North American Academic Research | Volume 5 | Issue 3 | March 2022 | Monthly Journal by TWASP, USA | Impact Factor: 3.75 (2021)

North American Academic Research

Monthly peer reviewed Journal by **The World Association of Scientists & Professionals**
TWASP, United States

RESEARCH ARTICLE

A Blockchain-based Lightweight Access Control Solution in the Healthcare Sector for Developing countries: A case from Conakry

Bah Raguiata[1*], **Jihui Shi**[2], **Barry Dialikhatou**[1]

1 School of Information Engineering, Huzhou University, Huzhou, China
2 School of Economics and Management, Huzhou University, Huzhou, China

OPEN ACCESS

Accepted March 18, 2022

Published March 19, 2022

***Corresponding Author:** Bah Raguiata

Funding: Self

How to cite this article: Bah Raguiata, Jihui Shi, Barry Dialikhatou (2022). A Blockchain-based Lightweight Access Control Solution in the Healthcare Sector for Developing countries: A case from Conakry. *North American Academic Research, 5(3) 402-418*, doi: *https://doi.org/10.5281/zenodo.7030387*

ABSTRACT

Medical data protection has always been a primary concern in the healthcare sector. As information technologies improve over the years, medical records management approaches are shifting to prominent and fully automated systems. The common issues in medical service provision within most developing countries are primarily associated with data availability among healthcare providers, doctors' referral process, privacy protection, and portals for patients to conveniently access their medical information history. Practical implications arise from these issues, such as patients' improper identification that may lead to records inconsistency across healthcare providers with weak security systems. To address these issues, Blockchain-based electronic medical records (EMRs) systems show particular benefits, providing a secured healthcare environment where involved stakeholders can collaborate. In this paper, we adopted a fit-for-purpose approach to propose a Hyperledger Fabric-based design for electronic medical records management, adaptable in developing countries using Conakry as a case study. Our approach focuses on the hypotheses of privacy protection and data accessibility among involved stakeholders. This approach presents a decentralized, immutable medical environment, where patients have easy access to their medical information across different healthcare providers in Conakry. Finally, we conducted a qualitative evaluation to illustrate the portability and efficiency of the solution.

Our design is presented to contribute to EMRs solutions adaptable in developing countries for future in-depth analysis.

Keywords

Blockchain-based EMRs, privacy protection, Hyperledger Fabric, chain-code.

1. INTRODUCTION

The accessibility to relevant and accurate medical records is essential for each individual's well-being as they contain critical information that can question one's survival. These records are crucial health information that healthcare providers use for the diagnosis and treatment of patients. Therefore, due to their sensitive contents, they require management within a closed and highly secure environment.

Recent technological advancements have significantly contributed to the healthcare sector, where health practices are multiplying and diversifying. Records management strategies are moving towards fully electronic and automatized systems for improved healthcare services while maintaining patient information in a way that can be easily accessed and shared adequately between healthcare providers.

In the last decade, Blockchain has been proved to be a technology that, when adopted, helps bring security without third parties[1]. Satoshi Nakamoto, a pseudonym, first coined the term Blockchain in 2008[2] to name a distributed ledger technology (DLT) that stores data in a series of individual data clusters called blocks. Blockchain has been revealed promising for various industries where decentralization, immutability, network robustness, and automated tasks among multiple stakeholders are required[3]. The technology is highly secured where data is saved in blocks, linked together using cryptographic signatures, and stored in a shared ledger whose state is constantly kept in sync by dependable consensus algorithms. the highlighted technology can guarantee medical records integrity, ensure security, enable records ownership, facilitate records accessibility, and improve network resilience[4].

Research scope

In recent years, various approaches have been applied worldwide to adopt Blockchain technology to address medical data protection, storage, and sharing, thus data management. In the context of developing countries, more precisely in sub-Saharan African countries, Blockchain technology is increasingly being adopted in finance [5], e-government [6], agriculture [7], energy [8], and other fields. However, relatively little progress is noticed in the healthcare sector. Consequently, our research focus is to design a Blockchain-based EMRs solution to the existing pain points and challenges the healthcare systems face in developing countries' environments, using Conakry as a case study. This study can present a basis for a more in-depth analysis of these countries' medical sectors and other areas of study.

Motivation

Despite the tremendous technological advancements, paper-based medical records are still utilized in many developing countries' healthcare institutions as a primary tool to maintain a long history of medical records. These types of systems present several hurdles. In Conakry, the healthcare sector faces common issues such as accessibility, availability, integrity, affordability, sustainability[9]. Since a single patient's medical data may be spread across multiple healthcare providers, this situation results in siloed databases that are currently ineffective for healthcare applications outside of those silos. The fragmented structure prevents an individual's medical records from tracking that could assist healthcare providers in making accurate diagnostics. Besides, the issue of data access control is prevalent, and the inefficiency in sharing patients' medical records can result in lengthy healthcare process workflow and increased treatment costs by repeating medical tests. A Blockchain-based EMRs system is an excellent choice to address these issues for better healthcare service delivery. In addition to being a distributed ledger technology, Blockchain preserves data in a tamper-evident way as the records transactions are linked and updated by consensus.

Our contribution

In this paper, we proposed a Blockchain-based design to mainly address the fragmented structure of EMRs' in Conakry and strengthen records access control. The main contribution of our study includes:

- A decentralized patient-centric system design, enabled with chain codes to secure EMRs while ensuring their integrity among healthcare stakeholders.
- A design process for a lightweight access control scheme based on Hyperledger Fabric Framework that fits the context of Conakry.
- A thorough discussion of the essential design components relevant in our study context.
- An illustration of the approach's essential features and functional hypotheses.

We organized our paper as follows: In section II, we briefly discuss the related works and the current health situation in Conakry. We present the key concepts of Blockchain technology relevant to our study and some preliminaries in section III. Section IV discusses the study approach, whereas section V presents our proposed design, further we conduct a qualitative analysis of the solution at the end of the section. Finally, we summarize the paper in Section VI and provide recommendations for future studies.

