End of Module Project

MEDICAL FILE WITH BLOCKCHAIN

Supervisor : *Pr. Ikram BENADBELOUAHAB*

Realized By :
BENJELLOUN Abdelmajid
DAGHMOUMI Marouan
AACHABI Mohammed

Computer Science Department
Faculty of Sciences and Technology, Tangier, Morocco

Abstract

Secure management of medical data is a major challenge for the health sector. Systems traditional are often vulnerable to hacking, human error and unauthorized access. Blockchain, with its decentralized and immutable nature, offers a reliable solution to overcome these challenges in ensuring the confidentiality, integrity and transparency of medical data.
In this project "Medical Record with Blockchain" we've created a decentralized application (DApp) which allows to manage and secure the medical records of patients through technology Blockchain. Smart contracts are developed in Solidity and deployed on the Ethereum blockchain. The application front-end has been developed in Python, offering a native graphical interface to interact with medical records in a secure and decentralized manner.
This project implements an innovative solution using the Ethereum blockchain for the management of medical records, ensuring their safety, traceability and confidentiality. The choice of Python allowed the development of a native and powerful user interface all by ensuring a smooth interaction with the blockchain. This meets the growing needs of decentralization, transparency, and security in the health sector.

Introduction

Medical data management is a major strategic and operational challenge in the health sector. These sensitive and critical data require solutions that guarantee their confidentiality, integrity, and accessibility. In traditional systems, several problems persist :

- **Vulnerability to cyber attacks :** Centralized databases are prime targets for hackers.
- **Human errors and inefficient management :** Manual data manipulation increases the risk of errors and loss of information.
- **Unauthorized access :** Permissions control is often complex to implement, resulting in breaches of confidentiality.
- **Lack of traceability :** It is difficult to ensure accurate and transparent tracking of changes made to medical records.

In the face of these challenges, blockchain is an innovative and powerful solution. With its decentralization, immutability, and transparency characteristics, this technology offers unique opportunities to rethink the management of medical data.
The objective of this project is to design a decentralized application (DApp) for managing medical records. This solution aims to ensure the security and confidentiality of patient information, propose a transparent and traceable system through the use of the Ethereum blockchain and offer a simple and intuitive platform, accessible to the different players in the medical sector he medical sector. Thanks to the integration of smart contracts developed in Solidity and the use of technologies such as IPFS for distributed storage, the project aims to overcome the limitations of traditional systems while meeting growing security and interoperability needs.

State of the Art

Traditionally, medical data management was based on electronic health record systems (EMRs). These systems, while improving access to patient information, have limitations :

- **Centralization :** Data is often stored in centralized databases, making it vulnerable to cyber attacks and system failures.
- **Security :** Data privacy is a major issue. Data leaks can have serious consequences for patients.
- **Interoperability :** The different EMR systems used by health facilities do not always communicate easily with each other, which complicates information exchange.

To overcome these limitations, new technologies are emerging, including blockchain.

Blockchain is a distributed and secure technology for storing and transmitting information. It is made up of blocks containing data, linked together in a cryptographic way. The main characteristics of blockchain are :

- **Decentralization :** Data is distributed over a network of many computers, making the system more resistant to failures and attacks.
- **Security :** Each block is protected by an encryption mechanism, which guarantees the integrity of the data.
- **Transparency :** All transactions are recorded on a permanent and transparent basis, which builds trust.
- **Immutability :** Once data is saved, it can no longer be modified retroactively.

Several existing projects illustrate the potential of blockchain in this field :

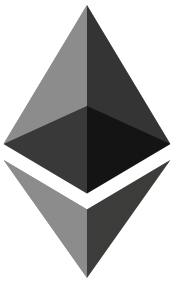
- **MedRec :** One of the first projects to explore blockchain use for electronic medical records.

- **Patientory :** A platform for patients to monitor their health data and share it with healthcare professionals.

- **Hashed Health :** A company that develops blockchain solutions for the management of health data.

Technologies Used

- **Blockchain Ethereum :** Ethereum runs on a decentralized network where transactions are recorded in blocks. This technology is used in the project to ensure the security and transparency of medical records, thus allowing reliable and immutable access to information.



