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

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

Abstract: This paper presents a solution for securing patient medical records using blockchain technology. In our approach, we first conducted a comparative study of various 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 smart contracts, the possibility of creating private channels between network members, 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 decentralised application that exchanges data in a consortium-type blockchain network, involving three different organisations 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 utilises the IPFS (Interplanetary File System) protocol for distributed document storage, thereby enhancing 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 utilises a single Ordering Service node to process transactions and add them to blocks. 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 secure and transparent platform for storing and sharing data. The healthcare industry is one sector that can significantly benefit from this technology. Medical records contain sensitive information that must be secured and accessible only to authorized persons. Additionally, traceability in the patient's medical pathway is a crucial element for healthcare professionals to deliver 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. Several types of blockchain meet the needs of different use cases. Hyperledger Fabric is not only an open-source consortium blockchain framework with features and functionalities that are interesting for Business-to-Business (B2B) applications, but also for the needs of a safe and secure medical data storage and sharing application. This is the primary 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 that can be viewed 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 altered and consequently invalidates the entire chain (see Figure 2). This is what gives the blockchain its characteristic of immutability [3][4].

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

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

(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 $H(B_{n+1})$ It 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.

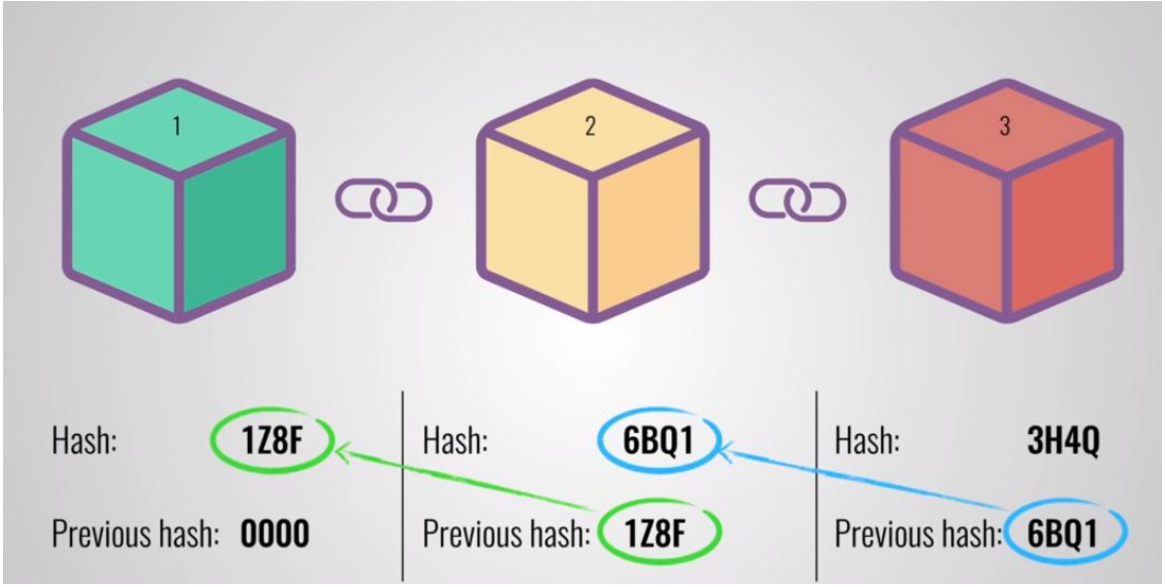


Fig. 1. Cryptographically linked blocks [5]

