Patient Medical Records: Implementation of a Security Solution Based on the Hyperledger Fabric Blockchain

Abdou-Rahamane Ambarka Tenga, Tahirou Djara, Abdou-Aziz Sobabe

Abstract: In this paper, we have developed a solution for securing patient medical records based on blockchain. In our approach, we first carried out a comparative study of different blockchains. This comparative study, based on the Ethereum, Corda and Hyperledger Fabric blockchains, enabled us to select Hyperledger Fabric as the development framework for our blockchain. The criteria justifying our choice are essentially: the modularity of the architecture, the variety of programming languages for smarts contracts, the possibility of creating private channels between members of a network, high access control and data confidentiality, and a flexible consensus model. These criteria are crucial as they guarantee both the robustness and flexibility of the network in a shared medical record context. The proposed solution is a decentralized application that exchanges data in a consortium-type blockchain network, with three different organizations in a healthcare pathway: a hospital, a pharmacy and a laboratory. Other organizations can be added to the network taking into account the need to share and secure healthcare information. Our solution uses the IPFS (Interplanetary File System) protocol for distributed document storage, increasing data security and availability. To facilitate exchanges between network nodes, particular emphasis was also placed on the choice of consensus algorithm. First we chose the Solo Orderer algorithm, which uses a single Ordering Service node to process transactions and add them to blocks, and then we used the Kafka orderer algorithm, which offers high scalability and robust resilience in production environments. The choice of these two consensus algorithms enabled us to set up and deploy a blockchain network that stores and secures sensitive data from medical analyses or examinations in a patient's care pathway.

Keywords: Medical Data, Blockchain, Smart Contracts, Hyperledger Fabric, IPFS, Interoperability, Transparency, Trust, Consensus Algorithm.

Manuscript received on 16 September 2023 | Revised Manuscript received on 27 September 2023 | Manuscript Accepted on 15 October 2023 | Manuscript published on 30 October 2023.

*Correspondence Author(s)

Abdou Ambarka*, Department of Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée (LETIA/EPAC), Université d'Abomey-Calavi (UAC). Institut d'Innovation Technologique (IITECH), Cotonou, Benin. E-mail: abdou.ambarka@gmail.com, ORCID ID: 0009-0000-1932-1144

Tahirou Djara, Department of Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée (LETIA/EPAC), Université d'Abomey-Calavi (UAC). Institut d'Innovation Technologique (IITECH), Cotonou, Benin. E-mail: csm.djara@gmail.com, ORCID ID:0000-0002-8591-6610

Abdou-Aziz Sobabe, Department of Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée (LETIA/EPAC), Université d'Abomey-Calavi (UAC). Institut d'Innovation Technologique (IITECH), Cotonou, Benin. E-mail: azizsobabe@yahoo.fr, ORCID ID: 0000-0002-1505-3143

I. INTRODUCTION

Blockchain technology has gained in popularity thanks to its ability to provide a secured and transparent platform for storing and sharing data. The healthcare industry is one of the sectors that can benefit from this technology. Medical records contain sensitive information that must be secured and accessible only to authorized persons. In addition, traceability in the patient's medical pathway is an essential element for healthcare professionals to provide the best care.

Web2 solutions suffer from a lack of security and data privacy: the example of Wannacry [1] in 2017, a cyberattack that affected the medical data management system with more than 200,000 computers in 150 countries and billions of dollars of loss. Web3 technologies can overcome these shortcomings, specifically blockchain. There are several types of blockchain that meet the needs of different use cases. Hyperledger Fabric is not only an open-source consortium blockchain framework of which features, and functionalities are interesting for Business to Business (B2B) applications but also for the needs of a safe and secured medical data storage and sharing application. This is the main goal of this article.

II. SOME DEFINITIONS

A. Medical Record

All medical information relating to a patient, used to follow/establish a diagnosis or a treatment, or which has been the subject of written exchanges between health professionals, is called the medical record [2].

It is an essential tool for coordinating care and monitoring patient progress. It allows us to trace the patient's medical history.

B. Blockchain

The blockchain is a distributed ledger technology, which can be seen as a shared and immutable ledger. But it is primarily a chain of time-stamped blocks. Indeed, as we can see in Figure 1, the blocks of the chain are cryptographically linked to each other so that block n+1 contains the hash of block n (previous block). Thus, any attempt to modify data in a block of transactions causes the hash of the block to be modified and consequently invalidates the entire chain (see Figure 2). This is what gives the blockchain its characteristic of immutability [3][4][17].

$$B_{n+1} = E(Tx)_{n+1} + H(B_n) + H(B_n + 1) \quad (1)$$

$$H(B_{n+1}) = H(E(Tx)_{n+1} + H(B_n)) \quad (2)$$

(1) the block B_{n+1} consists of the set E of transactions Tx, the hash of the previous block and the hash of the current block (n+1).

