Sharing Health Records in Senegal Using Blockchain

Mouhamadou Moustapha Mbaye(✉) and Abdourahime Gaye

Department of Computer Engineering and Communication,
University Alioune DIOP of Bambey, Bambey, Senegal
m3moustapha@gmail.com, abdourahime.gaye@uadb.edu.sn

Abstract. Electronic Health Records offer real advantages for accessing and storing patient health information, which can improve the management of patient care. However, the attractive features of electronic records (accessibility, portability, and portability of patient health information) also present privacy risks. Organizations need to share person-specific health data without disclosing the privacy of their subjects.

Current mechanisms for effective management and protection of health records in Senegal have proven insufficient. In this paper, we propose a system that addresses the issue of sharing health data between hospitals in a trustless environment based on the Consortium Blockchain to improve the quality of care and the efficiency of the health system in Senegal. After a brief introduction, we present some characteristics of Blockchain as well as the different types and securing of Blockchain using cryptographic algorithms. Then an overview of related work is conducted. Finally, we presented the preliminaries of sharing health records with the Blockchain in Senegal. Our work ends with the description of the functioning of our medical record management mechanism with the Blockchain in Senegal and its implementation.

CCS Concepts: Security and privacy · Distributed systems security · Authorization

Keywords: hospitals · blockchain · data sharing · privacy · security · electroNic health records

1 Introduction

In Senegal's hospitals, there is a concern for good management practices to assist health professionals in their care process, so it is necessary to find solutions to the problems essentially posed by the management of health records in public health establishments. To do this, it is essential to make a representation of computer domain knowledge easily interpretable and exploitable, the organization of medical data collection considering the context of the patient and the exploitation of good practice guides and shared clinical experience [18, 19].

Y. Chen et al. (Eds.): BICT 2023, LNICST 512, pp. 156–165, 2023.
https://doi.org/10.1007/978-3-031-43135-7_15

We must therefore trust‘ this enterprise to manage this shared data within the parameters of confidentiality. We can imagine a professional network operating based on a decentralized application. The application could link all users to connect them to each other to facilitate information exchange without the transaction being secured and validated by a central authority. Instead of a central authority, the Blockchain uses a consensus mechanism to reconcile discrepancies between nodes of a distributed application [1, 2].

To solve the above problems, we propose to build a consortium blockchain for security and privacy preserving EHR sharing. This health files could assist the doctors and other authorized health and social services professionals responsible for your care to access to the files in any hospital in order to offer better care and more efficient follow-up.

2 Presentation of the Blockchain

2.1 Characteristics of a Blockchain

It consists of a register composed of a series of time-stamped blocks of transactions. It is this precise aspect of the Blockchain technology, which is the object of the present development, that has led to its name being given, by metonymy, to all these protocols.

A block generally consists of the hash value of the previous block, the payload, the signature of the contributor and the timestamp. A block consists of a format that uniquely identifies the block. This is followed by the block size, which contains the entire size of the block [2]. Once the block is validated, on average every ten minutes for the bitcoin example, the transaction becomes visible to all the holders of the register, potentially all the users, who will then add it to their block chain. The blockchain is defined as a technology that allows the storage and transmission of information in a decentralized manner from one individual to another.

The blocks, thus constituted of several transactions “signed” by public keys are then “time-stamped” by their author and constitute a basic unit to be verified. The Blockchain allows to timestamp digital documents impossible to backdate or to modify the content once data is recorded. This aspect, called timestamping, is essential because it allows the relative dating of the blocks, thus constituted, as all the blocks are chained, the order of the blocks is deterministic; therefore, each block can serve as a timestamp of the transactions included to solve the problem of double spending [3]. Krawiec et al. [4] presented several existing problems with current health information ex-change systems and the advantages offered by blockchain technologies. The protocol invented by Nakamoto proposes a solution to limit the risk of such a simultaneous pro-duction of two blocks, and to ensure that a valid block has time to spread throughout the network before a next one is created (Fig. 1).