- **Solidity :** Solidity is a programming language specially designed to write smart contracts on the Ethereum blockchain. These smart contracts automate and secure the management of medical records, ensuring that data cannot be falsified or altered.

- **IPFS :** The InterPlanetary File System (IPFS) is a distributed storage protocol that allows large files to be managed by distributing them over a network of nodes. This facilitates quick and secure access to medical data, while ensuring its integrity.

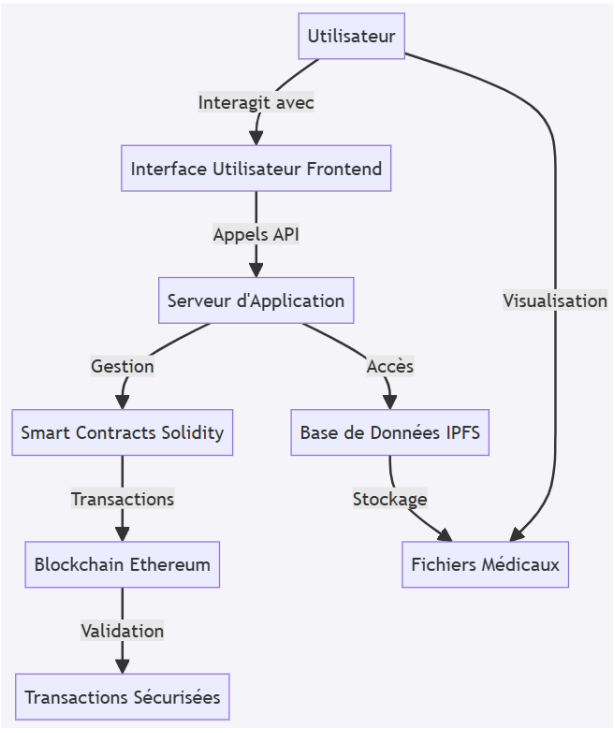
- **Front-end (Python) :** For the development of the user interface, Python is chosen because of its simplicity and power. This choice creates an intuitive interface that facilitates user interaction with the decentralized application (DApp) while effectively integrating underlying technologies.

System Architecture

Global Architecture Scheme

The system is based on a decentralized architecture that integrates three main components :

- **Front-end** pour l'interface utilisateur.
- **Back-end** pour la gestion des transactions et l'interaction avec la blockchain.
- **Blockchain** et stockage distribué pour la sécurité et l'immuabilité des données.



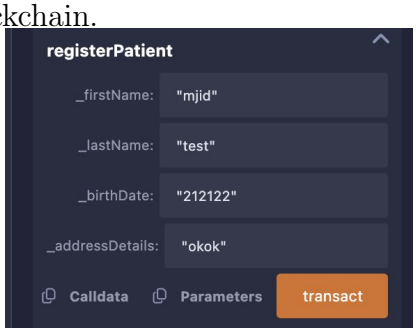
Smart Contracts

Smart contracts are the core of the decentralized system, ensuring secure and immutable management of medical data. They allow to define specific rules for each action, to automate processes and guarantee traceability. The different contracts deployed are as follows :

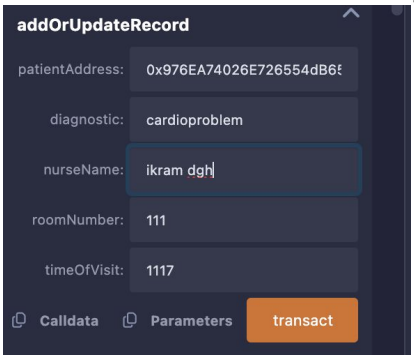
1. **ContractPatient**
   This contract manages personal information and medical records of patients.

   Features :

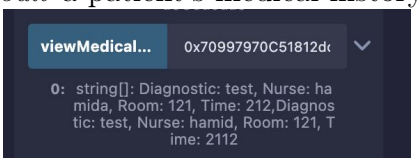
   - *Patient registration* : each patient is identified by a unique address on the blockchain.



   - *Update* or *add new* medical records as hashes to ensure their immutability.