(2) the hash of block n+1 $H(B_{n+1})$ is formed from the transactions of the block and the hash of the previous block.

NB: The operator (+) does not refer to simple mathematical addition.

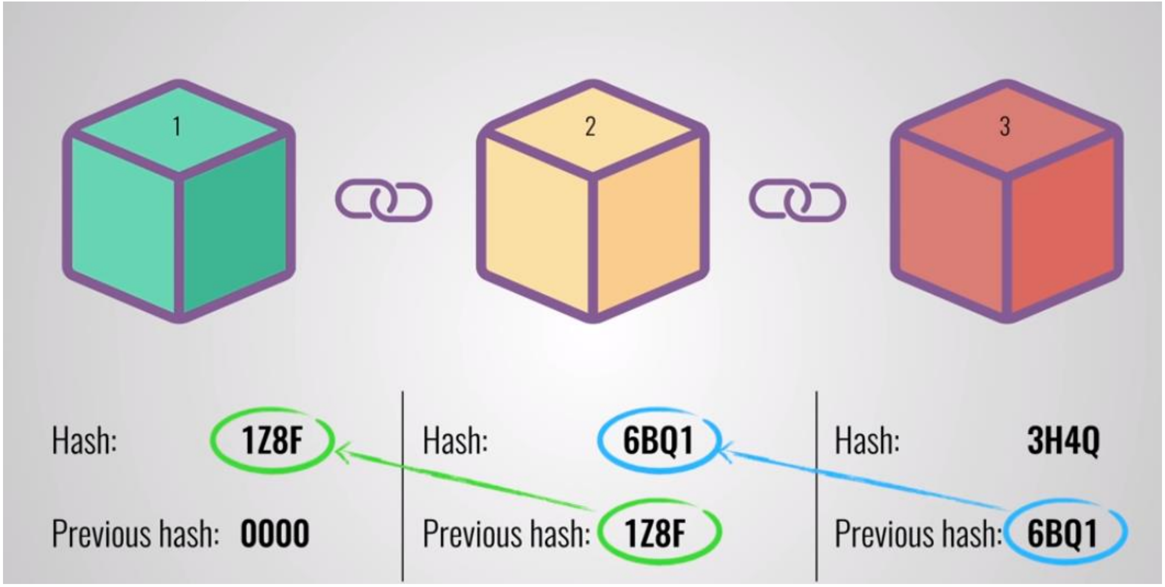


Fig. 1. Cryptographically linked blocks [5]

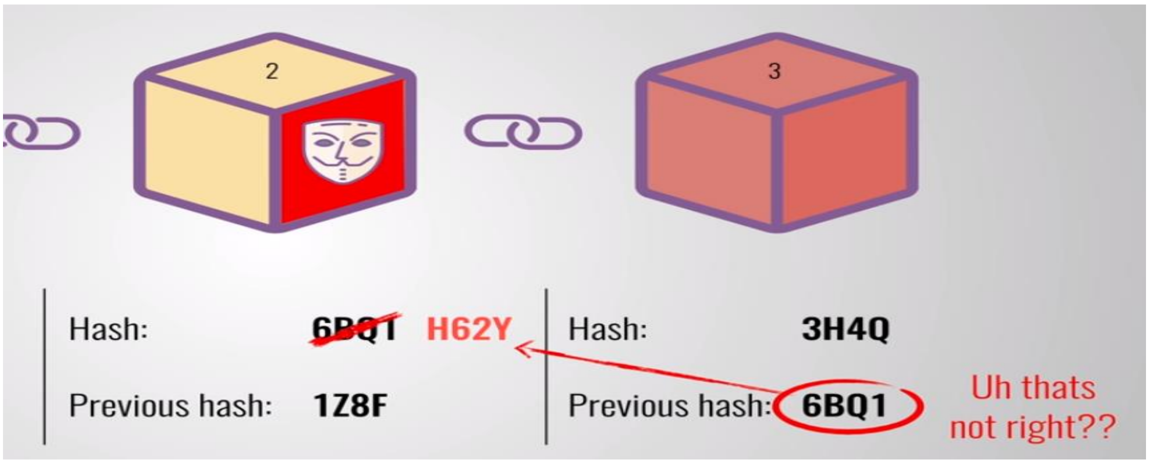


Fig. 2. Detection of an attempted modification in a block [5]

III. HYPERLEDGER FABRIC

A. Definition and Operation

Hyperledger Fabric is an open-source distributed ledger technology (DLT) platform designed for enterprise use cases and enables the creation of authorized networks, where only authorized participants can have access and transact on the network. It ensures high levels of access and privacy controls, so that only the data you want to share is shared among authorized participants in the network. Smart contracts are the logic at the heart of the application. They allow executing traceable and irreversible transactions between network participants [6]. The transactional mechanics within Hyperledger Fabric take place in several steps (see Figure 3): First, the client, after logging in with an SDK (Node.js or other), initiates a transaction via the SDK API and sends it to a validator node[16]. The other nodes also receive the transaction proposal, check the client's signature, simulate the transaction with the chaincode and send back a signed response. Depending on the defined approval policy, the transaction is accepted or rejected. If accepted, the transaction proposal and signed responses are sent to the ordering service to be ordered into blocks. These blocks are then distributed to nodes in the network, which further check the validity of the block before adding it to the chain.