2. LITERATURE REVIEW

This section provides general information applicable to the objective of our study. First, we discuss several studies proposed in recent years that adopted Blockchain technology to address data security, integrity, and accessibility in the healthcare sector. Then we present the current healthcare situation in Conakry.

2.1 Related works

A systematic review shows that Blockchain-based healthcare records designs were proposed early in 2016 by [10] named Medrec. The approach is a Blockchain implementation for medical record management based on the Ethereum platform that uses Smart Contract, key cryptography to handle identity confirmation, and PoW algorithm as a consensus mechanism. Similar works were proposed by [11-13] based on the same platform as permissioned-based solutions for electronic health records access control and interoperability. The most common adopted components in these approaches are smart contracts, public-key cryptography for identification in a public Blockchain framework, yet permissioned-based environments.

Another commonly adopted framework is Hyperledger fabric (HF). Authors in [14] presented a Blockchain-based solution using HF combined with FTPS (file transfer tools) to record only emergency medical data as patients pass from one medical facility to another, resulting in a data source. The ledger is used only for emergency medical data management in their approach. A similar approach is presented in [15] named MedBlock, a Blockchain-based information management system for handling patients' information using asymmetric cryptography and a hybrid consensus mechanism based on byzantine fault tolerance and a delegated proof of stake (DPos). However, the presented approach requires computational power, making it an expensive solution. Likewise, Medchain proposed by [16] also adopted HF based approach for secure

medical records access and privacy-preserving. The consensus mechanism is proof-based, which requires considerable running power. [16] Opted for a consortium Blockchain to compose a distributed system using the HFF to make patient records accessible in a distributed fashion. Besides, chain codes are part of the design to handle nodes' business logic agreements.

A set of works presented medical data management design based on Blockchain combined with cloud storage. Authors in [17] proposed a design based on a timestamp mechanism to ensure the timing link of blocks and a hash function to protect data from being altered. They considered data storage and access control to be the main transaction processes where the ledger records only information indexes and medical data stored under the chain in cloud storage. Similarly, [18] engineered a system data sharing. The proposed system considered patient privacy protection based on permissioned Blockchain and cloud storage for actual records storage.

The combination of cloud storage and Blockchain allows robustness of the system but high implementation costs. Additionally, public Blockchain such as the Ethereum platform involves enormous operating power with complex architecture. This set of solutions can lead to high latencies in request processing that is unfavorable for medical data often queried and unpractical in developing countries where access to the internet might be challenging. The last set of approaches is the adoption of HLF for EMRs since complete data disclosure between all participants is not appropriate in the healthcare context. Fabric architecture provides small ledgers shared between stakeholders with greater control over data privacy.

A dependable design option common to discussed studies is the adoption of on-chain and off-chain approaches [19] due to medical records' large volume for efficiency reasons and to avoid redundancy. Further smart contracts, also called chain codes, are utilized to handle business logic agreement and records mapping, representing a potential solution to achieve access control and allow automated transactions. Besides, the asymmetric cryptography mechanism is adopted to handle data security, nodes identification, and data integrity[20]. Moreover, Patients can meet their confidentiality and privacy needs using appropriate Consensus algorithms to verify and distribute Blockchain operations with relevant permissions [21, 22].

2.2 Healthcare Situation in Conakry

The healthcare system in Conakry is structured around three levels. The structure is made of health post and health centers (HP, HC), communal medical centers (CMCs), and university hospital centers (CHUs) [23]. The latter are the ultimate benchmark in the hierarchy of healthcare service provision in the city. The system is divided into two sub-sectors: the public and private sectors. In Conakry, the public healthcare supply is not sufficient to guarantee access to healthcare for a constantly expanding population; consequently, alongside national hospitals, there are many dispensaries and private clinics that the population turns to for healthcare. The majority of healthcare facilities have installed the district health information software II (DHIS2) under a program of the Ministry of Health implemented freely in different levels of health facilities[24]. A large number of facilities develop and manage their systems. The choice of a hospital or clinic varies depending on

patients' socioeconomic status. Often, it is the financial means, including the wealthiest patients that refer to private clinics. At the same time, for other populations, it is social and community services that are decisive [25]. When a patient needs to be referred, he is sent with a referral bulletin to a referral healthcare provider, either CHUs or private specialized clinics. The new healthcare provider conducts their medical tests and stores patient records in their EMRs system. It results in a fragmented structure of patient records stored in those different systems. Furthermore, the system faces pain points regarding confidentiality and privacy protection: patients' EMRs are not correctly encrypted. It takes little to link a patient's identity to his medical file, even for non-medical staff. Moreover, the system does not fully assure the sustainability of medical records where often, it is the patient who summarizes their medical history verbally, leading healthcare providers to predict inaccurate diagnoses. At the same time, the integrity of records held by patients is called into question because the current medical system lacks a mechanism for verifying medical records' integrity. Figure1 describes the current health management system in Conakry.

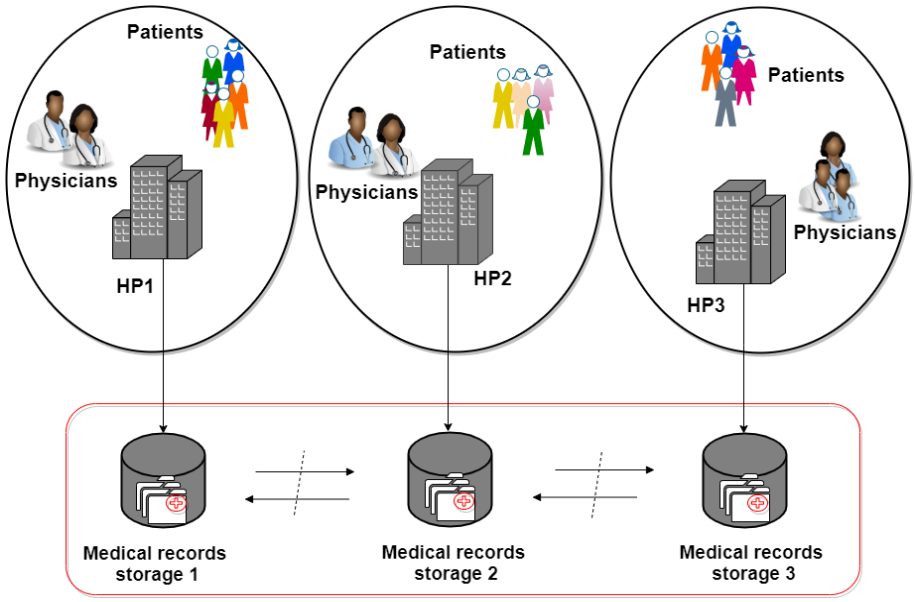

Figure1 Current medical records management in Guinea

3. CONCEPTUAL PRELIMINARIES

3.1 Blockchain components

Blockchain is built on a modular architecture [26], including digital identification modules, data structure modules, smart contracts execution modules, and network consensus modules.

