requires a distributed consensus throughout the network.

9 Conclusion

Blockchain technology is a new strategy that gives users a new decentralized power over businesses and public authorities, guaranteeing users' security, transparency and confidentiality, which is offered by a database similar to a register. implemented on a shared peer-to-peer network on all network nodes. Thus, we have proposed in this paper to use Blockchain technology as a tool to provide a new model for health care information exchanges by making EHR more secured in order to reduce and eliminate medical errors. We also explained the tools and methodologies adopted for the development of our EHR Blockchain system by illustrating the operating principle of this system as well as the different tools and methodologies needed. We believe that the proposed EHR Blockchain has the potential to support the healthcare sector by providing a better support to health data management for doctors and patients.

References

Friend, T. H. et al. (2017). Communication Patterns in the Perioperative Environment During Epic Electronic Health Record System Implementation. *Journal of medical systems*, *41*(2), 22

Gaffney, T. (2016). The Peer-to-Peer Blockchain Mortgage Recording System: Scraping the Mortgage Electronic Registration System and Replacing It with a System Built off a Blockchain. *Wake Forest J. Bus. & Intell. Prop. L.*, *17*, 349.

Somani, U., et al. (2010, October). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on* (pp. 211-216). IEEE.

Kishigami, J., et al. (2015, August). The blockchain-based digital content distribution system. In *Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on* (pp. 187-190). IEEE.)

Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE* (pp. 180-184). IEEE

Kallahalla, M, et al. (2003, March). Plutus: Scalable Secure File Sharing on Untrusted Storage. In *Fast* (Vol. 3, pp. 29-42).

Rifi, N., et al. (2017, October). Towards using Blockchain technology for eHealth data access management. In International Conference on Advance in Biomedical Engineering (ICABME17). *4th international conference on Advances in Biomedical Engineering*. IEEE.