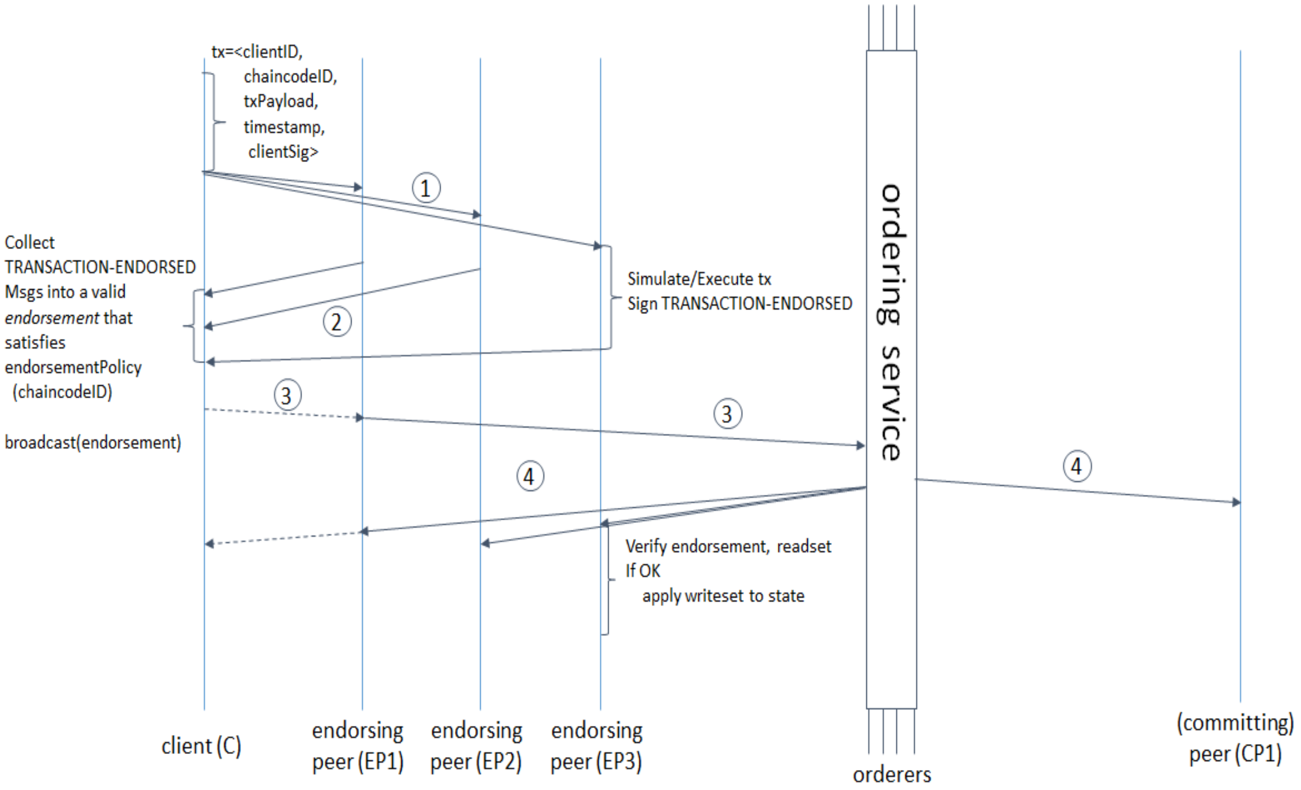


Fig. 3. Flow of a transaction [7]

Some of the main hashing algorithms used by Hyperledger Fabric are presented as follows:

- Elliptic Curve Cryptography (**ECC**): ECC is a public key cryptography algorithm used for digital signatures in Hyperledger Fabric. ECC is based on the mathematics of elliptic curves and provides a more efficient alternative to traditional public key cryptography algorithms such as RSA.

$$y = x^3 + ax + b \ (3)$$

- Asymmetric cryptography to ensure that only the sender and receiver of the message can decrypt it: suppose a message M, a sender E, a receiver R, K_{pu}^{E}, K_{pr}^{E}, K_{pu}^{R} and K_{pr}^{R} the public and private keys of the sender and the receiver. The sender encrypts the message M thanks to a function C using the public key of the receiver :

$$V \ = C(\ K_{pu}^{R}\ , M)\ (4)$$

When the receiver receives the value V, he is the only one able to decrypt it thanks to a function D using his private key :

$$M \ = D(\ K_{pr}^{R}\ , V)\ (5)$$

In order for the receiver to ensure the authenticity of the message, the sender sends his signature S established thanks to his private key so that only his public key can decrypt it.

$$S \ = C(\ K_{pr}^{E}\ , M)\ (6)$$

The receiver uses the public key of the supposed sender to decrypt S and obtains m.

$$m \ = D(\ K_{pu}^{E}\ , S)\ (7)$$

If m=M, then the authenticity of the message is assured [8].