Digital signature embodies methods that issue necessary credentials for user identification and transactions authentication[27]. Transactions and participants' identities are approved based on asymmetric encryption[28]. Blockchain's particularity resides in the data structure. Data is contained in an ordered list of blocks, where each block contains a small (possibly empty) list of transactions. Each block in the network is chained back to the previous block by having a hash representation of the previous block making the chain tamper-evident. As a data storage facility, information in a Blockchain is recorded within the transactions, contained in

blocks[4]. The potential of the technology is introduced by smart contracts that make the construction of decentralized and self-executing programs possible. Technically, a smart contract is a software code that comprises a set of self-executed rules and regulations that run on Blockchain networks [29]. When deployed on a Blockchain platform, smart contracts significantly simplify exchanges by allowing automatic actions to eliminate intermediaries and enable effective communication and transparency.

The existence of Blockchain platforms is contingent upon Consensus protocols. It defines mechanisms deployed on the network for blocks validation, ordering blocks, and ensuring that most network nodes agree on the state [30]. A consensus algorithm backs practically every Blockchain network [31] which manages the order of transactions. Based on their operation modes, there are two primary types of Blockchain. Permission-less (Public Blockchain) [32] and permission (private Blockchain) [22]. Other types of Blockchain combine features of the two main types [33]. Accordingly, diverse Blockchain frameworks are available[3], each with distinct application fields and visions [31]. Though not all types of Blockchain frameworks are suitable for all study contexts; therefore, an in-depth analysis of trade-offs is essential to understand which type best fits the use case.

3.2 Blockchain components

Practically, storing non-transaction data in the actual Blockchain ledger is not feasible. Some forms of off-chain or side database storage are required. The blockchain is physically implemented in a file[34], which improves transaction processing performance by avoiding traversing the entire transaction log.

Ideally, the off-chain is self-contained processing storage capable of tiering non-critical data and providing optimal speed for critical data like medical records. It would hold actual records on the network, and only index information obtained by hash or signature of the actual off-chain data should be on the blockchain (on-chain). Off-chain storage refers to any data storage that resides external to on-chain data. Traditional data storage technologies, decentralized data storage platforms such as IPFS are aligned with the blockchain for increased system robustness and security.

- **CouchDB**

CouchDB is a JSON format data storage that allows information mapping of the database documents [35]. It supports rich queries and indexing for more efficient queries over large datasets[36]. A CouchDB is different from a relational database management system; rather than rows and columns, the database stores data in a collection of JSON documents. Hence, the data must be modeled in JSON format to perform content-based JSON queries in CouchDB. It supports various query methods, including get, put, and delete in conjunction with a state key. CouchDB is compatible with blockchain networks settings as an off-chain storage, and ensures data protection.

- **IPFS**

Interplanetary File System (IPFS) is a content-based addressing technology that introduces dynamic storage locations. It offers a distributed peer-to-peer storage structure to keep and access massive encrypted volumes of data when required. Additionally, data stored in the IPFS is encrypted using a unique cryptographic public key encryption algorithm to create network robustness. Every file on IPFS has a unique hash via which it can be retrieved[37].

The key feature of the off-chain approach is its ability to improve scalability to maintain an immutable and auditable environment. The approach resolves critical issues such as cost efficiency, reducing data storage requirements on the blockchain while enhancing data privacy and network robustness.

4. FIT FOR PURPOSE

This section presents the approach we adopted to achieve our study objective. First, we conducted a qualitative research analysis based on desk research and observation to depict the current healthcare management system in Conakry. Besides, we employed the keywords "Blockchain-based EMRs," "chain codes," "data sharing" to do full-text searches in available repositories. Consequently, we reviewed relevant literature proposed in recent years on Blockchain-based EMRs to understand the involved techniques thoroughly. Then, we adopted the "Fit for Purpose" (FIP) design approach presented in [38], which has specific design principles to propose a Blockchain-based solution to the existing issues: namely, a) Blockchain Framework selection, b) network nodes identification, c) Authorizations structure.

4.1 Hyperledger Fabric Framework

EMRs require special protection as the context in which the data is processed may entail severe risks to fundamental rights. Hence a tightly controlled and confidential framework is most appropriate for our study context. The public does not openly access participants' identities, and only involved entities and authorized third parties should participate as network nodes. Therefore, the private Blockchain HFF [39] best fits our study case.

Hyperledger Fabric is a permission-based platform anchored by a modular design. The framework provides high levels of confidentiality and flexibility. It supports several layers of permission, enabling a data owner to determine which portions of their data can be accessed by whom [40]. Fabric consists of several primary components that serve a particular role. Many of the parameters are correlated for security, efficiency, and network stability [41]. The framework is flexible, scalable, secure, and membership services are pluggable. Fabric uses Low-cost consensus mechanisms as there is no crypto mining, and POW algorithm, thus faster transactions processing. It sustains the sufficient level of privacy required in our approach.

