# Blockchain-based Electronic Healthcare Information System Optimized for Developing Countries

Anass Rghioui, Said Bouchkaren, and Anas Khannous

*Abstract*—**Healthcare is the most crucial sector in people's life. Many applications and systems have been proposed to improve the healthcare area. The outbreak of the novel coronavirus Covid19 turns more focus on healthcare applications.**

**To manage medical data, healthcare professionals in developed countries have adopted several electronic healthcare information systems and technologies in recent years. However, these technologies show serious privacy risks and security issues, especially in the transfer of data and the recording of data transactions. Furthermore, the high cost of these technologies acquisition, as well as the complexity of their management, make their application in underdeveloped nations extremely problematic.**

**This article proposes a solution based on a decentralized Blockchain architecture to reinforce the security of health information systems. This solution is particularly recommended for developing countries which lack high-tech infrastructures and suffer from poor interoperability between existing information systems.**

**Various researches and works that implement blockchain-based solutions in the security of electronic health information systems (eHIS) are discussed in this article. A new approach based on a hyperledger fabric, implementing smart contracts and several other components is proposed. The suggested architecture involves many actors who can interact with medical records such as patients, doctors, pharmacists, laboratories and insurance companies. Data privacy is guaranteed because there is minimal risk of unauthorized access entities, and by design, the smart contract is the sole way to manipulate participant data. Various optimization and measurement experiments were carried on. The results covering various key parameters of system performance such as throughput, latency, CPU usage, memory consumption and network usage are presented.**

*Index Terms*—**blockchain, electronic healthcare information system, eHIS, EHR, EMR, PHR, e-Healthcare, Developing Countries, LMIC**

## I. Introduction

ELECTRONIC HEALTH INFORMATION SYSTEMS (eHIS) are computerized systems that facilitate the management of patient data to improve health services. They ensure the exchange of information between healthcare practitioners and patients.

These systems are generally centralised systems, which take the form of Electronic Health Records (EHR), Electronic Medical Records (EMR), Patient Health Record (PHR) [1] or other types [2]. The stored information includes medical history, lab test results, demographic data, and billing information [3]. The healthcare system is made up of all formal and informal public and private institutions to promote, restore or maintain people's health [4].

eHIS aims to improve the quality of healthcare services by enabling optimal access to information and improving real-time communication, as well as reducing working time, human errors, and increasing procedure accuracy. As a result, healthcare organizations will be able to improve the efficiency and effectiveness of administrative tasks related to the management of patient records. Consequently, patients receive more care.

The first e-healthcare system was introduced in 1991. It consisted of a digital tracking system for monitoring and recording patient data, as well as handling papers and invoices for administration [5]. After that, healthcare providers started sharing these information and put it on the Internet on cloud servers and grant access to documents and patient records via mobile devices to help clinicians gain secure, accurate and faster access to patient data, and for research purposes too [5].

These systems are continuously evolving thanks to the inclusion of new technologies such as Artificial Intelligence, Big Data, IoT and Cloud Computing, to provide cooperative health services to enable more personal healthcare [5].

Therefore, storing, communicating and analysing patients' records over public network raises major concerns about privacy and security of patients' sensitive data such as authentication credentials, personal information and medical records.

Nowadays, more and more private and sensitive information is stored and managed electronically. These information are personal data and must be properly protected against unauthorized access as indicated by the General Data Protection Regulation (GDPR) EU 2016/679 [6].

Due to the legal component of medical information protection and the confidentiality of patient data, we must keep in mind that the healthcare system has special security and confidentiality standards. This forces us to be aware of its technical aspects and requirements during the preparation phase of the technical specifications of any healthcare solution.

### A. Security issues and challenges

Health records require strict control of access mechanisms to prevent data healthcare recipients from being tampered

Manuscript received August 09, 2021; revised July 09, 2022.

Anass Rghioui is a full professor and SIRC Research Team member at Hassania School of Public Works (EHTP) Casablanca, Morocco e-mail: a.rghioui@ehtp.ac.ma.

Said Bouchkaren is a full professor and ERMIA Research Team member at National School of Applied Sciences (ENSAT) Abdemalek Essaadi University, Tangier, Morocco. (e-mail: sbouchkaren@uae.ac.ma).

Anas Khannous is a full professor and ERMIA Research Team member at National School of Applied Sciences (ENSAT) Abdemalek Essaadi University, Tangier, Morocco. (e-mail: akhannous@uae.ac.ma).

or viewed by unauthorized parties. Especially since health service providers store records in a central database. Despite the implementation of numerous protection systems, eHIS remain ineffective at the required level [7]. Despite the use of cryptographic mechanisms, which are among the most efficient and widely used solutions, the use of different cryptographic standards in different systems can become a problem and will not allow interoperability.