- Secure Hash Algorithm (**SHA)**: SHA is a family of cryptographic hash functions used to ensure data integrity in Hyperledger Fabric. SHA-256 is the most commonly used SHA algorithm in Hyperledger Fabric and generates a 256-bit message digest.

Merkle Trees: Merkle trees (see Figure 4) are a type of data structure used in Hyperledger Fabric to ensure the integrity of the blockchain. Merkle trees are based on the mathematics of hash functions and are used to efficiently verify the integrity of the blockchain.

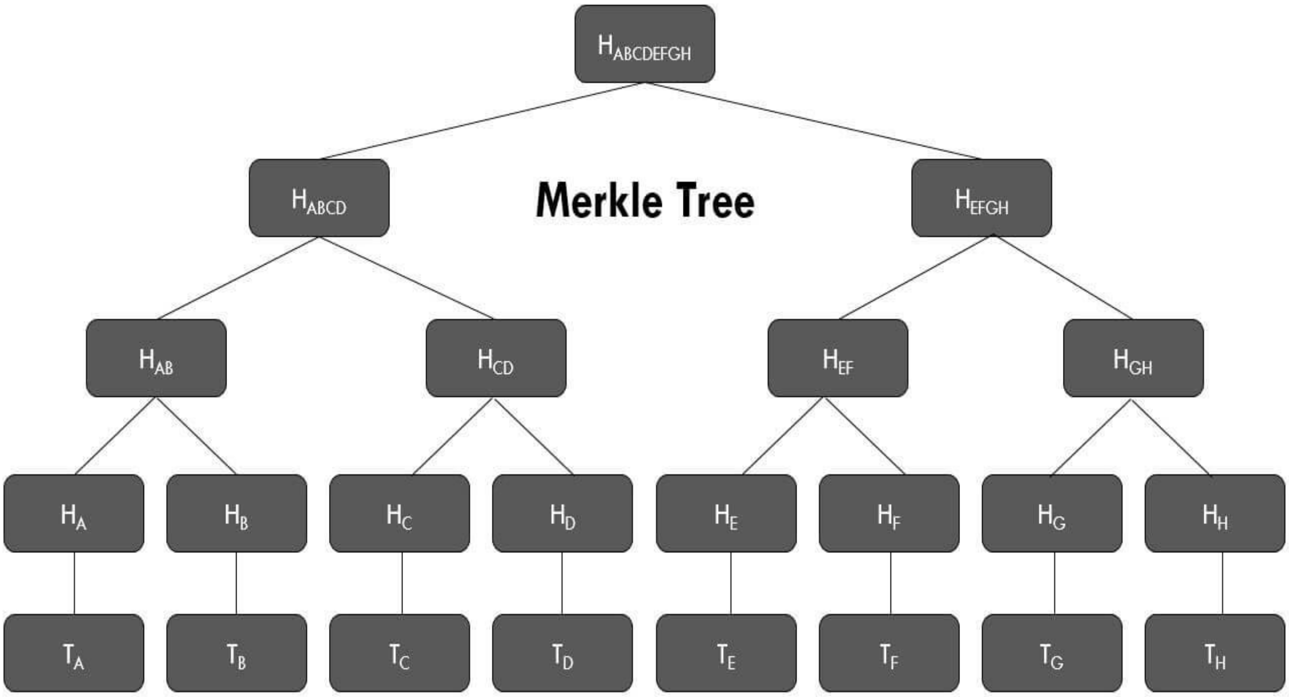


Fig. 4. Flow of a transaction [9]

B. Specific Characteristics

Hyperledger Fabric has the following advantages:

- an authorized network allowing to establish trust between known participants thanks to the system of rights attribution;
- confidentiality of transactions ;
- flexible and modifiable architecture according to the needs;
- a variety of smart contract programming languages;
- free of charge.