2.2 Categories of Blockchain

Generally, blockchain can be classified into three categories:

Blockchain without authorization (Public Blockchain), this type of Blockchain implementation in which any node is free to join the network and participate as a miner without requiring authorization or access authorization.

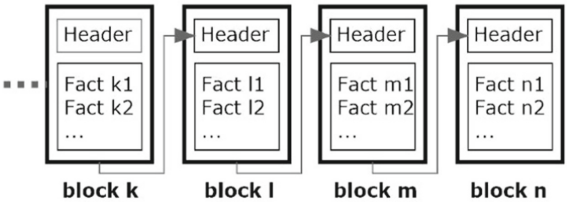

Fig. 1. Example of use of a Blockchain

Authorized blockchain: in this type participants must be authorized and have appropriate access permissions before they can join and participate in the network. In the Authorized Blockchain, only certain nodes can be authorized to participate in the mining process, this type is called the Private Blockchain or the Consortium Blockchain. The distinction between private and consortium blockchains is based on the number of nodes allowed to be miners. If only one node is allowed to be a miner, it is private, whereas if two or more nodes are allowed to participate in the mining process, it is a consortium blockchain [5]. For the consortium blockchain, all the members of its organizations will be able to read the transaction and verify that the sender was indeed the last owner of the transactions sent. Only the receiver will be able to sign the transaction with his private key to prove possession.

2.3 The Consensus Method in the Blockchain

Due to the incompressible latency of the network discussed above, multiple valid blocks could be created simultaneously by multiple nodes. The nodes would add one or another of these blocks and the network would then contain registers in different states.

The consensus mechanism is the core technology of the Blockchain, as it determines whether the new block is validated and who keeps the record [6]. This ensures that the most up-to-date and complete version‘ is the one used as a reference to validate transactions. Thus, this influences the security and reliability of the whole system. Therefore, it is necessary for the nodes to agree on the next block to be added to the chain, which is why Blockchain protocols provide a “consensus method”. In practice, in a public blockchain such as Bitcoin, a mechanism for designating the validated block is used. Its author must provide proof of its designation to the other users of the network [7]. The simplest method of designation would be to draw lots for this validator, at a given interval of time (sufficient for a block to spread throughout the network.

3 Related Work

Xia, et al. [8] discusses a Blockchain-based data sharing framework that addresses the access control challenges associated with sensitive data stored in the cloud by using the built-in immutability and autonomy properties of the Blockchain. The proposed platform uses secure cryptographic techniques (encryption and digital signatures) to provide effective access control to sensitive shared data pools using an authorized Blockchain for enhanced security and a tightly monitored system. It allows users to access electronic

medical records from a shared repository after their identities and cryptographic keys have been verified. Each block, in addition to the transactions and timestamp, has an identifier, which takes the form of a "hash" that links the blocks together. This hash is always the result of the "hash" of the previous block, the hash value of the previous block makes the blockchain unchangeable. The merkle root hash is part of the header, ensuring that none of the blocks in the Blockchain network can be modified without changing the header. This is achieved by taking the hashes of all events in the Blockchain network and adding of the output to the current block. The final output is a sha256 (sha256 ()) [7]. The proposed decentralized system consists of three entities, namely the user, system management and storage.

Zhang, et al. [9] Proposes a Blockchain-based secure and privacy-preserving PHI (BSPP) sharing scheme for diagnosis improvement in e-health systems. The patient's PHI and corresponding keywords are encrypted for data security while they are searchable by authorization for diagnostic improvements. Two types of Blockchain, Private Blockchain and Consortium Blockchain, are built by designing their data structures and consensus mechanisms. Lam Private Blockchain is responsible for storing PHI while the Consortium Blockchain keeps records of secure indexes of PHI.