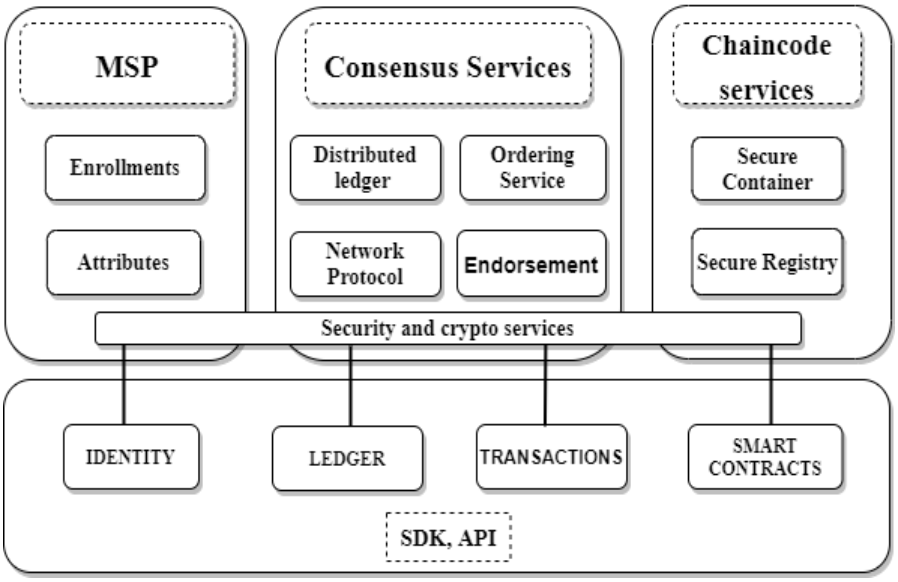

Figure2 Hyperledger Fabric architecture [42]

4.2 Network nodes identification

In the case of Conakry, four entities are mostly involved in the healthcare process. The network comprises participants from various entities, each having distinct roles and predefined access permissions.

- **Admin:** Enrolment authority (medical and health management regulatory). He is the regulating body in charge of coordinating the adequate policy for determining which participants should be admitted as network members.
- **Healthcare Provider:** Any Certified and authorized healthcare provider can exclusively perform EMRs adding and updating medical records for patients. Practically, this entity concerns a healthcare provider who has a patient new record to update on his EMR history.
- **Patient:** Primary records owner and he should be able to control the access permissions to his medical records history.
- **Data requester:** He represents an authorized party such as a medical insurance company. He might obtain view only permission for relevant records if his attributes meet the corresponding access policy.

As long as these entities participate in the network, the Blockchain log maintains the data history and provenance.

4.3 Authorization structure

To design the network business logic, the authorization structure on the network must be established for each involved stakeholder, as shown in the table below. Based on their personal information, each stakeholder has a predefined role and permissions that have been determined in the study context.

Table 1 Blockchain-based EMRs authorization structure.

Stakeholder	Requirement	Role& permissions
Admin (Enrolment authority)	Login	• He restricts identity registration to only certified participants (healthcare providers, requesters). • He assigns or deletes participants' identities on the network.
Patient (Data owner)	Registration & Login	• Grant permission to healthcare providers or requesters to read or write EMRs. • Revoke read or write permission access from healthcare providers or data requesters. • Read EMRs history, edit profile, and verify which records he acknowledges. • Permit emergency contact to read or grand permission.
Healthcare Provider		• Read or write permission on EMRs. • Register patients • Request permission from patients to read or write EMRs. • Read, create, and update patients' records.
Data requester		• Request access permission from patients to read specific EMRs. • Read permissioned EMRs.

4.4 Network communication structure

For feasibility reasons, we adopted CouchDB for our off-chain storage (document store database).

Traditional storage facilities present environments that require additional efforts and configurations to comply with the Blockchain network. In the contrast, distributed storage facilities like IPFS are not practical for healthcare in Conakry because it may require huge additional computation costs.

CouchDB provides rich query support when the chain code data is represented as JavaScript Object Notation (JSON) to perform content-based JSON queries. On HLF, LevelDB stores chain-code data as key-value pairs that maintain the network logic structure[36].

Technically, the peer-to-peer communication method over the network is supported through channels. A channel between two healthcare providers allows isolated communications from other providers on the network. Each peer (peers exist under each healthcare provider) joining the channel is assigned its own identity by Fabric MSP (Membership Service Provider), which also authenticates its channel and services. The channel-based isolation of peers enables network members to coexist with other restricted members on the same Blockchain network. In other words, a channel is comparable to a separate private Blockchain where data exchange flows. Such a configuration primarily provides security and privacy while having various members on the network.

Practically, the Hyperledger Fabric network can be set between two organizations on a local machine, each with two peer nodes using Docker containers. However, it would be in separate IP networks or protected cloud environments in the real world. The configuration can be extended to multiple peer nodes and organizations in different machines. Figure3 depicts the described network communication structure.

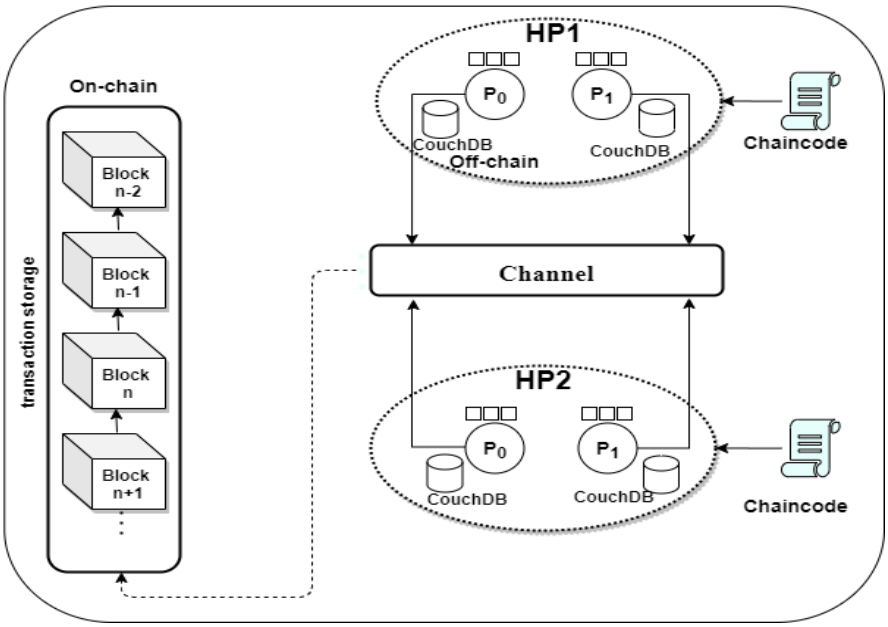

Figure 3 Network communication structure

5. PROPOSED DESIGN FOR CONAKRY

5.1 Network diagram

This section outlines our proposed approach. Our design is based on the Hyperledger Fabric framework, which is enabled with chain code to store interoperable EMRs safely. The solution is composed of 2 parts: the CouchDB facility holds actual medical records, and only index information and metadata should be on-chain (also referred to as the blockchain part).