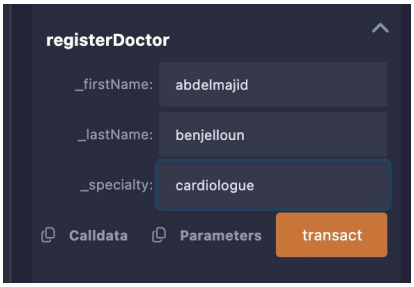
   - *Consult* a patient's medical history.



2. **ContractDoctor**
   This contract deals with the management of health professionals and access permissions.

   Features :

   - *Registration of doctors* with their information (name, surname, specialty).

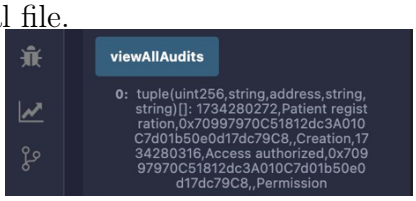


   - *Permissions management :* patients can grant or revoke access to their medical records for specific physicians.
   - *Access control :* a mechanism to verify whether a physician is allowed to view a patient's data before performing an operation.

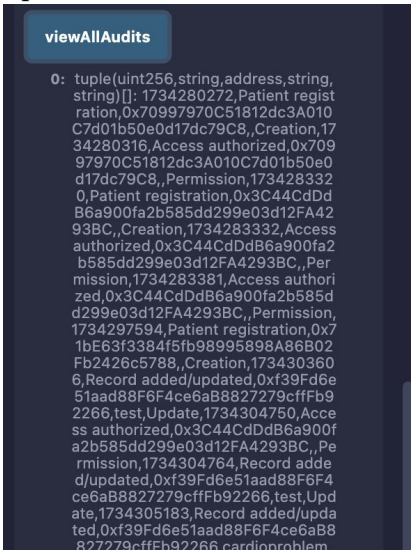
3. **ContractAudit**
   This contract guarantees the traceability and transparency of all actions carried out on medical records.

   Features :

   - *Audit record :* each action (creation, update, consultation) is recorded with a time stamp, the type of action, the user concerned and a hash of the medical file.



   - *Audit consultation :* it is possible to view all actions or filter audits related to a specific medical record.



4. **UserAuthentication**
   This contract ensures secure authentication of users (patients and doctors).

   Features :

   - *Secure registration :* users are registered with a password and an 8-character

unique key is generated.
- *Authentication :* allows users to log in by verifying their unique key associated with their address.
- *User information management :* facilitates access to data related to registered users.

Application Features

The decentralized application offers a number of innovative features that answer the rising needs of managing medical data, while leveraging the unique benefits of blockchain technology. These features help ensure the security, traceability, and confidentiality of medical records while simplifying the user experience.

1. **Patient registration**
   This system enables a patient to get a blockchain address that secures it and makes any hacking activities impossible. Upon signing up, a patient should state first and last name, birth date, and physical address. That kind of information gets registered on the blockchain decentralized way by the **ContractPatient**. This ensures that a patient cannot have a duplicate or erroneous record due to human errors at the time of registration. It also ensures a unique identity for every patient. Furthermore, adding and updating of patient-related medical data, such as patient health history, is possible only by authorized users, hence adding to privacy and security.
2. **Creation and updating of medical records**
   This application allows health professionals to generate and update the medical record of patients. A medical record created by a doctor will be changed into a unique and secure hash, which then gets stored in the blockchain. This approach guarantees records are not changed without permission while being easy to reach. Updates of the records are likewise immutable, traced on the chain, in such a way that an open, traceable history about the entire cycle of its transformation could be maintained. This feature increases patient trust in the system while reliably managing the patient's medical information.
3. **Medical record sharing and access**
   The system introduces an advanced permission management mechanism that allows patients to share their medical records with health professionals at their discretion. With the **ContractDoctor**, it is possible for patients to grant or revoke access to their information in real time. This is fully automated through smart contracts that record each change in permissions. When a physician wants to access a medical record, the system automatically checks his permission first before allowing him to consult. This feature ensures sensitive data is only accessible by authorized individuals while giving the patient full control over their information. Secure sharing also enhances collaboration between different actors in the medical sector, such as hospitals and clinics, therefore improving the quality of care.
4. **Audit and Action History**
   At the heart of the application is transparency and traceability of actions, thanks to **ContractAudit**. Every action on the medical record, whether creation, consultation, update, or deletion, is recorded in an unchangeable manner on the blockchain. For each event, the most important information is the user responsible, timestamp, and type of action. Audits can be accessed by either a patient or an administrator in order to verify the interaction history with their records. In this way, the feature of audits prevents abuse and facilitates the detection of suspicious activities, making the system robust and reliable. In addition, by providing transparency and access to audited processes, the application builds trust between patients and healthcare providers.
5. **Data encryption and decentralized authentication**
   The application will protect sensitive patient data using advanced encryption mechanisms. Medical information is encrypted and only authorized persons can decrypt it. This way, data breaches and unauthorized access are completely avoided. In parallel, the authentication of users is done via a decentralized system using **Ethereum** wallets-like **Me-**