Actually, sharing health records is an unavoidable requirement. Healthcare recipients move from one place to another, a patient may need some of his medical records stored at the hospital where he has his medical follow-up for a specialized treatment in another hospital. It is a difficult task when using independent systems, as it is difficult for people involved in health systems or healthcare recipients to be aware of data scattered among these systems [8], due to the correlation of records based on dispersed entities which may or may not share a common identifier [9].

### *B. Healthcare security requirements*

Each medical examination produces valuable sensitive data belonging to the patient that must be properly shared with physicians, analytical labs, pharmacies, insurance companies or other actors in the healthcare scenario. At the same time, it must be protected against other access.

All of these personal medical data is usually stored in a single electronic medical record, usually managed by medical institutions and practitioners who are not technically informed or well-appointed to guarantee the appropriate level of security.

Health data requires a high level of security. This requires consensus between healthcare providers and regulators, as well as the creation of agreed policies and procedures. This includes managing access control to patient information, securing patient data from unauthorized users, as well as modifying and destroying stored data, etc. As the size of health data increases, strong security mechanisms are needed to protect these data.

General rules of data security are almost the same across all areas, but each of them has its own specific security requirements. In healthcare, any system or application should consider the following security points [10]:

- Confidentiality: the electronic healthcare information system must ensure that health data is preserved and cannot be accessed by unauthorized entities. Patient data and information must not be provided to any third party without his permission.
- Integrity: the state of health data must not undergo any deliberate or accidental alteration or destruction during processing, storage or transmission, and must retain a format allowing their use by authorized entities.
- Availability: it helps maintain the proper functioning of the information system so that health data must be available when required, without delay.
- Authentication: it consists in assuring the identity of a user, and guaranteeing to each of the correspondents that the healthcare provider or the healthcare recipient is indeed who he believes to be. Access control is required to guarantee that only the authentic party has the right to access or modify health data.
- Non-repudiation: it is used to ensure that a transaction cannot be denied. Neither the healthcare provider nor the healthcare recipient can refuse or deny the data provided.
- Audit: it refers to the veracity of the requesting entity, which means that only the authentic party can access or modify the health data [11].
- Access control: the system must subject access to data to full control and ensure the identity and the right of the person or the entity to access such data, whether public or private [12].
- Data refresh (freshness): it makes sure the data is fresh and consistent. Any asynchronous update between the different entities or delay in providing the necessary data for a diagnosis could lead to a disaster affecting the life of the patient and the quality of his treatment.
- Property: specifically for health data, regardless of the creator and generator of this data, it belongs to the patient with all rights.
- Anonymity: it refers to the confidentiality of patient identity, withheld from public and unauthorized entities. It ensures that the data thus stored guarantees the anonymity of patient identification [13].
- Secure Data Transit: it ensures that data in transit is also secure and is not changed or observed. It guarantees that the adversary will not have access to the data in transit, nor will it be able to inspect or modify it [14].

Electronic healthcare information systems must be reliable and secure. However, several studies have concluded that these systems lack effective management of health records shared between several organizations [15]. These systems present problems of interoperability, confidentiality and data integrity [16]. Developed countries have managed to solve a lot of problems by proposing a set of standards and solutions to protect their health information such as the Health Level Seven (HL7) [17] and HIPAA [18] standards.

These solutions focus on existing systems that are based on a centralized architecture, while they run the risk of a single point of failure and insider threats such as untrusted administrators. Also, these solutions do not take into account the implementation constraints in developing countries that suffer from several problems and which will be detailed in the following section.

### *C. E-healthcare in developing countries*

In developing countries, particularly in sub-Saharan Africa, several efforts have been made to develop e-health systems. Improved Internet access increased collaborations between health facilities and international partners, which increased the use of Information and Communication Technologies (ICT) in healthcare practice [19]. Unfortunately, the adoption of healthcare information systems is limited in these countries, despite the enormous benefits derived from its use. Unfortunately, implementation still very weak [20], [21].

Many factors hinder widespread adoption of an electronic healthcare information system in developing countries. Main reasons identified as the high purchase and maintenance costs of such systems, unstable Internet connectivity, limited IT skills of primary users, lack of health and IT professionals, high cost of telecommunications, etc [22]. Adoption of such systems is very slow and varies from country to another [23], [24]. Even within the same country, there is a huge difference between urban and rural areas, between public and private institutions, and between a health sector and another [25].