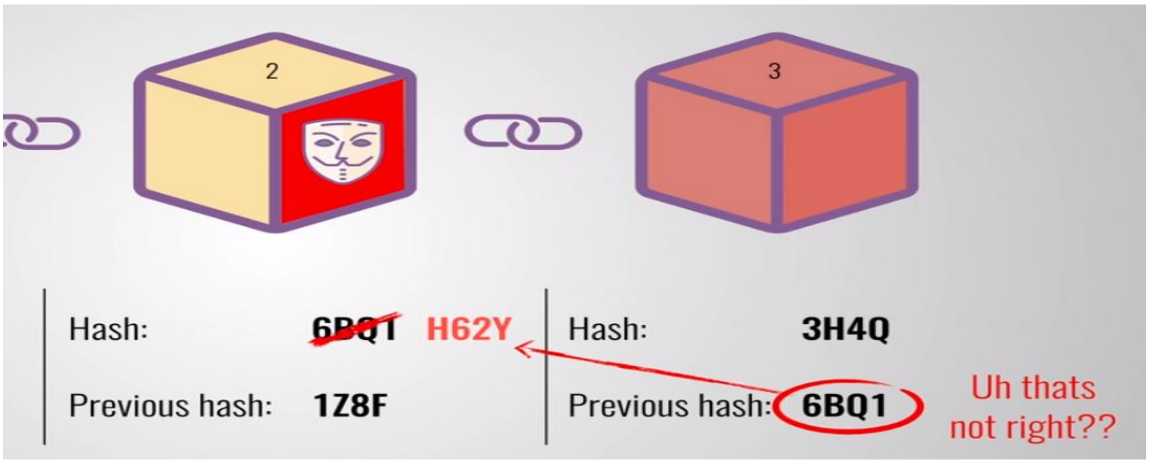


Fig. 2. Detection of an attempted modification in a block [5]

III. HYPERLEDGER FABRIC

A. Definition and Operation

Hyperledger Fabric is an open-source distributed ledger technology (DLT) platform designed for enterprise use cases, enabling the creation of authorised networks where only authorised participants can 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 underlying logic of the application. They allow executing traceable and irreversible transactions between network participants [6]. The transactional mechanics within Hyperledger Fabric occur in several steps (see Figure 3): First, the client, after logging in with an SDK (such as Node.js), initiates a transaction via the SDK API and sends it to a validator node. 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.