taMask or private cryptographic keys. In the **ContractUserAuthentication**, every user has to create an **8-character** key at the time of registration, which is later used for authentication. It enhances the security of the system access, eliminates the traditional password usage dependency, and reduces the chances of hacking.

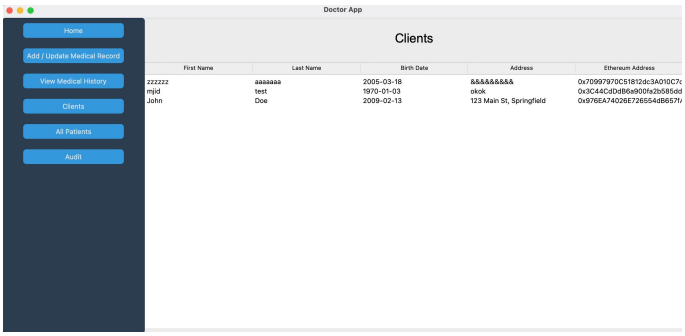
Project Progress

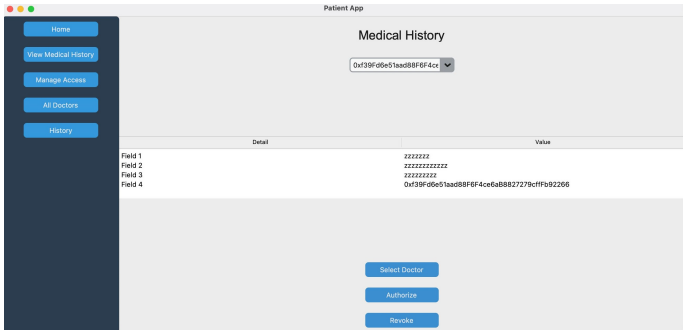
The development of the decentralized application for medical records management followed a structured methodology, divided into several essential stages. The main objective was to design a functional solution while implementing tools and technologies adapted to the project requirements. Here is a detailed overview of the different steps, highlighting the role of each team member and the technologies used.