However, Covid19 pandemic has made the provision of similar systems a necessity and an urgent need rather than a luxury. About half of the world's population have been urged to stay at home to prevent the spread of the deadly Covid19 virus [26]. Mobility restrictions have emerged as an obstacle for patients who suffer from various acute and chronic illnesses and need to see a doctor regularly. Not being able to get medical help for a long time can increase their health risk. With the lockdown, people who were far from their home and who follow a doctor or a healthcare center far from where they were confined, found themselves without documents and without a history of their medical follow-up [27]. It makes thing more complicated since it is necessary to redo tests and analyzes, a waste of time for doctors who are busy caring for patients infected with the virus and whose staff lack human resources.

Countries which have adapted a connected electronic healthcare information system have been able to quickly manage the situation and the patients have been able to benefit from healthcare services even remotely, unlike patients in developing countries who found themselves without any follow-up and they were forced to go to hospitals despite the risk, or to stay at home as their condition worsens day by day [28], [29].

One of major health problems around the world is the high cost of care, especially in Low-to-Middle-Income Countries (LMIC). For this, health insurance systems have been put in place to ensure access to healthcare services for everyone. Developing countries face particular challenges in scaling up health insurance due to particularly limited public resources for health care, inefficient allocation, overdependence on out-of-pocket payments and a large population [30]. Even with insurance, the different conceptions of insurance models make support difficult and the delay in processing files leads to a delay in reimbursement. These present obstacles to the use of their services and generate enormous social problems such as non-access to care despite the presence of a care offer [31]. There is a huge difference between coverage in developed and developing countries. Insurance schemes in LMIC exclude populations from the informal sector because of difficulties in traceability, and the larger the informal sector, the greater the coverage gap, due to the lack of clear data [32].

Following these several problems linked to health insurance, which is a very important component for facilitating access to care, new mechanisms in electronic healthcare information systems must be put in place, making the insurer a key stakeholder in the overall system.

### D. Organization

This paper deals with problems presented above in two parts: the first part concerns the study and the definition of the needs for the security of a health information system in general and the case in developing countries in particular. The second part focuses on proposing a suitable and optimized solution for developing countries and for any organization that lacks resources to deploy a sophisticated IT solution. The study conducted in this paper propose a blockchain-based system. A solution that should be able to solve both the security and management issues of current centralized systems, and also a technology that can be adopted by countries which lack the resources but which have a minimum to deploy a computerized and Internet-based information system.

The choice of blockchain technology as a solution will be defended in the next section, where also the requisite background knowledge regarding blockchain is presented. In the other sections, the paper is organized as follows: Section 3 examines related works; the paper presents related research in blockchain applications in healthcare. A detailed overview of the proposed system network and architecture is described in Section 4. The paper presents an overview of the blockchain solution network and the system architecture, followed by the proposed algorithms. To further illustrate the feasibility of the proposed solution, a test of the performance and the optimization of the proposed framework is performed and presented in Section 5. This section also includes a description and discussion of the results obtained using various optimization metrics. Finally, Section 6 concludes this study.

## II. BLOCKCHAIN AS A SOLUTION

### A. Solution requirements

According to the studies of [24], there is a strong possibility of introducing healthcare services based on Information and Communication Technologies (ICT) in developing countries. Despite the large difference recorded between urban and rural areas in some of the countries concerned by the study. The majority between African and Asian countries experience a high penetration of the use of mobile telephony, that reaches 100%, and a high rate of internet use, that exceeds 30%, but it varies from a country to another [24]. Especially since these countries suffer from a low rate of the number of doctors and health services.

However, it should be noted that several challenges hinder the use of healthcare information systems. A traditional system will not be sufficient because of the problems mentioned below.

To meet these challenges, the proposed system must offer new functionalities and meet the majority of constraints:

1) a decentralized system to avoid single point of failure problem;
2) a secure system respecting the security and privacy requirements of any healthcare information system;
3) a system accessible to everyone;
4) an interoperable system between the different HIS, since traditional HIS were never designed to manage multi-institutional medical records. As patients move from one healthcare provider to another, their data is scattered across different organizations, losing access to past records;
5) a mobile system where the patient's data belongs to him and he has access whatever the conditions that prevent him from directly consulting his doctor;
6) a low-cost system, easy to deploy by LMIC.

One of the technologies showing promise for meeting these general and specific needs for developing countries is Blockchain technology [32]. Blockchain provides many services, including traceability, integrity, security and non-repudiation, while storing all information in a decentralized manner to maintain confidentiality, removing the need for a trusted central authority [32]. Blockchain is rapidly gaining its place by integrating with other technologies such as cloud [33], IoT [34] and others. However, in developing countries, very little attention has been given to the issues of interoperability, privacy and data integrity for healthcare information systems using blockchain technology.