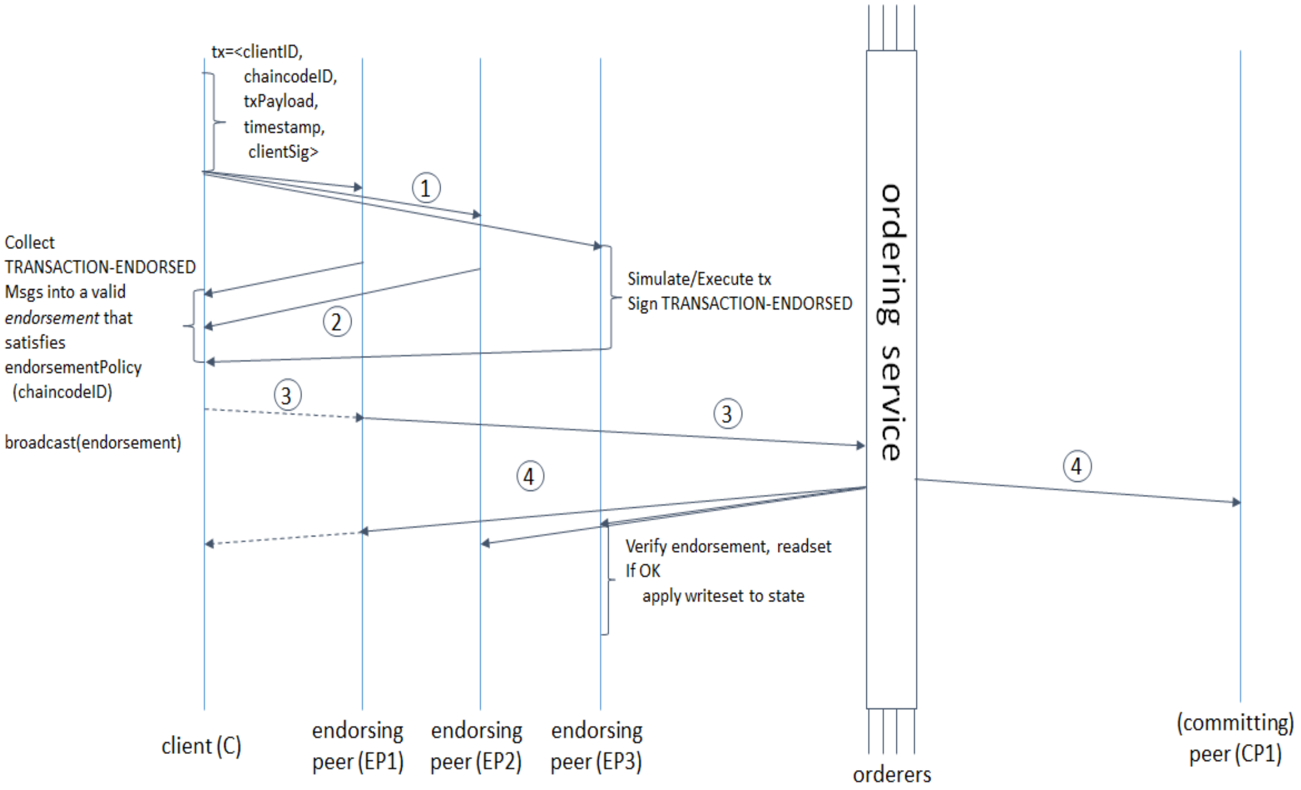


Fig. 3. Flow of a transaction [7]

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 offers 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 :

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

To ensure the authenticity of the message, the sender must include their signature S, established using their private key, so that only their 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, generating 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 verify the integrity of the blockchain efficiently.

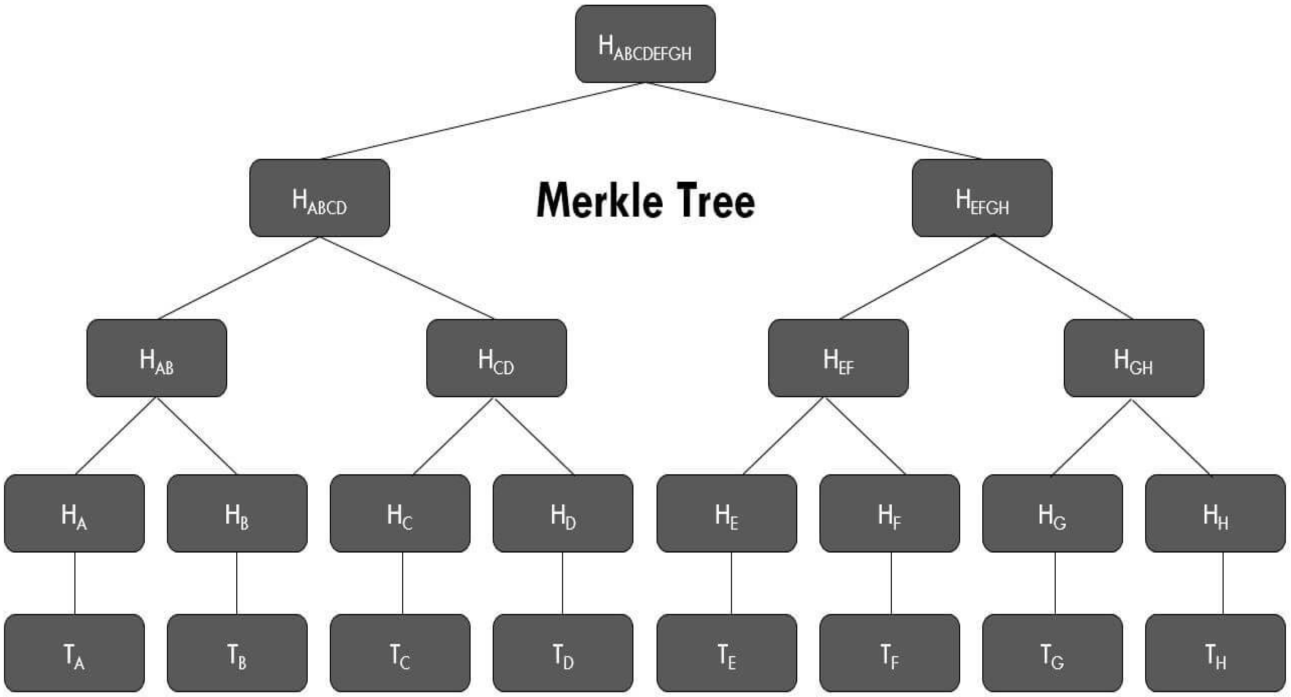


Fig. 4. Flow of a transaction [9]