The blockchain part immutably stores the transaction information on the network along with medical records' hashes. Therefore, it serves as a set of access links to actual medical records. The actual EMRs are encrypted and stored in the CouchDB. Fabric MSP provides the network participants' identities, and identity authentication is handled via digital signature techniques, namely asymmetric encryption using standard PKI (public key infrastructure). A signing algorithm generates a one-way hash of each data on the ledger to be signed, ensuring data integrity and identity authentication. Moreover, the network business logic and the medical records access control strategy are contained in the chain code and deployed to all network peers. The Chain code is responsible for records mapping and authorizing access to actual EMRs.

The Computation between on-chain and off-chain incorporates cryptographic and consensus algorithms that maintain unified management.

This approach requires lesser computational cost, strengthens access security to medical records regardless of their location, eliminates the fragmented structure of EMRs, and minimizes practical constraints such as cost-effectiveness, storage capacity, and bandwidth issues. Figure4 presents a pictorial illustration of the proposed network.

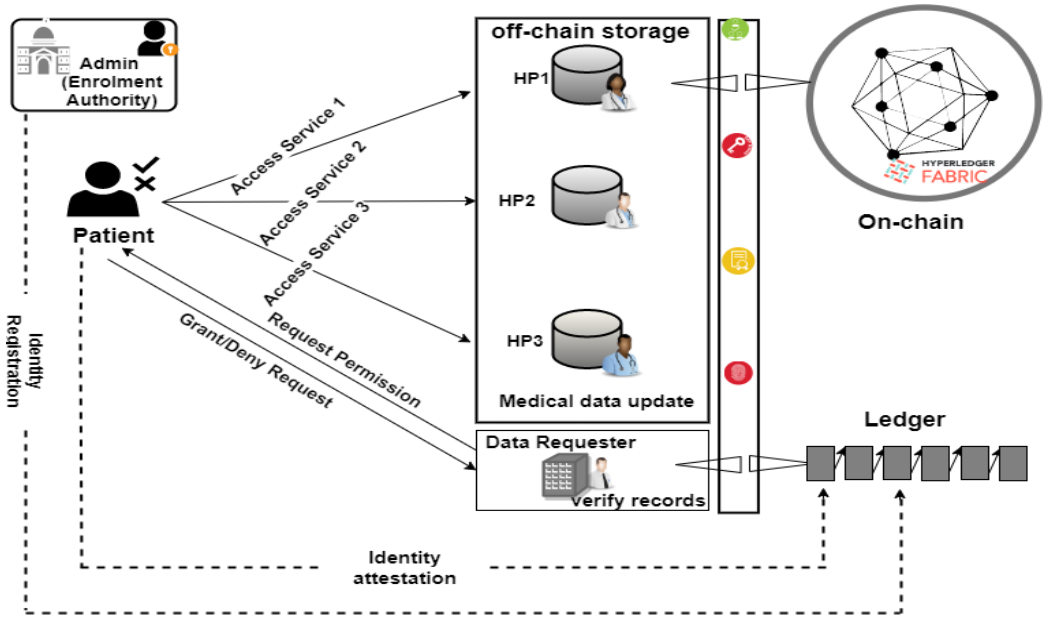

Figure 4 Proposed network diagram

Functional hypotheses:

- The enrolment authority (regulatory & admin) register stakeholders and assign IDs.
- Healthcare providers add patients and collect medical data from patients.
- The data is then hashed and stored off-chain (in CouchDB).
- A hash is generated from each data source and forwarded to the blockchain.
- Patients decide who access their EMRs.
- Authorized Data requesters can query the Blockchain network to read medical details under the data owner's permission.