### B. Blockchain

Most medical institutions store and create patient medical records in different formats that are often incompatible between different organizations, sometimes even between different laboratories in the same hospital. The need for a unified system to securely manage and store medical records has led to many proposals for the use of a blockchain in this field [10], [32], [35].

The characteristics of the blockchain are :

- Distributed ledger: transactions are added to a distributed system over the network, which creates system recovery by eliminating a single point of failure or centralized entity. All transactions in a blockchain network are recorded, while the shared distributed ledger cannot be altered or tampered with.
- Smart contracts: smart contracts are a major implementation of blockchain technology and allow a user or agent to create a legal document through the use of the blockchain system. Smart contracts are autonomous agents that are stored in blockchain technology that encodes and transforms transactions into a contract or legal documents to provide legal services.
- Authentication: it is accomplished by requiring a specific private key linked to a public key to initiate the creation, modification or viewing of information stored in the blockchain.
- Consensus mechanism: the consensus of a blockchain is defined from its creation by its founders. Transactions are only updated when all verified users on the network accept the condition of the transaction. This depends on the type of blockchain used, public, private or consortium.
- Hash cryptography: a blockchain uses the SHA256 hash to add transactions. This is developed by the NSA and is 64 characters long. Hash algorithms include features such as unidirectional cryptography, deterministic and faster computation, avalanche effect and must resist collisions.

These properties make blockchain technology attractive to certain communities of health IT researchers and practitioners as means to improve clinical communications while protecting the privacy of healthcare participants. The remainder of this article examines how to effectively leverage an optimized blockchain-based system to securely share clinical data that enables collaborative decision support.

Blockchain system is not without limitations. As a relatively new and immature technology, there is a lack of standardization and this hinders its wide acceptance and slows down development [33]. This can be an advantage for organizations and countries that do not yet have laws or standards in this direction and suddenly they remain more flexible compared to others for the adoption of this technology according to their needs.

### C. Research Contribution

To address issues above, this paper offers an alternative: a distributed healthcare information system using blockchain. Which can function as a full-fledged solution, standalone solution, an alternative to or an annex to existing centralized healthcare information systems.

This article proposes a blockchain-based framework for efficient storage and maintenance of health records. It provides secure and efficient access to medical data by healthcare recipients, healthcare providers and other entities such as pharmacists, laboratories and Insurance companies, while preserving the patient's private information. This article aims to analyze how the proposed framework meets the needs of patients, providers, and third parties, and to understand how the framework parameters can be optimized to offer better performances.

## III. RELATED WORK

Blockchain Health data is a valuable source of health information. Sharing health data is an essential step in making the health system smarter and improving the quality of health services. Health data should be owned by the patient to prevent endangering patient privacy, instead of being dispersed across different healthcare systems.

In today's age of smart cities and smart homes, patients' private information such as name, address and illness are routinely breached, which is indirectly related to the security of healthcare information systems. For security purposes, existing electronic healthcare information systems have made data generally inaccessible to patients. These systems struggle to provide an effective balance between data privacy and the need for patients and healthcare providers to interact with data on a regular basis. Blockchain technology solves the aforementioned problem because it shares data securely in a decentralized and transactional way.

Relying on the use of a blockchain platform to develop a health data management solution in developing countries, lacking financial and human capacity, is justified given that this technology reduces development costs. The blockchain network is inexpensive and efficient due to its ability to eliminate duplication and reduce the need for middlemen, resulting in low cost of operation compared to non-blockchain network. It is also less vulnerable to attacks because it uses proven models to verify information; therefore, transactions are secure, authenticated and verifiable. Healthcare organizations will have the opportunity to reduce the need for manual intervention for data aggregation, modification and sharing. Regulatory reporting and audit documents could become easier, requiring less manual processing. As a result, employees could focus exclusively on value-added activities [36].

Due to the growing interest in using distribute ledger technologies for electronic healthcare information systems, related work has explored various blockchain-based design considerations and prototypes. This paper pulls some of the main motivation of this work to explore blockchain in healthcare. This section summarizes these related works.

Estonia is one of the most digitally advanced countries and one of the first to use blockchain to protect citizens' data [37]. In 2011, Estonia collaborated with Guardtime which operates a healthcare platform based on Blockchain technology. Since then, Estonian citizens, healthcare providers or health insurance companies have been able to retrieve all the information about medical treatments performed in Estonia using the Guardtime Blockchain. Estonia has thus proven that a complete public health infrastructure can be operated using Blockchain.

MedRec is a solution supported by the MIT Media Lab Consortium [38]. It is a decentralized case management system to manage EHR, using blockchain technology. The system design gives patients a complete and unchanging log and access to their medical information across providers and treatment sites. The validation goes through the actors of the health sector (researchers funded by the government, public health authorities, etc.) to participate in the network as "miners" of the blockchain. This gives them access to aggregated and anonymized data as mining rewards, in exchange for the sustainability and security of the MedRec network via proof of work.