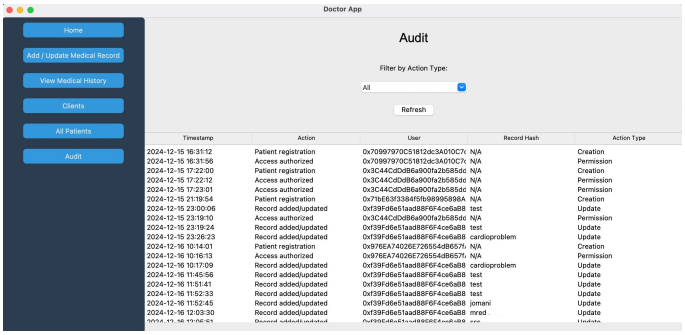
1. **Design and planning stages**
   The first phase of the project was to define a clear strategy and structure tasks to ensure smooth progress. Being a three-person team, we have divided the project into three main parts :
   (a) **Development of smart contracts :** A person took over the design and programming of smart contracts in Solidity. This included the development of functionalities to manage patients, physicians, audits, and user authentication. This step required a thorough understanding of the functional requirements and careful planning to ensure that each contract was interoperable.
   (b) **Desktop application development :** Two members focused on developing the user interface with Python, using frameworks such as PyQt or Tkinter. The goal was to design a user-friendly application that would allow end users to manage medical records in an intuitive and secure way.
   (c) **Writing and documenting :** The team also spent time on the project report. This task was shared fairly to document each step from technology choices to final results.
   We used Git and GitHub for collaboration and versioning. Each member had his own branch to work on, which made the integration of contributions and resolution of potential conflicts easier. Regular code reviews and weekly team meetings have helped to maintain alignment with objectives and ensure consistent quality in development.
2. **Development and testing**
   The development phase involved the practical implementation of planned functionalities. It took place in two sub-stages :
   (a) **Development of smart contracts :** Smart contracts were written in Solidity for the Ethereum blockchain. Tools like Remix IDE were used to facilitate contract writing, compilation, and debugging. Remix provided an interactive environment where each contract function was tested individually.
   To simulate a blockchain environment, we used Hardhat, a powerful tool that allowed us to set up an Ethereum LAN with test accounts. Thanks to Hardhat, we were able to run automatic tests to verify the proper functioning of smart contracts, including patient registration, permission management and traceability through the audit of actions.
   Once unit tests were completed, smart contracts were deployed on an Ethereum test network to validate their behavior in a near-real environment.
   (b) **Development of the desktop application :** The user interface was developed in parallel using Python and libraries like Tkinter. in this part we have worked to create an interface that would allow end users (patients and doctors) to interact with smart contracts in a transparent way.
   Manual testing was conducted on each application feature to ensure that it met the requirements and worked properly with smart contracts.
   The development and testing phase helped to create a reliable, secure, and user-friendly blockchain-based medical records system.

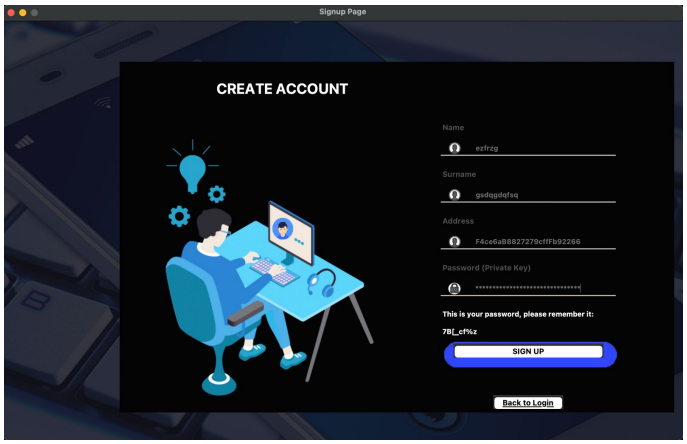
Thanks to clear role division and collaboration tools such as GitHub, we managed to develop a functional solution that meets the requirements of the project. Each step was an opportunity to learn, allowing us to deepen our skills in blockchain, application development, and project management. This project forms a very good foundation for future improvements and scaling into business environments.