C. Hyperledger Fabric vs Corda vs Ethereum

Table-I presents a comparison of Hyperledger Fabric, Corda, and Ethereum based on some relevant criteria. To sum up, Hyperledger Fabric is a highly configurable blockchain that offers advanced privacy features and uses a PBFT consensus method to ensure enhanced security. The platform also allows for customization of smart contracts and offers great scalability through a modular architecture

Table-I: Comparison of Hyperledger Fabric with Other Blockchains [10]

Blockchain	Architecture	Langage	Network	Consensus	Smart contracts	Scalability	Privacy
Hyperledger Fabric	Modularized, which allows nodes to be added dynamically for greater scalability.	Go, Java Javascript , Typescrip t	Permission is granted	PBFT (practical byzantine fault tolerance) which guarantees high security and low power consumption	Chaincode (Smart contracts)	Horizontal	Highly configurable, as participants can choose who can access certain parts of the network and data.
Corda	Decoupled	Java, Kotlin	Permission is granted	One-way transaction chains	Smart contracts notary	Vertical	High
Ethereum	Monolith	Solidity	Permitted or not permitted	Proof of work	Smart contracts	Low	Not configurable

D. Why Is Hyperledger Fabric Best Suited for Patient Health Records?

Hyperledger Fabric provides end-to-end security features, such as the ability to encrypt data stored on the blockchain and protect user authentication and authorization through advanced cryptographic algorithms. It also enables better interoperability between different medical data management systems through its modularity and interoperability features. One of the main features of Hyperledger Fabric is the ability to create private communication channels between members of the blockchain network. This feature allows access to sensitive medical information to be limited to only authorized healthcare professionals and patients, while protecting the privacy of user data. The ability to create private channels of communication is a key feature of Hyperledger Fabric for managing sensitive medical data. Private channels allow access to sensitive medical information to be limited to authorized members only, enhancing patient data privacy and preventing the risk of information leakage. These channels can be used to create patient- or healthcare professional-specific discussion groups, for example. Authorized members can exchange confidential medical information securely without the risk of interference or unauthorized access [11][18]. In addition, private channels allow for fine-grained control over access to medical information, allowing only authorized members to have access to specific information. Permissions can be managed using smart contracts, making it easy to implement customized security and privacy rules. In addition, Hyperledger Fabric uses a pluggable consensus model, which allows the most suitable consensus to be chosen for each use case [12]. This allows different medical data management systems to use different consensus algorithms, while being connected to the same blockchain network. This flexibility enhances system interoperability and ensures compatibility between different systems.

IV. ASSESSMENT OF THE ART ON SECURING MEDICAL RECORDS USING BLOCKCHAIN

Among the existing solutions is the decentralized platform Patientory [13] based on the Ethereum blockchain to store patients' medical information and allow them to give access to other health professionals.

Azaria A. et al [14] in their work proposed a blockchain-based solution that as Patientory offers the possibility to store and share medical data with control over access by the patient. Jathin Sreenivas et al [15][19] based on the Hyperledger Fabric platform to offer a secure storage service for medical information, with smart contracts allowing access to the data and control over this access by the owner (the patient).

V. THE PROPOSED SECURITY SOLUTION

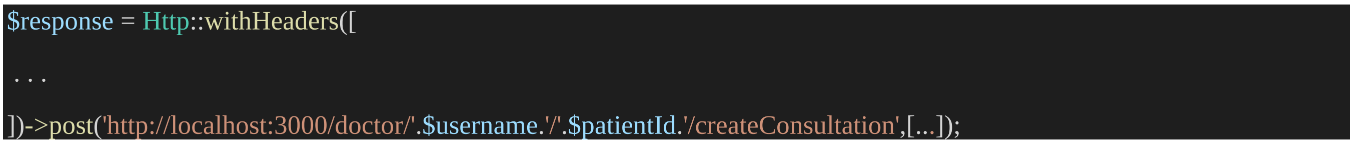
We propose a solution for securing medical records based on the Hyperledger Fabric blockchain following an architecture presented in Figure 9.

A. Global Operation

Any user interacts with the system through the frontend application. The identity information in his wallet is used to establish the connection with the blockchain network. Thanks to the API, the smarts contracts corresponding to the action the user wants to perform are called. In the specific case of a laboratory technician who wishes to upload an analysis result to the platform, the requests are made to save the document on IPFS and the unique identifier of the document is then saved on the blockchain so that only the rightful owner can access it. The Identification and Authentication System by Fingerprints and Veins (SIAEDV) is designed to secure certain processes, notably the sharing of medical data by the patient and the emergency access process by the administrator.

B. Web Application (Laravel)

This is the layer closest to the user, the frontend made up of different graphical interfaces from which each user (patient, doctor, pharmacist, laboratory technician) can perform operations according to his role. We used the php framework Laravel which is based on an MVC (Model-View-Controller) architecture. At the level of the controller, the operations of reading or saving data are indeed API calls to the NodeJS server which takes care of the communication with the blockchain network.



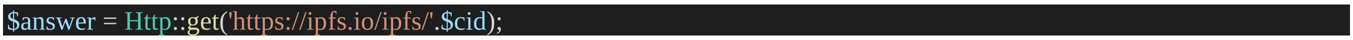
```
$response = Http::withHeaders([

 . . .

])->post('http://localhost:3000/doctor/'.$username.'/'.$patientId.'/createConsultation',[...]);
```

Fig. 5. Call to the Node JS API.