Medicalchain allows the user to give healthcare professionals access to their personal healthcare data [39]. Medicalchain then records interactions with this data in an auditable, transparent and secure manner in Medicalchain's distributed ledger. Also, Medicalchain is a platform that others can use to build applications that complement and enhance the user experience.

FHIRChain contributes to the use of blockchain technologies in sharing clinical data to improve collaborative decision support by using HL7's Fast Healthcare Interoperability Resources (FHIR) data elements in conjunction with a Token-based design to exchange data resources in a decentralized and verifiable manner, without uploading data to a centralized repository [40].

MEDIBCHAIN is a platform that gives the control of the private data of the patients to themselves [41]. The main idea of this solution is to keep sensitive health data on the Blockchain. Patients will have overall control over the blocks where their data will be stored, offering patients pseudonymity.

BHEEM offers a blockchain-based framework for efficient storage and maintenance of EHRs [42]. By offering the patient sole control and ownership of his records, he can monitor the transactions that take place there. Unauthorized access by various actors is further minimized and a sense of decentralization while consisting of certain nodes with improvised authority is achieved.

SimplyVital Health provides an ecosystem to create a health market and the opportunity to share health data [43], with the aim of reducing friction and increasing financial benefits for providers participating in effective coordination. Also, offering terms for token-based insurance payments and reimbursements.

Robomed is a network of clinical organizations that is controlled and administered by smart contracts based on the Ethereum blockchain [44]. It allows healthcare organizations to register, connect and manage themselves within the Robomed network using Ethereum smart contracts [45].

Gem, an American startup, launched the Gem Health Network based on Ethereum Blockchain technology [46]. Through this shared network infrastructure, different healthcare professionals can access the same information. Gem Health Network represents a healthcare ecosystem that combines businesses, individuals and experts, and which, at the same time, improve patient-centered care while solving operational efficiency issues.

MedShare is a model for sharing data between cloud service providers using blockchain [47]. The design uses smart contracts and access control mechanisms to effectively trace data behavior and revoke access to violated rules and data permissions.

Healthureum is a gateway to secure blockchain-based healthcare operations [48]. It provides users with a secure and transparent method of purchasing and paying for medical services worldwide. It provides instant access to historical and real-time medical data that a patient can share with his doctor. Healthureum operates on the Ethereum blockchain to deploy smart contracts for health-related services.

Hashed Health is a healthcare innovation company focused on accelerating the design, development and meaningful use of blockchain technologies and networks [49]. Hashed Health develops distributed and decentralized solutions that solve health problems.

Patientory, a digital health company, has developed a distributed application solution that provides individual consumers with secure access to their health data [50]. Patientory's distibuted applications (DApp) leverages blockchain technology, an open and secure technology that captures transaction records on connected blocks and stores them in a distributed, encoded database that acts as a ledger. However, users can only access blocks to which they are authorized.

OmniPHR is a distributed model, which targets the integration of PHRs. The solution offers an architecture model to support a distributed PHR, where patients can maintain their health history from anywhere [8]. Model evaluation demonstrates that is able to promote PHR divided into datablocks and proportional distribution in a routing overlay network. The results showed that even by increasing the number of nodes the latency remains stable. This demonstrates that OmniPHR is able to support an increasing number of nodes and requests without significantly increasing the delivery time.

Healthcare Data Gateway (HGD) proposes a blockchain-based application architecture that allows patients own, control and share their own data easily and securely without violating privacy [51]. Their access model is centered on Secure Multi-Party Computing (MPC) which is a solution to allow untrusted third parties to perform calculations on patient data without violating confidentiality.

In one of the few solution offered for developing countries, authors of [52] proposed two blockchain-based systems, an autonomous identity system for already existing health informations systems, that aims protecting data in these existing infrastructures. In addition to a secure and decentralized system for sharing health data between healthcare establishments.

In the pharmaceutical sector, MediLedger project has developed a blockchain ecosystem application that prevents counterfeit pharmaceuticals from entering the pharmaceutical supply chain in the United States [53].

Centralized healthcare information systems suffer from many problems, including managing the mobility of patient files and the security of his data. For this, the blockchain has been proposed as a complement or an alternative to existing systems. However, the literature lacks solutions for organizations with low resources. Especially, blockchain solutions that require mining or very high network bandwidths. The most of studies focus on the technology aspect of the blockchain without taking user experience into consideration as a parameter. For a good management of health data in developing countries, a decentralized information system is seen as a relevant solution, being based on a technology that has its own security mechanisms such as blockchain will avoid many deployment problems. With a management method adapted to users in these countries. As a conclusion, these studies fail to address the deployment of the solution in an environment with low resources, or fail to address the user experience aspect, or both. This is the challenge that the paper will address in the following sections.