Yue, et al. [10] propose a blockchain-based App architecture (called Healthcare Data Gateway (HGD)) to enable patients to own, control, and share their own data easily and securely without violating privacy, which offers a potential new way to improve the intelligence of healthcare systems while maintaining the privacy of patient data. The system is a smart smartphone application that allows patients to easily manage and control the sharing of their health data. The authors combine blockchain and off-blockchain storage to build a privacy-oriented personal data management platform, it manages personal electronic medical data on the blockchain storage system, evaluates all data requests by leveraging goal-centric access control, and uses secure multi-party computing to enable a third party to perform treatment on the given patient without risking patient privacy.

4 Sharing Medical Records with Blockchain for Health in Senegal

Given its characteristics, Blockchain technology could provide solutions to problems encountered in sensitive areas, particularly in the health sector. This leads us to reflect on the impact of the Blockchain in the health field. To put it plainly, what would be the contribution of Blockchain technology in the field of health? Several use cases are possible in the health sector. Blockchain could be used to [3, 11]:

- drug traceability;
- securing health data;
- managing patient data.

In recent years, Blockchain has been proposed as a promising solution to achieve personal health information (PHI) sharing with security and privacy preservation due to its immutability advantages [12]. Decentralization is an important feature of the Blockchain for health applications because it enables distributed health applications that do not rely on a centralized authority. Because the information in the Blockchain is replicated

between all the nodes in the network, it creates an atmosphere of transparency and openness that allows healthcare stakeholders, and especially patients, to know how their data is being used, by whom, when and how.

The strength of the Blockchain lies in the fact that the compromise of one node in the Blockchain network does not affect the state of the ledger since the information in the ledger is replicated across multiple nodes in the network. Therefore, by its nature, the Blockchain can protect health data from potential data loss, corruption, or security attacks [13, 14].

5 Modeling the Health Record with the Blockchain in Senegal

In our field of application in this case that of health, the Blockchain would allow with effectiveness to justify the design and the setting in circulation of the medical files, i.e. to ensure its traceability, but also to fight against the attacks and usurpations of identity. In our project we implement our system composed of three entities, namely the hospital (doctor, nurse…), the system management (central authority) and the patient.

a. Node as hospital (doctors, nurses);
b. Minor as central authority (Ministry of Health and authorized physician);
c. Block as patient's medical record (EHR).

Each doctor will have his ID code at the central authority (Ministry of Health). Usually, each hospital has a server and many computers. Each computer is operated by a doctor to record the health information of his patients and then generate blocks for the health records of the patients and broadcast them to the Blockchain. In addition, the selected central authority is responsible for verifying the new blocks to come [9].

The use of cryptographic algorithms to encrypt the data stored on the Blockchain ensures that only users with legitimate permissions to access the data can decrypt it, thus improving the integrity and confidentiality of patient data (Fig. 2).

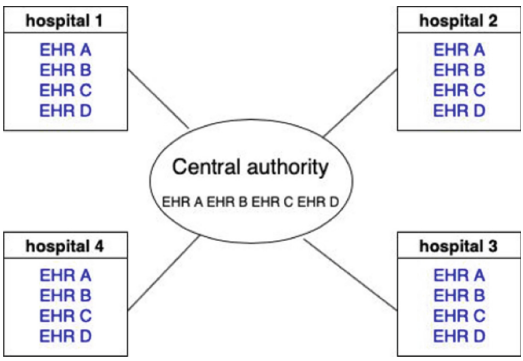

Fig. 2. Design of the medical record management mechanism

6 Operation of the Health Record Management Mechanism with the Blockchain in Senegal

We propose a data sharing mechanism based on the Blockchain consortium to secure electronic health records. The functioning of each entity can be described as follows:

1. Hospitals: are the users who are composed of doctor, nurse and patients who wish to register a patient record or access the data in the record. In the system, health records must be created by professional physicians and cannot be created by anyone else, including the patient himself. Personal health data belong to the patient and is used by requesters with the permission of the data owner. The doctor is part of the hospital layer by authenticating the patients to join the blockchain. He sends the block to the verifier (central authority) to accept patients who request to join the system. New blocks are accepted only after they are verified by the verifiers, who are responsible for checking the validity of the new blocks. The processes of generating, verifying, and adding new blocks to the blockchain is called mining.
2. The Central Authority or The Ministry of Health (verificator): The verifier is part of the data management layer by further authenticating the patient record and receives the physician's transaction key which is retained. The verifier subsequently approves the blocks that have been signed by the physician. This authenticates a block from the system into the Blockchain. To ensure the confidentiality and reliability of the mining processes, a consensus mechanism is essential in the Blockchain network. It determines who keeps the records and how to verify the validity of the new block. The consensus node is responsible for processing and verifying the authenticity and details of a block. Processed blocks are disseminated in the blockchain by the consensus node. An important role of the consensus node is to process and publish results based on irregularities in the system. The consensus node is the only entity allowed to access the system of unprocessed requests.

We have proposed consensus building for the validation of a new medical record as presented´ in the figure below:

- A hospital creates a new block (record) with patient information;
- The central authority verifies that the request has been´ issued in the network by a physician authorized to create a record through his or her identifier (Physician Id);
- If the central authority approves the record, and more than half of the randomly drawn hospital servers verify the new transactions are correct, they are accepted as a new validation block in the blockchain. The file can be shared to the whole network by meeting all the necessary requirements;
- If the consensus is successful, then a new record is entered into the Blockchain.

Since the Blockchain is immutable, it is impossible for a person to be able to open a record already‘ stored to add content without the presence of the patient who holds the private key for example. Indeed, by encrypting the data using asymmetric cryptography, there is no antagonism to sharing private data insofar as it will not be read by other users. Only the person with the private key will be able to decrypt and enjoy the data stored on the blockchain [15] (Fig. 3).

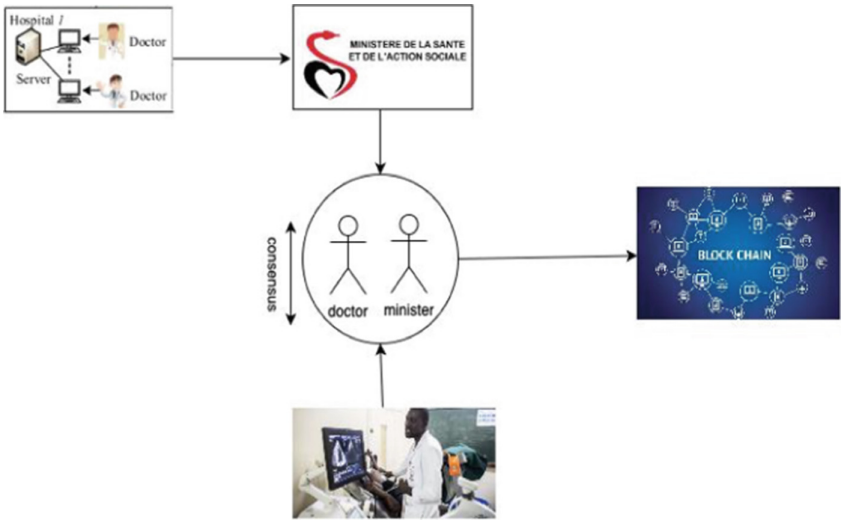

Fig. 3. Overview of a healthcare transaction associated with a Blockchain

7 Implementation of the Health Record Management Mechanism with Blockchain in Senegal

The purpose of this section is to provide a framework for building a system while analyzing the secure structures implemented to facilitate Blockchain-based data sharing for the logic of the electronic medical record system between hospitals in Senegal. We describe designed structures that achieve data sharing by presenting our data access system that aims to provide an appropriate sharing scheme while preserving the required security properties of the Blockchain.

The data structure of the Blockchain consortium is shown in Fig. 4. It consists of the block header, payload, contributor signature and timestamp.