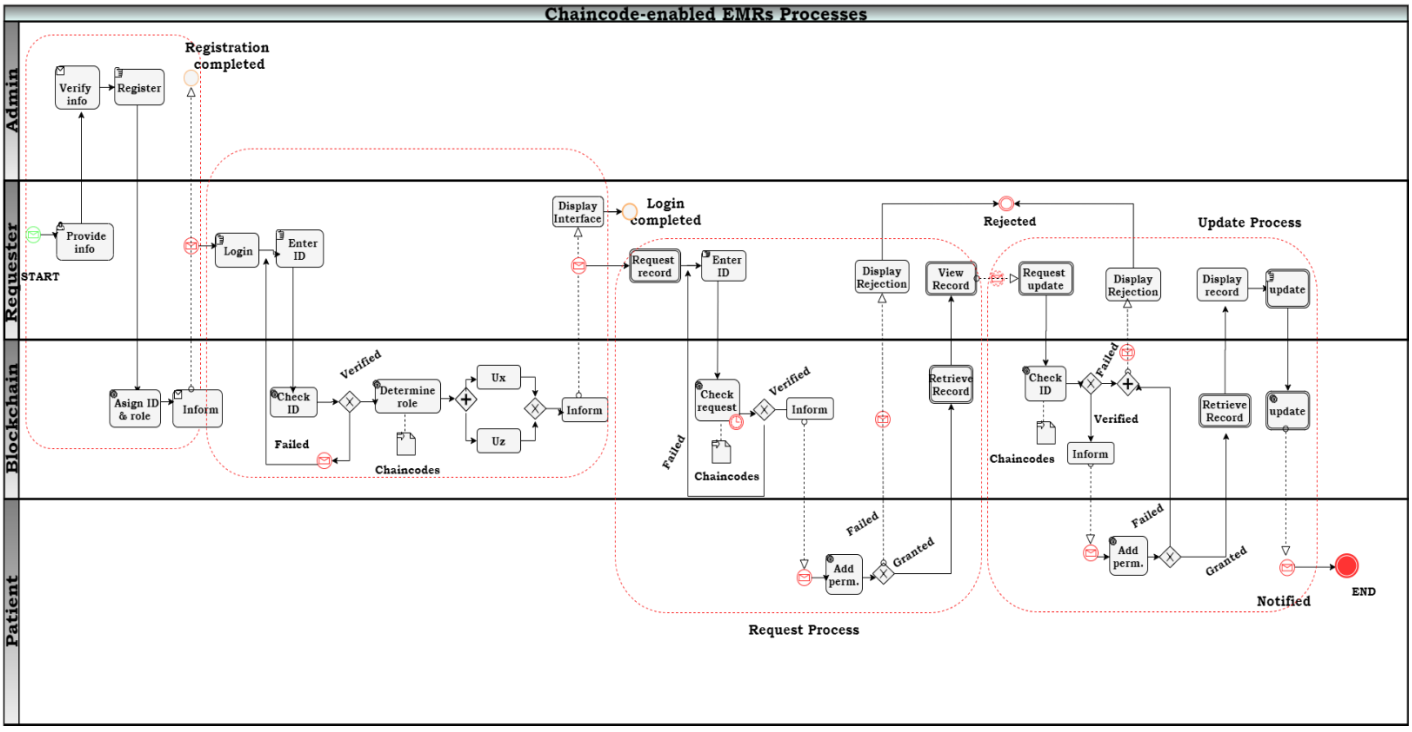

Figure 5 System functional processes

5.2 Architecture of the proposed system

We structured the architecture in three main phases, which are described in the following lines.

- **Phase1: Stakeholders identification**

In this phase, participants, namely healthcare providers and healthcare insurers, request registration on the network from the admin. Except for the patient whose account is initially created by the healthcare provider. The Enrolment authority generates a digital certificate for each participant based on his information such as name or email, then a simple initial data is created as a block corresponding to his ID in HF. Unique IDs are assigned through the client application or SDK by the MSP with the CA (certificate Authority) which is responsible for issuing the certificate with public/private keys to users.

- **Phase 2: EMRs storage**

The second phase of the architecture focuses on the EMRs storage structure. The healthcare provider generates patients' records placed in the blockchain by invoking chain code functions. To ensure the design scalability, the actual records are stored in the CouchDB which offers rich query support when the chain code data is modeled as JSON to perform content-based queries. CouchDB represents the world state database (records storage database) in the proposed design. It stores data in the JSON file format rather than as a key-value pair. Querying data in the CouchDB returns the actual medical records contents.

- **Phase 3: Authorization structure.**

The third and final phase of the proposed architecture is the authorization structure. This phase describes the access mechanism to medical records. A patient (records owner) may be able to control who has access to his or her EMRs. He may as well revoke access permission to certain network members. Furthermore, a healthcare insurer can check the validity and integrity of records claimed by the patient.

When a data requester (including a healthcare provider) requires access to a patient's medical history, he initiates a search on the network. Then, the chain code determines whether he is an authorized user; if so, request access permission from the patient then return the corresponding seek result; otherwise, the operation is rejected. The transaction is completed if the user has the permission to make the request, or if his credentials match the predefined chain code. If this is not the case, the request is denied.