Also, we communicate with a public IPFS gateway for saving documents such as analysis results to preserve the speed of transactions within the blockchain.



```
$answer = Http::get('https://ipfs.io/ipfs/'.$cid);
```

Fig. 6. Connection to the IPFS gateway.

C. Nodejs Backend

We developed an API in NodeJS of which endpoints allow the laravel application to make requests to the blockchain based on the user's role. The **Fabric SDK** is used to interact with the network nodes, registering users.

```
// Function to connect to the blockchain network
async function connectNetwork(ccpP, walletOrg, identity_name) {
 . . .
 // Create a new gateway for connecting to our peer node.
const gateway = new Gateway();
await gateway.connect(ccp, { wallet, identity: identity_name, discovery: { enabled: true, asLocalhost: true } });
 . . .
}
// Function to create a user
async function registerUser(orgId="org1", username="appUser", walletOrg) {
 . . .
}
```

Fig. 7.: Network Connection and User Registration.

D. Fabric Network

We set up a Fabric network of three organizations (Hospital, Pharmacy, Laboratory) each having a node in the network (peer0.org1, peer0.org2, peer0.org3). Each node has a copy of the Ledger (L) and has installed the chaincode package (C). Indeed, any interaction with the ledger must be done by calling a smart contract. The chaincode is the set of defined smart contracts. We have implemented several smart contracts in Javascript, depending on the user's role:

- for a patient, we have the **PatientSmartContract** containing the patient's different authorized actions, namely granting access to his medical data, and consulting the access history, etc;

```
// ----------------- Access history -----------------//
async getHistoryOfAccesses(ctx, patientId){
 let resultsIterator = await ctx.stub.getHistoryForKey("...");
 let asset = await this.getAllPatientResults(resultsIterator, true);
 let accesstab =[];
 for (let i = 0; i < asset.length; i++) {
 let obj = asset[i];
 if(obj.Record.patientId == patientId){
 asset[i]={
 accesslogId: obj.Record.accesslogId,
 accessor: obj.Record.accessor,
 mention : obj.Record.mention,
 biometric : obj.Record.biometric,
 queryType : obj.Record.queryType,
 patientId : obj.Record.patientId,
 docType: obj.Record.docType
 }
 accesstab.push(asset[i]);
 }
 }
 return accesstab;
}
```

Fig. 8. Access History-Patient Smart Contract.

- **DoctorSC** allows a doctor to create consultations, prescriptions, analysis vouchers, etc;
- **PharmacianSC** and **LaboratorianSC** are dedicated to the pharmacist and the laboratory technician for respectively the interaction with an assigned prescription and the insertion of a test result;
- **AdminSC** is the smart contract used by an admin to create users and the hospital admin especially in case of emergency can grant a doctor access to a medical record.