1. The block header is hashed with sha256 (sha256()) as it is done in Bitcoin headers. The block header plays an important role in the Blockchain network in guaranteeing immutability. By changing a block header, an attacker should be able to change all block headers from the genesis block to forge a block record. The block header concludes three components:
   a. the block ID: a block consists of a format that uniquely identifies the block;
   b. the block size: the block size that contains the entire size of the block;
   c. the hash value of the previous block: which is a sha256 hash (sha256()) whose function is to ensure that no previous block header can be modified without changing that block header. If one of the transactions in a block is modified, even slightly, the corresponding hash output will change drastically, which will break the chain to the following blocks of the Blockchain.
2. The payload: is composed of four parts: The identity of the PHI generator (physician) which is the identity of the physician who created or accessed the record, the identity of the PHI owner (patient's first and last name), blood type and keyword which may

include test results for a patient and a corresponding diagnosis from a physician which are encrypted. Notably, not all PHI information is stored in plain text format. Since all hospitals can view the data transmitted by a node, the confidentiality of the data will not be intact, but physicians cannot open it without the patient's permission. The patient can select a representative who can access his information and/or medical history on his behalf, in case of emergency or the doctor contacts the central authority to access the file.

3. The contributor's signature allows to follow the generator (physician) of the block, for each node having contributed to the block, a digital signature is required.
4. The timestamp: indicates the time of generation of the block. When the conditions for this field are met, the block is ready to be distributed in the Blockchain network. The block lock time generally means the time the block enters the Blockchain. An update of the Blockchain by adding the new block into the Blockchain to all participants.

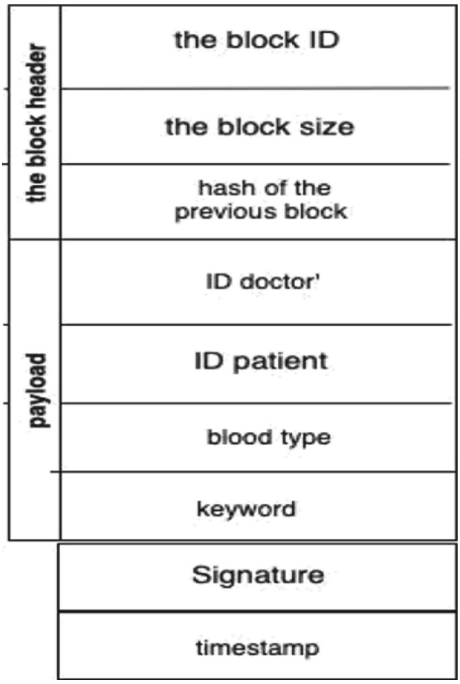

Fig. 4. Structure of a medical record block in the Blockchain consortium

8 Discussion

The fact that the information on the blockchain is replicated among all hospitals in the country creates an atmosphere of transparency and openness, allowing patients to know how their data is being used. When a transaction is performed, the corresponding

healthcare parameters are sent to the validation devices which are the central authority (Ministry of Health) and the hospitals with the use of the Blockchain consortium that is‘ to say that the validation of the data and thus the registration of a new record would only be authorized by the central authority as well as the selected hospitals… Sharing electronic health records can help improve diagnostic accuracy, where security and privacy preservation are critical issues in systems.

Hospital’s store, health records in the Consortium Blockchain, which has the advantages of faster transaction, better privacy preservation, low cost, and better security performance. However, access to the data could be public, at least in part. Patients can access‘ all the data related to the file thanks to their private key, others could for example, just see the name, first name and blood type of the patient. The blood type is in clear in the file because it allows in case of an accident to solve emergency problems without resorting to decryption protocols.

Each system adopts a different algorithm that meets the requirements. The proposed protocol ensures data security and access control. The essential features of the Blockchain guarantee the immunity of the proposed protocol. In other words, the data stored in the Blockchain are immutable unless there is a significant attack (51%) that occurs when there are fewer honest nodes than malicious nodes in the whole network [16, 17]. This protocol ensures the effectiveness and reliability of the proposed system to work in different environments and can provide satisfactory security protection.