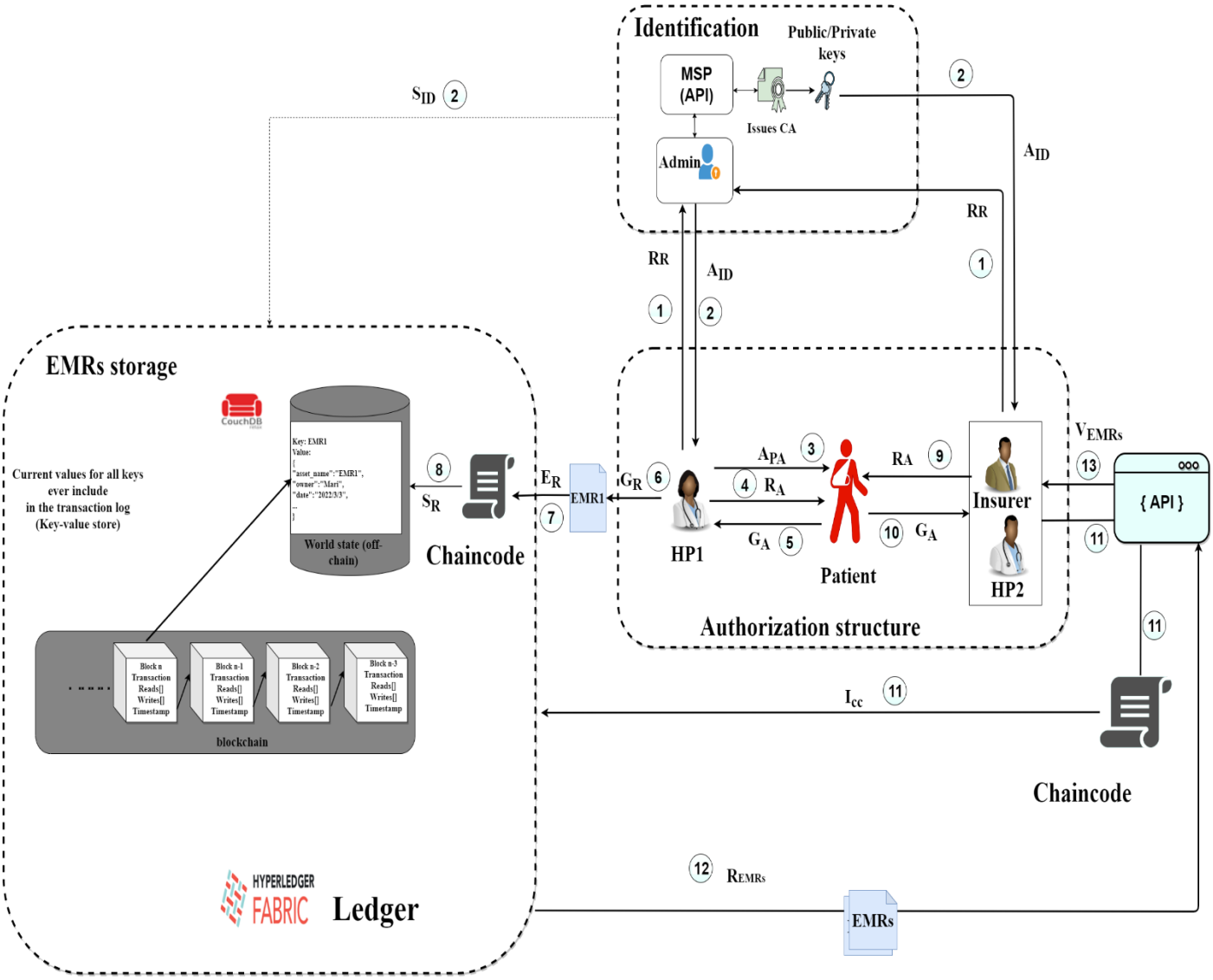

Figure 6 Proposed system architecture

Table 2 Steps' abbreviations

Abbreviations			
MSP	Membership service provider	**G_R**	Generate record
CA	Certificate authority	**E_R**	Encrypt record
R_R	Request registration	**S_R**	Store record
A_{ID}	Attribute ID	**HP**	Healthcare provider
S_{ID}	Store ID	**I_{CC}**	Invoke chain code
A_{PA}	Add patient account	**R_{EMRS}**	Retrieve EMRs
R_A	Request access	**V_{EMRS}**	View EMRs
G_A	Grant access		

System architecture logic flow

① Stakeholders (healthcare providers and insurers) request for membership registration from the network Admin.

② The certificate authority (CA) generates public/private keys for each network member via the fabric MSP.

③ Initially, a healthcare provider, who is also responsible for generating EMRs, creates the patient account.

④ In the event that a patient already has a medical account on the Blockchain network, a healthcare provider may request access to the patient's medical history.

⑤ The patient grants his EMRs access permission by adding the requester to his list of authorized members.

⑥ When a healthcare provider has access, he can then generate EMRs based on the patient's health status, to be appended to the latter history.

⑦ The obtained record is encrypted along with the chain code rules.

⑧ The EMR is saved as JSON format in the CouchDB while the transaction hash is attached to the chained list of blocks (the blockchain).

⑨ A healthcare insurer may request permission to view the patient's EMR or verifies the integrity of records.

⑩ By adding the new requester to his list of approved members, the patient permits access to his records.

⑪ The authorized user searches the concerned patient on the system, the process invokes the chain code to retrieve the EMRs.

⑫ The associated records are retrieved from the CouchDB via the transactions hashes and synchronized.

⑬ The data requester can access records that have been retrieved via file blocks from the entire network associated with the file hashes index.

This sequence of actions is automated on the chain code-enabled system and does not involve external parties.

5.3 QUALITATIVE ANALYSIS

This sub-section covers the evaluation undertaken for our design. We proposed the design to address existing issues. The novel idea in the context of Conakry is that patients' EMRs are unified in the distributed Blockchain network. Besides, they can control their medical records and allow permission requests for accessing their medical history; this way, their privacy is protected. We conducted a qualitative comparison between our solution and the current system. As outlined in Table3, we analyzed its pros and cons based on seven aspects. The evaluation presented proves our proposal's robustness based on the highlighted technology. It is subject to replacing the current method of storing medical records by applying Blockchain technology considering the promising practical significance. Comparatively, healthcare institutions that will adopt such an approach will have more advantages than those using the current method.

Table 3 comparison of the existing system and the proposed solution

	Current system	Our Approach
Decentralized	No	Yes
Patient-centric	No	Yes
Private protection	Weak	Strong
Sharing Operation	Under referral bulletin, time-consuming	Fine-grained data with micro-request/grant
Architecture	Fragmented, scattered, inaccurate	P2P, continuous medical history
Administration cost	Require a lot of human resources, is time-consuming	Automatic consensus execution fast and accurate
Legal regulatory	Possible leakage, fraud	Proper identification and integrity ensured

The proposed solution can be sufficient for meeting improved healthcare coordination in Conakry. It can significantly reduce delayed communications and lengthy workflow among healthcare stakeholders, especially in emergencies. Adopting such a solution can also be beneficial economically as patients will no longer spend additional fees on repetitive medical examinations in different healthcare institutions. Another important aspect is that our proposal can contribute to implementing unique identifiers that improve tracking and monitoring processes that constantly change among healthcare stakeholders. The approach can considerably enhance records integrity, transparency and combat differential versioning of identities, thus enabling secure healthcare stakeholders' identification in Conakry.

6. CONCLUSION

In this paper, we proposed a Blockchain-based design to address existing issues in the healthcare sector in Conakry. Our study scope is the adoption of this new technology in the context of developing countries. We briefly presented Blockchain fundamental concepts and detailed the design process we adopted. Based on the Hyperledger Fabric framework, we proposed a decentralized patient-centric design to secure EMRs by ensuring their integrity between medical stakeholders. This work may serve as a basis for in-depth analysis in improving the healthcare sector in many developing countries, particularly in sub- Saharan African countries. However, the development of solutions based on Blockchain presents several difficulties, and its application still has several challenges that require more efforts. These hurdles include integrating medical professionals to adopt these new tools, improving internet infrastructures and computation resources for higher bandwidths. In the future, we recommend an implementation of the proposal and testing the solution in a medical environment with real EMRs. We also recommend studies concerning the readiness and acceptance of Blockchain in various healthcare facilities in developing countries.