B. Specific Characteristics

Hyperledger Fabric has the following advantages:

- an authorized network allowing the establishment of 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 several relevant criteria. To summarise, Hyperledger Fabric is a highly configurable blockchain that provides advanced privacy features and utilises a PBFT consensus method to ensure enhanced security. The platform also allows for the customisation of smart contracts and offers excellent scalability through its modular architecture.

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

Blockchain	Architecture	Langage	Network	Consensus	Smart contracts	Scalability	Privacy
Hyperledger Fabric	Modularised, allowing nodes to be added dynamically for greater scalability.	Go, Java, Javascript , Typescript	Permission is granted	PBFT (practical byzantine fault tolerance), which guarantees high security and low power consumption	Chaincode (Smart contracts)	Horizontal	Highly configurable, allowing participants to choose who can access specific 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 offers comprehensive security features, including the ability to encrypt data stored on the blockchain and safeguard user authentication and authorisation 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 limits access to sensitive medical information to only authorised 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]. In addition, private channels enable fine-grained control over access to medical information, allowing only authorised members to view specific details. 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 enables different medical data management systems to utilise distinct consensus algorithms while being connected to the same blockchain network. This flexibility enhances system interoperability and ensures compatibility between various 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] 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

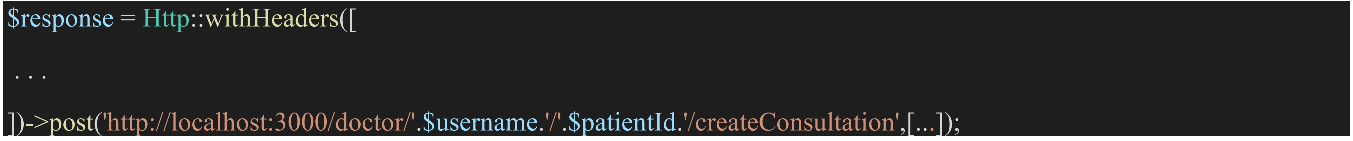
We propose a solution for securing medical records based on the Hyperledger Fabric blockchain following an architecture presented in Figure 9.

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 smart 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 request is made to save the document on IPFS, and the unique identifier of the document is then saved on the blockchain, ensuring that only the rightful owner can access it. The Identification and Authentication System by Fingerprints and Veins (SIAEDV) is designed to secure specific processes, notably the sharing of medical data by patients and the emergency access process for administrators.

B. Web Application (Laravel)

This is the layer closest to the user, comprising different graphical interfaces that enable each user (patient, doctor, pharmacist, or laboratory technician) to perform operations according to their role. We used the PHP framework Laravel, which is based on an MVC (Model-View-Controller) architecture. At the controller level, the operations of reading or saving data are indeed API calls to the NodeJS server, which handles communication with the blockchain network.