## IV. PROPOSED SOLUTION

### A. *Blockchain Network Overview*

The proposed systems will use a blockchain network based on hyperledger fabric (HLF). HLF is an implementation of the blockchain as part of the Hyperledger project of Linux foundation. It is an enterprise-grade permissioned distributed ledger platform that offers modularity and versatility for a broad set of industry use cases.

The following are the blockchain components that are required to build the proposed solution:

- Ledger: it stores the blockchain and patients data. It is maintained by each peer on the channel.
- Smart contract: it is the software that runs on the ledger and defines the rules and the access rights to patients' data.
- Peer network: a network of nodes that is distributed among the participants. The nodes work with each other to reach consensus on the order and correctness of transaction sets, and then complete the transactions that were initiated through the smart contract.
- Membership: membership services authenticate and manage identities on a permissioned blockchain network by using ecerts. An ecert is an enrollment certificate that is the long-term identity of the participant on the blockchain network.
- Events: they are used to integrate with outside systems by creating notifications when smart contract and certain blockchain operations are completed.
- Systems management: it is used to create, change, and monitor blockchain components.
- Client application: client applications always connect to peers when they must access ledgers and smart contracts. Transactions must be endorsed, and only endorsed transactions can be committed and their output stored in the database.
- Ordering service: they order the transactions, group them into a block, and send them to the peers. This action determines the order in which transactions will be committed to the shared ledger. The order is important to ensure that updates of patient's data that are made to the database are valid.
- Membership Services Provider (MSP): it is a component that offers an abstraction of membership operation architecture. MSP abstracts all the cryptographic mechanisms and protocols behind issuing and validating certificates and user authentication.

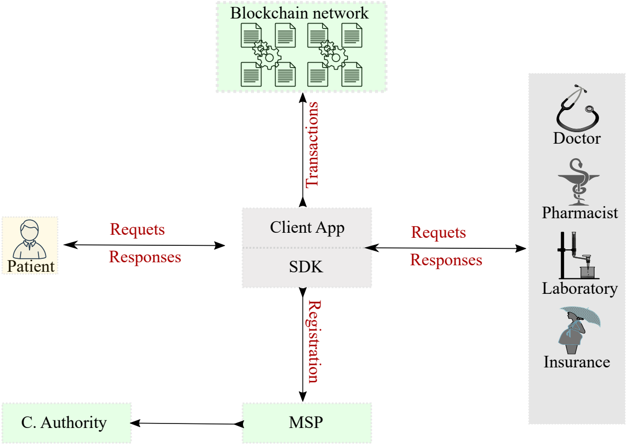

Fig. 1. System architecture

### B. *Architecture*

The pillars of the proposed system; as shown in figure 1; are: SysAdmin, Patient, Doctor, Pharmacist, Laboratory and insurance company. In the current system a number of smart contracts are defined, including: MedicalRecord, InsuranceRecord and AccessControl.

The workflow of the system can be summarized as: Participant uses client app to create personal wallet by requesting a certificate from the certificate authority through the Membership Service Provider (MSP). As a result, the participant receives a certificate and a private key. Transactions are distributed over the Blockchain network and each participant can only access records if he has granted access to. The proposed system will use Hyperldger fabric but it can be easily implemented in other Blockchain systems such as Ethereum.

The participants use client app to interact with the system by invoking smart contracts to commit transactions to the Blockchain network. By design, once a transaction is committed to the network all participants peer receive updates and transactions become immutable, verifiable and cannot be denied by the issuer thanks to cryptography. Records are available to all the users of the network but only authorized participants can view and update records thanks to AccessControl smart contract.

### C. *System Actors Roles*

The system has in total six actors: SysAdmin, Patient, Doctor, Pharmacist, Laboratory and Insurance Company. Each actor has a specific role in the system. Basically, a SysAdmin is responsible for the whole system, such as checking the validity and integrity of participants, adding