References

1. Tawornittayakun, J. and A. Leelasantitham, A Comparative Study of Library Information Storage System through Blockchain Technology: A Case Study of Undergraduate Researches. 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, ECTI-CON 2020, 2020(7): p. 5-8.
2. Nakamoto, S., Bitcoin: A Peer-to-Pear Electronic cash System. 2008.
3. Belotti, M., et al., A Vademecum on Blockchain Technologies: When, Which, and How. IEEE Communications Surveys and Tutorials, 2019. **21**(4): p. 3796-3838.
4. Xu, X., I. Weber, and M. Staples, Architecture for Blockchain Applications. 2019.
5. Ricci, P. and V. Mammanco, RemBit: A blockchain based solution for remittances to Ethiopia. Proceedings - IEEE Symposium on Computers and Communications, 2019. **2019-June**: p. 1165-1170.
6. Medina, A., M. Smoljan, and S. Parfenova, Blockchain and Sdgs : Programming a Sustainable World. 2014: p. 27-27.
7. Edwardsson, E. and E. Giannisi, Trading transparency: How it affects the coffee farmers? 2019.
8. Samuel, O., et al., Leveraging blockchain technology for secure energy trading and least-cost evaluation of decentralized contributions to electrification in sub-Saharan Africa. Entropy, 2020. **22**(2).
9. Kombe, C., et al., Blockchain Technology in Sub-Saharan Africa: Where does it fit in Healthcare Systems: A case of Tanzania. Journal of Health Informatics in Developing Countries, 2019. **13**(2): p. 1-1.
10. Azaria, A., et al., MedRec: Using blockchain for medical data access and permission management. Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016, 2016: p. 25-30.
11. Dagher, G.G., et al., Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 2018. **39**(August 2017): p. 283-297.
12. Madine, M.M., et al., Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records. IEEE Access, 2020. **8**: p. 225777-225791.
13. Sun, J., et al., A blockchain-based framework for electronic medical records sharing with fine-grained access control. PLoS ONE, 2020. **15**(10 October): p. 1-23.
14. Hasavari, S. and Y.T. Song, A secure and scalable data source for emergency medical care using blockchain technology. Proceedings - 2019 IEEE/ACIS 17th International Conference on Software Engineering Research, Management and Application, SERA 2019, 2019: p. 71-75.
15. Fan, K., et al., MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. Journal of Medical Systems, 2018. **42**(8): p. 1-11.
16. Tith, D., et al., Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. Healthcare Informatics Research, 2020. **26**(1): p. 3-12.
17. Chen, Y., et al., Blockchain-Based Medical Records Secure Storage and Medical Service Framework. Journal of Medical Systems, 2018. **43**(1).
18. Shi, S., et al., Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID- 19 . The COVID-19 resource centre is hosted on Elsevier Connect , the company ' s public news and information. 2020(January).
19. Engelhardt, M.A.J.T.I.M.R., Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. 2017. **7**(10).
20. Hewa, T., M. Ylianttila, and M. Liyanage, Survey on blockchain based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications, 2021. **177**: p. 102857-102857.
21. Ferdous, M.S., et al., Blockchain Consensus Algorithms: A Survey. 2020: p. 1-39.
22. Usman, M. and U. Qamar, Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. Procedia Computer Science, 2020. **174**: p. 321-327.
23. Doumbouya, Accessibilité des services de santé en Afrique de l'Ouest : le cas de la Guinée. 2008: p. 20-20.
24. National Directorate of Community Health, G., Plan de suivi evaluation du plan strategique de la santé communautaire 2018-2022. 2019. p. 1-38.
25. Somparé, A.W., La politique et les pratiques de santé en Guinée à l' épreuve de l' épidémie d' Ebola : Le cas de la ville de Conakry. [Health policy and practice in Guinea facing the Ebola epidemic: The case of the city of Conakry.]. Santé et politiques urbaines, 2017. **78**.
26. Nawari, N.O. and S.J.J.I.T.C. Ravindran, Blockchain technology and BIM process: review and potential applications. 2019. **24**: p. 209-238.
27. Wei, P., et al., Blockchain data-based cloud data integrity protection mechanism. 2020. **102**: p. 902-911.
28. Singh, A., et al., Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Computers and Security, 2020. **88**: p. 101654-101654.

29. Mandloi, J. and P. Bansal, An empirical review on blockchain smart contracts: Application and challenges in implementation. International Journal of Computer Networks and Applications, 2020. **7**(2): p. 43-61.
30. Yao, W., et al., A Survey on Consortium Blockchain Consensus Mechanisms. 2021: p. 1-51.
31. Valenta, M. and P. Sandner, Comparison of Ethereum, Hyperledger Fabric and Corda. Frankfurt School Blockchain Center, 2017(June): p. 8-8.
32. Seth, S., Public, Private, Permissioned Blockchains Compared. 2021.
33. Foley and Lardner, Types of Blockchain: Public, Private, or Something in Between | Foley & Lardner LLP - JDSupra. 2021(August).
34. Abbas, K., et al., A Blockchain and Machine Learning-Based Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry. Electronics, 2020. **9**(5).
35. Androulaki, E., et al., Hyperledger fabric, in Proceedings of the Thirteenth EuroSys Conference. 2018. p. 1-15.
36. Kaur, J., R. Rani, and N. Kalra, Blockchain-based framework for secured storage, sharing, and querying of electronic healthcare records. Concurrency and Computation: Practice and Experience, 2021. **33**(20).
37. Chenthara, S., et al., Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS One, 2020. **15**(12): p. e0243043.
38. Miyachi, K. and T.K. Mackey, hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information Processing and Management, 2021. **58**(3): p. 102535-102535.
39. Saraiva, R., et al., MIRIAM: A blockchain-based web application for managing professional registrations of medical doctors in brazil. IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021, 2021: p. 9-10.
40. Stewart, S., medical chain. 2018.
41. Krishnan, R., Hyperledger. 2020.
42. Nawari, N.O. and S. Ravindran, Blockchain technology and BIM process: Review and potentialapplications. Journal of Information Technology in Construction, 2019. **24**: p. 209-238.