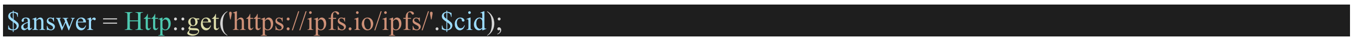
```
$response = Http::withHeaders([

 . . .

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

Fig. 5. Call to the Node JS API.

Additionally, we utilise a public IPFS gateway to store documents, such as analysis results, thereby preserving the speed of transactions within the blockchain.

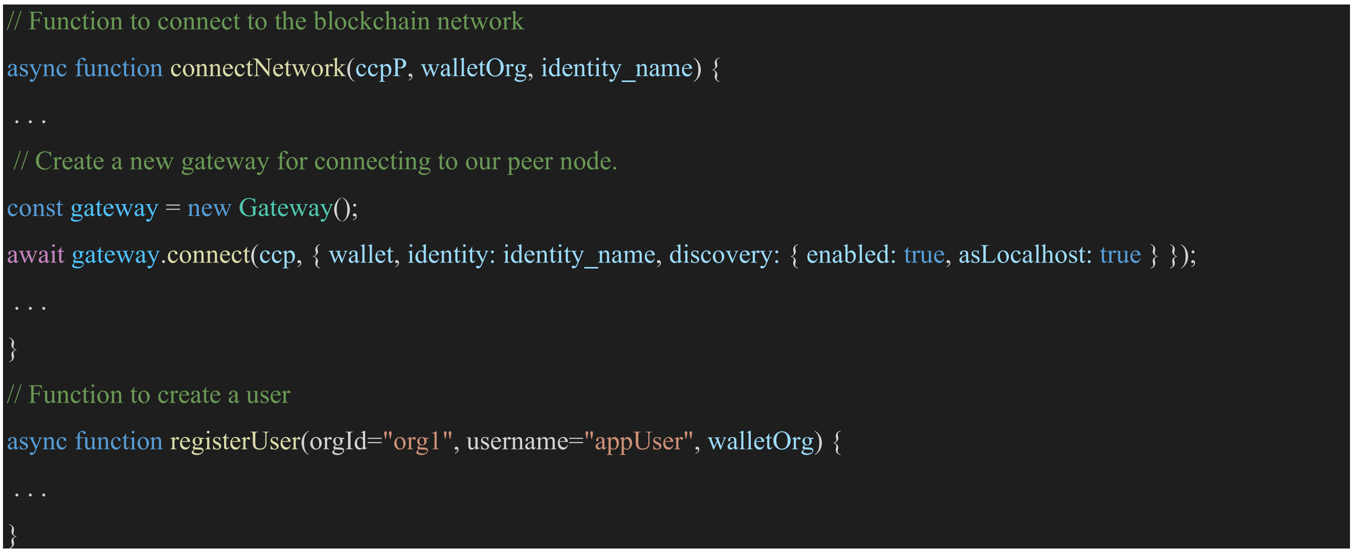