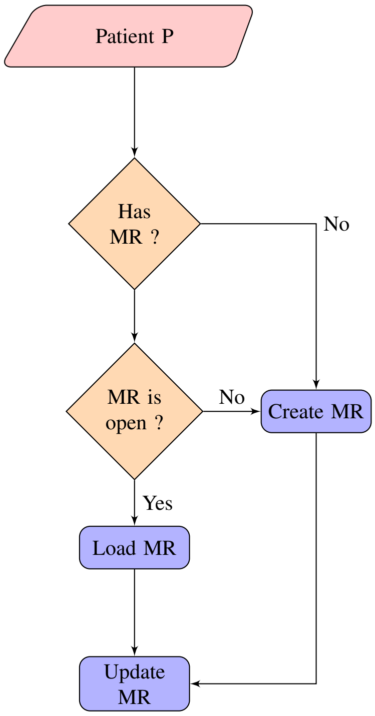

Fig. 2. Medical record lifecycle (creation phase)

and removing users and peers, and granting access to the Blockchain network. A Patient can grant and revoke access to a specific section in his records for a specific participant. A Doctor interacts with Patient by creating medical records, filling his part in the insurance record if applicable. Laboratory and Pharmacist update patient records, fill their part in insurance records if relevant. Insurance companies process insurance records of patients and seal it by marking its state as ”close”.

Each record type (Medical record or Insurance record) has a number of states: “open”: record is open and can be updated, it is the default state upon creation. “close”: record is sealed and cannot be updated.

*1) Medical record lifecycle, Creation part:*

Basically, the first interaction with the medical record (MR) is made by a doctor, he fills the relevant information, based on diagnostic results.

Other participants may interact with the medical record. The whole lifecycle of the medical record is presented in figures 2 and 3 :

- “MC”: Medical Record
- “P”: Patient
- “PH”: Pharmacy

*2) Insurance record lifecycle:*

The first interaction with the insurance record (IR) is made by the patient, he fills the relevant information, after that he submits it to the relevant contributor (Doctor, Pharmacy, Laboratory) and finally to the Insurance Company for processing. Other participants may interact with the medical record. The whole lifecycle of the insurance record is presented in figure 4 :

- “IR”: Insurance Record
- “P”: Patient
- “IC”: Insurance Company
- “NP”: The Next Participant

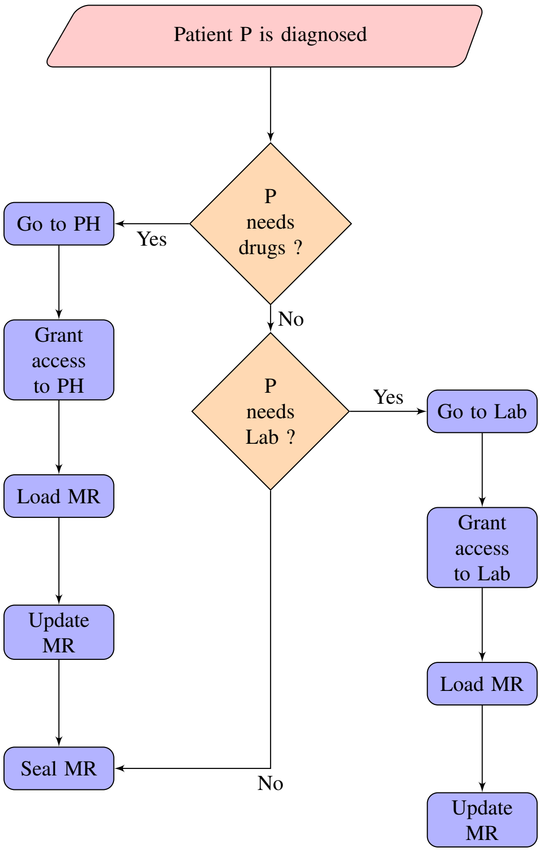

Fig. 3. Medical record lifecycle (Pharmacy and Laboratory access)

*3) System security:*

For Identities, the solution provides:

- A membership service provider (MSP), which maintains the identities of users, admins, peers, and orderers.
- A built-in certificate authority (CA) to issue certificates. The CA can be replaced by an external one.
- MSP manages the user enrollment process, which results in a user identity being issued and delivered to a participant.

For data privacy, by design, the participant data can be manipulated only via smart contract and there is a minimal risk to be accessed by non-authorized entities. To prevent any unauthorized access to participants' data we can implement strong data encryption using AES-256 to encrypt data at rest. To implement encryption, we have two options: encrypt data at client side in this case the overload of the blockchain peers will be decreased but the management of encryption keys will be challenging. The second option is to encrypt data in the network peer side, this option makes the encryption management key easier and can be centralized but the transaction throughput may decrease significantly. This is what the paper will try to verify through experiments and performance tests.

To secure the data in transit, SSL/TLS communication between clients and blockchain network can be implemented. In this case, all data transfer will be encrypted before exiting the client application.