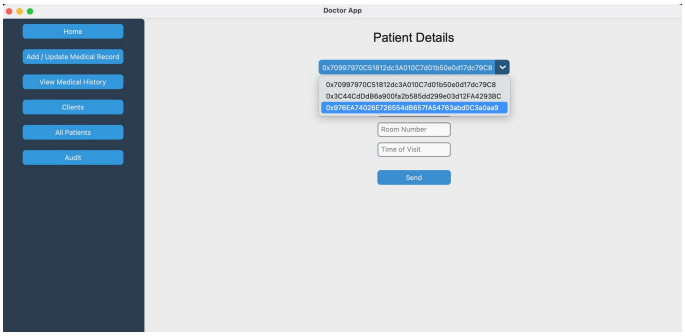
Results

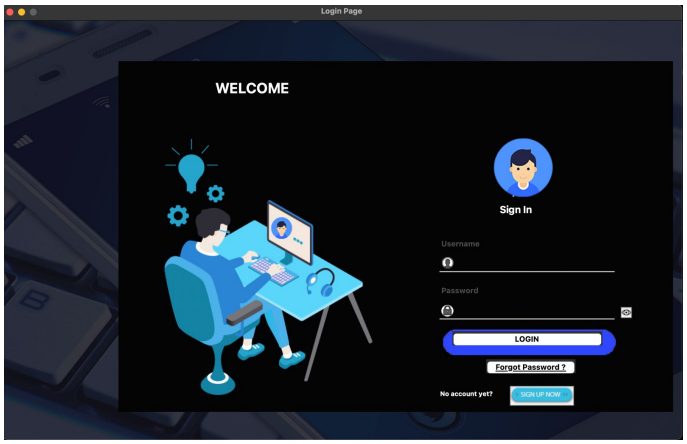


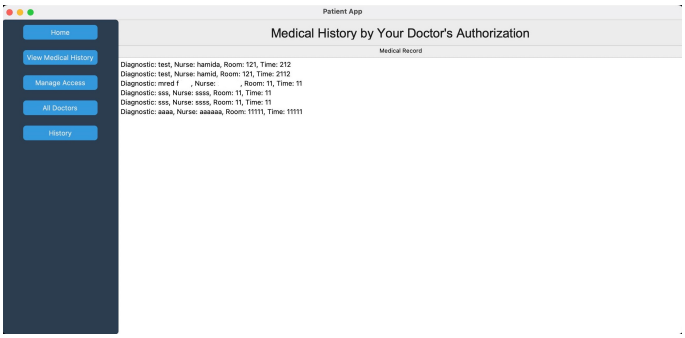












All those screenshots been taken from our application featuring the successful implementation with a demonstration

Conclusion

The project of a decentralized application for managing medical records is a huge step forward for blockchain technology applied in health, since it will respond to various limitations of traditional systems, including the deficiency in transparency, vulnerability to a hacking attack, and lack of user control, offering instead a modern and secure approach necessary for the sensitive growth demand. This we have enabled via an integration of the Ethereum blockchain with smart contracts written in Solidity, coupled with a front-end created in Python, thereby realizing an entire architecture that allows guarantees about medical data immutability, confidentiality, and traceability. Further, employing IPFS as distributed storage coupled with decentralized authentication mechanisms helps handle information more effectively and securely without loss of full ownership to the owner. Team collaboration was made easy with GitHub, and modern environments like Remix IDE and Hardhat helped to complete this project. Each member contributed in a vital way, be it in designing the contracts, developing the user interface, or documenting. It was such a collaborative effort that achieved not only what was targeted but also provided experience regarding project management and emerging technologies. This project is the expression of blockchain's potential to change the present systems by offering a solution that is decentralized, reliable, and transparent. This prototype application, though it sets a base for future works to be done such as integrating new modules or its adaptation for other sectors. This therefore means that this project highlights the meaning and the opportunity offered in innovation within the technological field on health.

Références

[1] Kuo, T. T., Ohno-Machado, L., & Huser, V. (2017). Blockchain in Health Care : A Systematic Review. *Journal of the American Medical Informatics Association, 24*(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068.

[2] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec : Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*, 25-30. https://doi.org/10.1109/OBD.2016.11.

[3] Silva, M. G. D., Almeida, A. S. M. de, & Lima, A. P. de (2020). A systematic review of blockchain applications in healthcare. *Journal of Biomedical Informatics, 103*, 103380. https://doi.org/10.1016/j.jbi.2020.103380.

[4] Kshetri, N. (2017). Can Blockchain Strengthen the Security of Electronic Health Records ? *International Journal of Information Management, 37*(6), 158-162. https://doi.org/10.1016/j.ijinfomgt.2017.07.004.

[5] B. K. S. K. R. B. S. K. R. B. S. K. R. B. K. R. B. (2020). Blockchain Technology in Healthcare : A Comprehensive Review and Directions for Future Research. *IEEE Access, 8*, 226373-226397. https://doi.org/10.1109/ACCESS.2020.3049674.

[6] Solidity Documentation. https://docs.soliditylang.org/.

[7] Blockchain.info. https://www.blockchain.com/.

[8] Metamask : A popular Ethereum wallet that can interact with DApps. https://metamask.io/.

[9] Remix : An online IDE for Solidity. https://remix.ethereum.org/.

[10] Tkinter : Python's standard GUI library. https://docs.python.org/3/library/tkinter.html.

[11] Web3.py : A Python library for interacting with Ethereum. https://web3py.readthedocs.io/en/stable/.

[12] Consensys. https://consensys.net/.