```
$answer = Http::get('https://ipfs.io/ipfs/'.$cid);
```

Fig. 6. Connection to the IPFS gateway.

C. Node.js Backend

We developed an API in Node.js, whose 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 network nodes and register users.



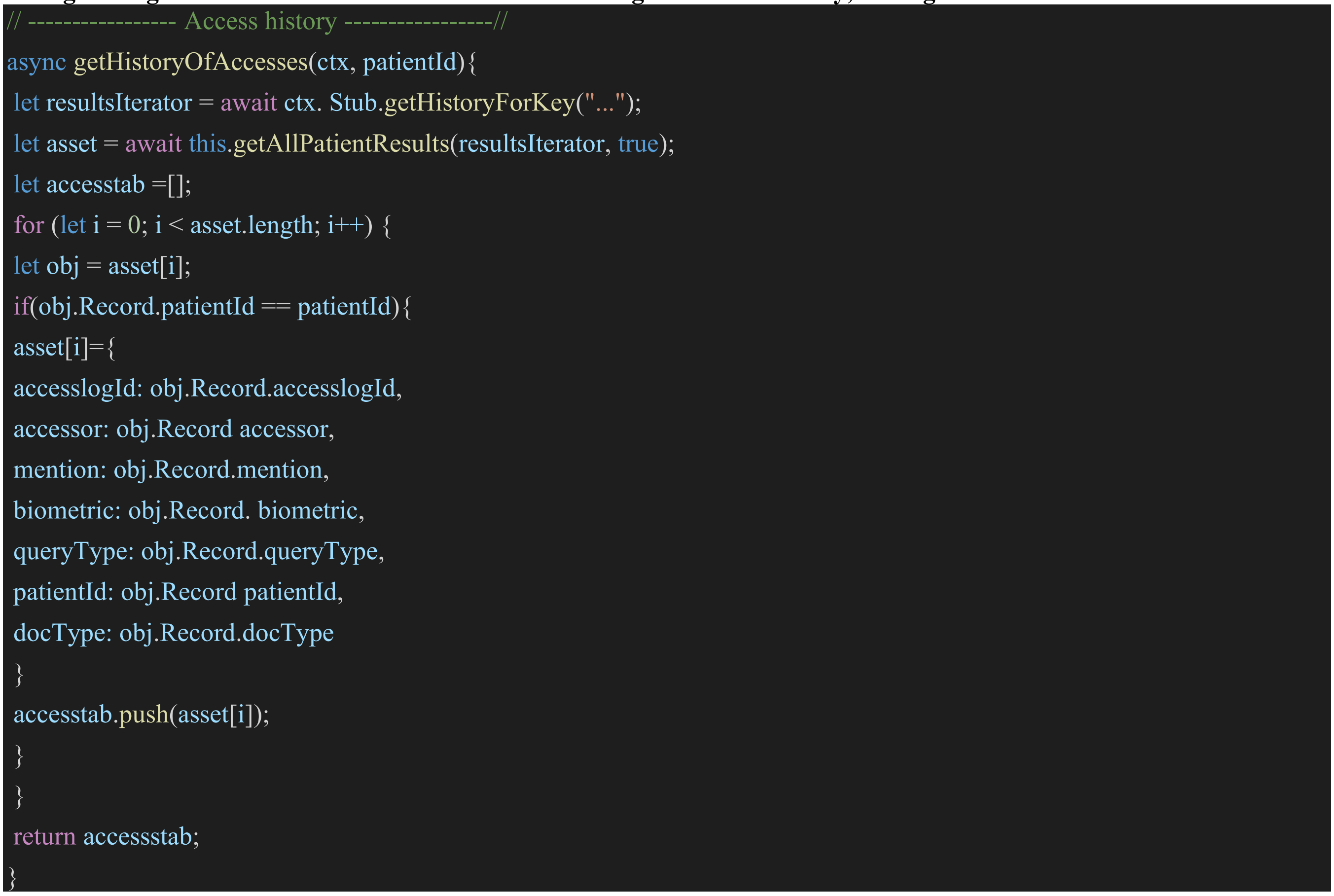
```
// Function to connect to the blockchain network
async function connectNetwork(ccpP, walletOrg, identity_name) {
 . . .
 // Create a new gateway for connecting to our peer node.
const gateway = new Gateway();
await gateway.connect(ccp, { wallet, identity: identity_name, discovery: { enabled: true, 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 comprising three organisations (Hospital, Pharmacy, Laboratory), each with 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, which contains the patient's authorised actions, including granting access to their medical data and consulting the access history, among others**.



```
// ---------------- 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 accessstab;
}
```

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, respectively, for 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. The hospital admin, especially in case of an emergency, can grant a doctor access to a medical record.