9 Conclusion

In this paper, we illustrate how to apply the Blockchain technique in healthcare. We proposed a secure and privacy-preserving Blockchain-based EHR sharing protocol for diagnostic improvements in the Senegalese healthcare system. Advantages of this strategy include easy authentication since a physician only needs to provide his ID associated with his identity to the central authority to access the system.

The digital health record, once implemented in Senegal, will be used to make available, in real time, all of a user’s medical data, from birth to death, to share data with all health professionals involved in providing care in order to provide management, quality and performance indicators, to feed registers, such as cancer, and the daily emergency situation report.

In our future work, we are analyzing the performance of our system and comparing it with current state-of-the-art solutions for data sharing between hospitals.

References

1. Swan, M.: Blockchain: Blueprint for a new economy. O’Reilly Media, Inc. (2015)
2. Angraal, S., Krumholz, H.M., Schulz, W.L.: Blockchain technology: applications in health care. Circul. Cardiovascul. Qual. Outcomes **10**(9), e003800 ((2017))
3. Kuo, T.-T., Kim, H.-E., Ohno-Machado, L.: Blockchain distributed ledger technolo-gies for biomedical and health care applications. J. Am. Med. Inform. Assoc. **24**(6), 1211–1220 (2017)
4. Transaction, C.P., MPI, M.P.I.: Blockchain: opportunities for health care, CP Transaction (2016)

5. Helliar, C.V., Crawford, L., Rocca, L., Teodori, C., Veneziani, M.: Permission-less and permissioned blockchain diffusion. Int. J. Inf. Manage. **54**, 102136 (2020)
6. Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M.: Proof of activity: Extending bit-coin's proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Perform. Eval. Rev. **42**(3), 34–37 (2014)
7. Zhou, T., Li, X., Zhao, H.: Med-ppphis: blockchain-based personal healthcare in-formation system for national physique monitoring and scientific exercise guid-ing. J. Med. Syst. **43**(9), 1–23 (2019)
8. Xia, Q., Sifah, E.B., Smahi, A., Amofa, S., Zhang, X.: Bbds: blockchain-based data sharing for electronic medical records in cloud environments. Information **8**(2), 44 (2017)
9. Zhang, A., Lin, X.: Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. J. Med. Syst. **42**(8), 1–18 (2018)
10. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found health-care intelligence on blockchain with novel privacy risk control. J. Med. Syst. **40**(10), 1–8 (2016)
11. Siyal, A.A., Junejo, A.Z., Zawish, M., Ahmed, K., Khalil, A., Soursou, G.: Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography **3**(1), 3 (2019)
12. Esposito, C., De Santis, A., Tortora, G., Chang, H., Choo, K.-K.R.: Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. **5**(1), 31–37 (2018)
13. Liu, W., Zhu, S., Mundie, T., Krieger, U.: Advanced block-chain architecture for e-health systems. In: 2017 IEEE 19th International Conference on e-Health Net-working, Applications and Services (Healthcom), pp. 1–6. IEEE (2017)
14. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: Medrec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30. IEEE (2016)
15. Burniske, C., Vaughn, E., Cahana, A., Shelton, J.: How Blockchain Technology can Enhance Electronic Health Record Operability. Ark Invest: New York, NY, USA (2016)
16. Buterin, V., et al.: A next-generation smart contract and decentralized application platform. White Paper **3**(37) (2014)
17. Greenspan, G.: Multichain private blockchain-white paper, pp. 57–60 (2015). http://www.mul-tichain.com/download/MultiChain-White-Paper.Pdf
18. Aly Konte, M. : Secteur de la santé au sénégal: malaises actuels et perspectivesfutures; rapport de conférence (2006)
19. Hane, F.: Production des statistiques sanitaires au sénégal: entre enjeux politiques et jeux d'acteurs. Santé publique **29**(6), 879–886 (2017)