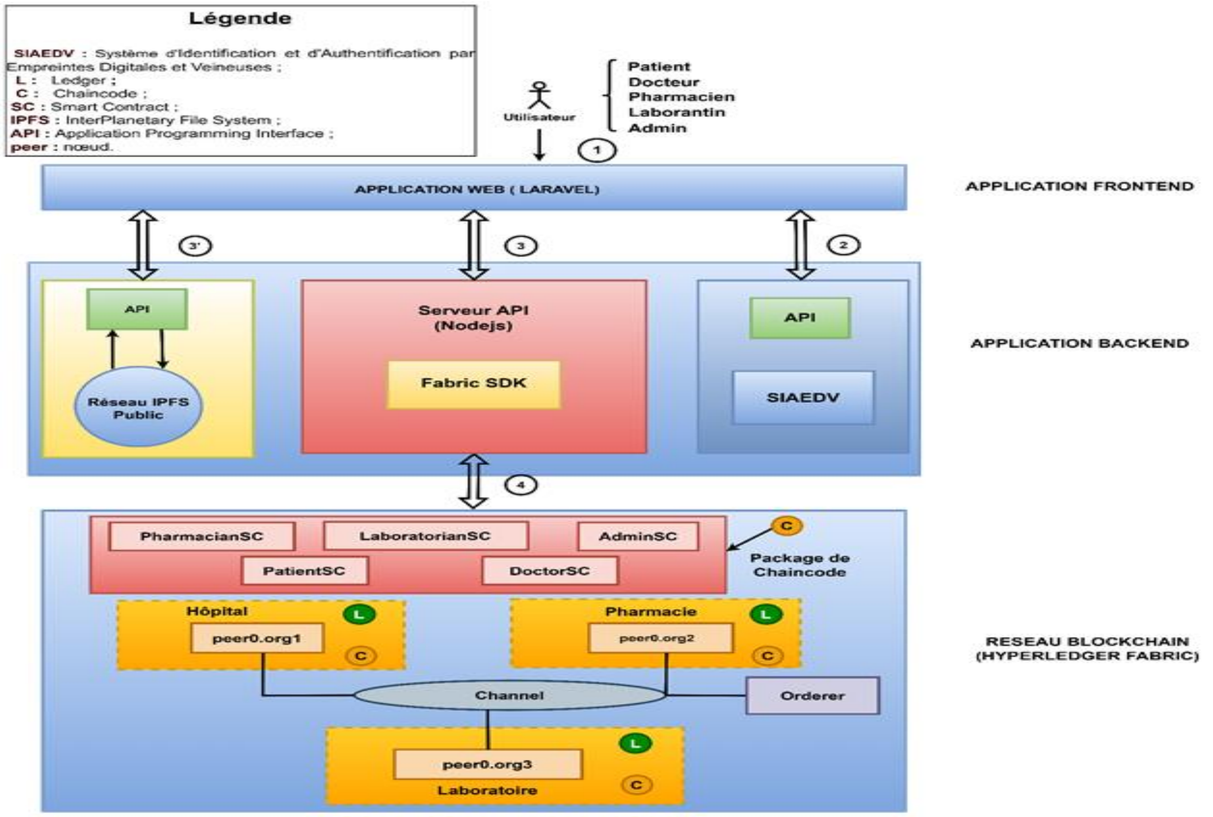


Fig. 9. Solution Architecture.

E. Consensus

Consensus is the mechanism by which the nodes of a network agree on the current state of the network. In Hyperledger Fabric, this consists in ensuring that the transaction is valid, and that the order and results of a block's transactions have met the explicit policy criteria checks. We have channel-level approval policies to define which nodes are endorsers and how the decision is made after collecting responses from these nodes. Then, at the ordering service level, where transactions are ordered, we need to ensure, using a consensus algorithm, that there is a minimum number of nodes sufficient to ensure block integrity and service availability. Several algorithms exist, including Solo, Kafka, Raft, PBFT, Clique, Istanbul BFT, Simple BFT, Proof of Elapsed Time. In our solution, we have implemented the Solo orderer algorithm, which uses a single Ordering Service node to process transactions and add them to blocks. From a real-world deployment perspective, we need to take into account the case where nodes may fail. This calls for algorithms such as Kafka orderer, which delivers high scalability and robust resilience in production environments.

The Kafka algorithm enables messages to be broadcast between ordering service nodes in a Hyperledger Fabric network. It is based on Apache Kafka, a highly scalable, distributed message dissemination platform.

When a transaction is submitted to the Fabric network, it is broadcast to ordering service nodes via Kafka. These nodes, known as broker nodes, receive the transactions and order them according to a specific sequence. The Kafka algorithm ensures that all transactions are processed consistently and sequentially.

F. SIAEDV

The Vein and Fingerprint Identification and Authentication System is a third-party service used to enhance the security of data access. It can be used in emergency situations to authorize a health care professional to have access a record, to identify a patient coming to a new hospital, while sharing data between the patient and health care professionals.

G. Result and Discussion

As result, our research has enabled us to develop a prototype to be deployed in a university environment in a pilot phase. Feedback will enable us to improve data exchanges in the blockchain network for large-scale deployment. In future research papers, we will proceed to a production deployment of our solution to evaluate its real performance. As perspective to this work, we would like to associate the IoT (Internet of Things) with the project. We intend to use a connected object (bracelet for example) to retrieve the variations of the patient's vital signs in real time in order to help the doctor in his analysis.

VI. CONCLUSION

The proper management of medical records being a very serious and vital issue, we have explored the possibilities offered by the blockchain to secure it, to ensure the availability of information, its traceability as well as interoperability between health professionals. We have opted for the design of a consortium-type blockchain using the Hyperledger Fabric framework, which offers the advantage of confidentiality and flexibility of architecture. This work can be improved by integrating the Internet of Things, for example, to capture data directly during a doctor's consultation. This data could then be directly secured in the blockchain network without human intervention.

DECLARATION STATEMENT

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors having equal contribution for this article.