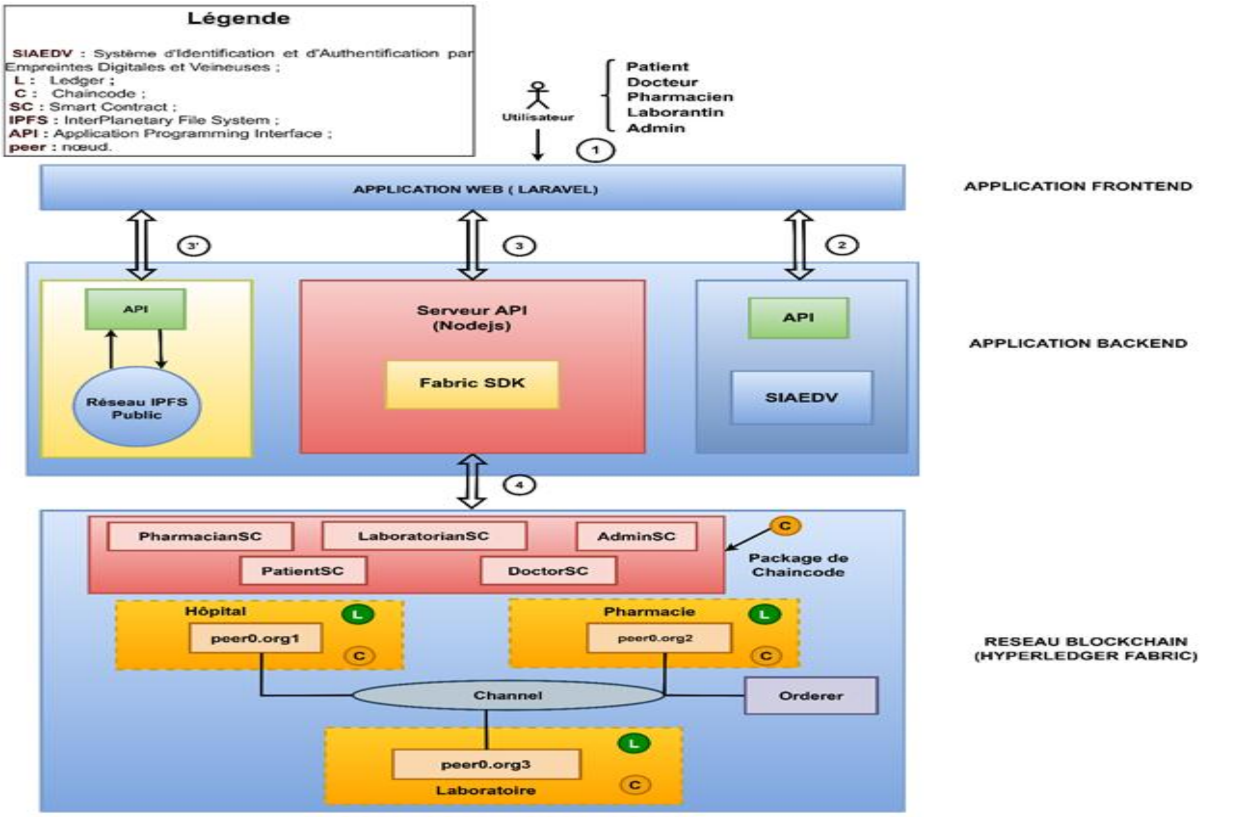


Fig. 9. Solution Architecture.

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 involves ensuring that the transaction is valid and that the order and results of a block's transactions meet 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 sufficient number of nodes to guarantee block integrity and service availability. Several algorithms exist, including Solo, Kafka, Raft, PBFT, Clique, Istanbul BFT, Simple BFT, and 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 consider 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 designed to enhance data access and authentication security. It can be used in emergencies to authorise a healthcare professional to access a record, to identify a patient coming to a new hospital, and to share data between the patient and healthcare professionals.

G. Results and Discussion

As a result, our research has enabled us to develop a prototype for deployment in a university environment during a pilot phase. Feedback will allow us to enhance data exchanges within 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 a perspective on this work, we would like to associate the Internet of Things (IoT) with the project. We intend to use a connected object (such as a bracelet) to retrieve the variations of the patient's vital signs in real-time, helping the doctor with his analysis.

VI. CONCLUSION

The proper management of medical records is a severe and vital issue. We have explored the possibilities offered by blockchain to secure it, ensuring the availability of information, its traceability, and interoperability between health professionals. We have opted for a consortium-type blockchain design using the Hyperledger Fabric framework, which offers the advantages of confidentiality and flexible 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 or consent to participate, as it presents evidence that is already publicly available.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal contributions to 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 primary 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

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, biometrics and software engineering. His areas of specialisation include multimodal biometrics, object detection, and distributed and decentralised architectures. In the field of artificial intelligence, he uses transfer learning methods applied to object detection for detecting the plasmodium stage of malaria.

Tahirou Djara is a Senior Lecturer at the Polytechnic School of Abomey-Calavi, located within the University of Abomey-Calavi, Benin. His research interests include biometrics, signal and image processing, computational intelligence, industrial applications and symbolic programming. He is a 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 a 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 field of software engineering, he is interested in object-oriented programming and relational databases for application development. In the field of artificial intelligence, he utilises machine learning methods applied to computer security (biometric authentication), e-agriculture, and 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.