REFERENCES

1. "WannaCry: Everything you need to know about the worst cyberattack in history." Accessed: 06/06/2022 at 4:22 PM, URL: https://www.cyberuniversity.com/post/wannacry-tout-savoir-sur-la-pire-cyberattaque-de-lhistoire.
2. N. Griffon and S. Darmoni, "Le Dossier Médical Santé Publique-Informatique Médicale."
3. Nicolas, "What is immutability? - Cointribune," Nov. 07, 2021. Accessed: 29/01/2023 at 09:00, URL: https://www.cointribune.com/quest-ce-que-limmuabilite/.
4. Smile, "BLOCKCHAIN The Sharing Economy Revolution." Available at: https://smile.eu/fr/nos-references.
5. "How does a blockchain work?", Simply Explained, Accessed on 28/01/2023, URL: https://www.youtube.com/watch?v=SSo%5C_EIwHSd4.
6. "What is Hyperledger Fabric? - IBM", Retrieved 03/02/2023, URL: What is hyperledger fabric? | IBM
7. Transaction Flow - Hyperledger Fabric Docs Main Documentation, accessed 04/02/2023, URL: Transaction Flow - hyperledger-fabricdocs main documentation
8. "How to represent a Blockchain through a mathematical model", COPERNEEC, April 2020, Available at: Blockchain-Coperneec.pdf (canopee-group.com)
9. Understanding Merkle Tree & Its Importance in Blockchain, Forex Academy, Accessed 24/04/2023, URL: https://www.forex.academy/understanding-merkle-tree-its-importance-in-blockchain/
10. "Hyperledger vs. Corda vs. Ethereum: The Ultimate Comparison," 101blockchains.com, Accessed 04/02/2023, URL: Hyperledger vs Corda vs Ethereum: The Ultimate Comparison (101blockchains.com)
11. Mueen Uddin et al, "Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records," February 15, 2021, DOI:10.32604/cmc.2021.015354 https://doi.org/10.32604/cmc.2021.015354
12. Introduction - Hyperledger Fabric Docs Main Documentation, accessed 04/02/2023, URL: https://hyperledger-fabric.readthedocs.io/en/release-2.5/whatis.html
13. "Patientory | Your Health At Your Fingertips."
14. Accessed: 02/02/2023, URL: https://patientory.com/.
15. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). "MedRec: Using Blockchain for Medical Data Access and Permission Management." Available at: https://doi.org/10.1109/OBD.2016.11. https://doi.org/10.1109/OBD.2016.11
16. Prof. Dr. Martin Kappes, "Blockchain Solution to Healthcare Record System using Hyperledger Fabric," Mar. 2021. K. N*, J. K. Murthy, and V. N. Naik, "Hyperledger F abric Block chain for data S ecurity in IOT D evices," International Journal of Recent Technology and Engineering (IJRTE), vol. 9, no. 1. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 2571–2577, May 30, 2020. doi: 10.35940/ijrte.a3040.059120. Available: http://dx.doi.org/10.35940/ijrte.A3040.059120
17. Dr. K. G. Formunyam*, "The Fourth Industrial Revolution and the Future of Engineering Education in South Africa," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 7. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 1116–1120, May 30, 2020. doi: 10.35940/ijitee.g4895.059720. Available: http://dx.doi.org/10.35940/ijitee.G4895.059720
18. I. Patel, S. Jain, J. K. Vishwajeet, V. Aggarwal, and P. Mehra, "Securing Electronic Healthcare Records in Web Applications," Regular issue, vol. 10, no. 5. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 236–242, Jun. 30, 2021. doi: 10.35940/ijeat.e2781.0610521. Available: http://dx.doi.org/10.35940/ijeat.E2781.0610521
19. T. Bharadwaj and A. Balaji, "Healthcare Prediction and Analysis System with Constant Data Polling," International Journal of Inventive Engineering and Sciences, vol. 5, no. 11. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 1–8, Sep. 20, 2020. doi: 10.35940/ijies.k0993.0951120. Available: http://dx.doi.org/10.35940/ijies.K0993.0951120

AUTHORS PROFILE

Abdou AMBARKA is a PhD student at the Doctoral School of Engineering Sciences located at the University of Abomey-Calavi in Benin. He conducts his research at the Laboratory of Electronics, Telecommunications and Applied Data Processing Technology (Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée – LETIA/EPAC). His research interests include: artificial intelligence, blockchain, biometric and software engineering. His areas of specialization include multimodal biometrics, object detection, and distributed and decentralized architecture. In the field of artificial intelligence, he uses transfers learning methods applied to objects detection for detecting plasmodium stage of malaria

Tahirou Djara is a Senior Lecturer at the Polytechnic School of Abomey-Calavi located in the University of Abomey-Calavi, Bénin. His research interests include biometrics, signal and image processing, computational intelligence, industrial applications and symbolical programming. He is member of the research laboratory: Laboratory of Electronics, Telecommunications and Applied Data Processing Technology (Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée– LETIA/EPAC). He received the PhD degree in signals and image processing from the University of Abomey-Calavi, in 2013. He is a consultant in quality assurance in higher education and consultant in the field of science and engineering technology.

Abdou-Aziz Sobabe holds a PhD in Engineering Sciences from the University of Abomey-Calavi in Benin. He conducts his research at the Laboratory of Electrical Engineering, Telecommunications and Applied Computer Science (LETIA). His research interests include biometrics, signal and image processing, affective computing and software engineering. His areas of specialization include multimodal biometrics, non-contact biometrics, score fusion and user-specific parameters in biometric systems. In the area of software engineering, he is interested in object-oriented programming and relational databases for applications. In the field of artificial intelligence, he uses machine learning methods applied to computer security (biometric authentication), e-Agriculture, e-Health

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.