### *D. Off-Chain Solution*

The patient interaction with Blockchain network requires a smart phone or computer with Internet connection, but in

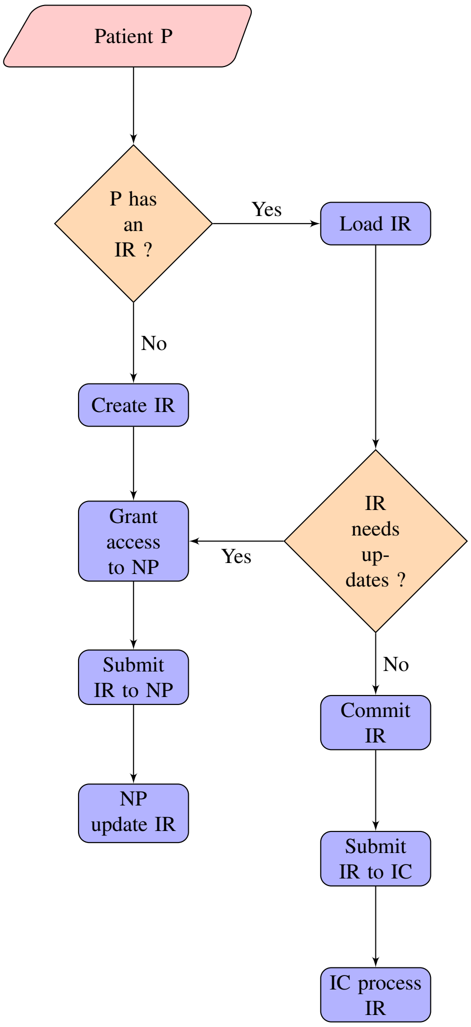

Fig. 4. Insurance record lifecycle

developing countries with limited resources this requirement may limit the use of this system. To address the situation, this solution proposes to use Short Messages (SMS) to interact with the system at least for granting access to other participants and retrieving basic information about records. Using this solution, users having a just simple phone can use services offered by the healthcare system based on Blockchain.

This proposition work as follow: The patient sends an SMS using a specific format to a secured central server, then the server identifies the patient using the phone number and associate him with his personal account, after that the server parses the SMS and instructs the Blockchain on behalf of the patient. This solution is an option but it is not fully secure and patient data privacy may compromised but it still more secure than using traditional medical records.

## V. PERFORMANCE EVALUATION

### A. Implementation & simulation settings

Performance evaluation consists of measuring different configurations of a system by changing different dependent variables. Results help to understand the performance of the system under test.

The solution was implemented through the Hyperledger Fabric framework made up of peers, customers and certification authorities. The measurements of the different experiments were carried out on Hyperledger Caliper. Caliper is used to test the performance of the system with respect to several parameters such as throughput, latency, CPU usage and memory.

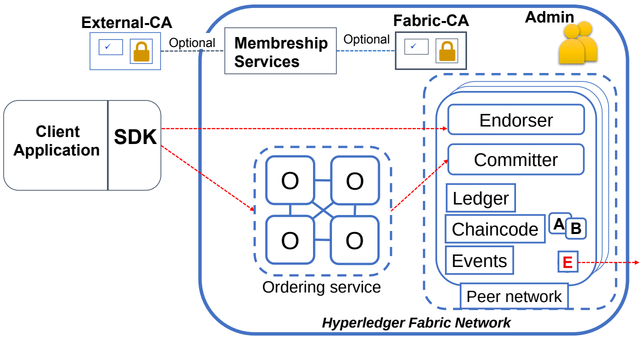

Fig. 5. Experiment system network

Experiments carried out in this work aim to evaluate the different configurations of components of the proposed solution to analyze the impact of each component in order to find the optimal value that can improve the performance of this solution for its deployment in a low resources environment.

Several measurements related to the number of transactions were taken to assess the capacity of the system, based on the data from the report generated by Caliper at the end of each test. This data covers the following metrics: send rate, throughput, maximum, minimum and average latencies. Regarding resource usage, the report presents information on CPU usage and memory consumption. Thus, data on the incoming and outgoing traffic was given. The whole experiment network is illustrated in figure 5.

The simulation configuration is as follow :

- Intel Core i7 (4 cores, 8th generation, 1.8Ghz)
- 8GB of RAM
- 1Gbit/s of network link

For each scenario, the host who took on the role of the Ordering organization was tasked with creating the blocks. The host in charge of Caliper was tasked with executing the charges. Each node of the network carried out the measurements for each experiment. For each of the test scenarios, the same metrics were evaluated based on the number of transactions.

To measure the performance of the solution, experiments were conducted to analyze the effects of varying the number of transactions from 200 to 2000.

The Blockchain basic network in these experiments contains: One ordering organization, 2 Organizations, 2 Certificate authority and 2 peers in each organization. Some network components may change depending the test.

### B. Initial optimization experiments

#### 1) Transaction send rate:

The transaction sends rate defines the rate at which transactions are input to the blockchain network system, which is a key factor for stress testing.

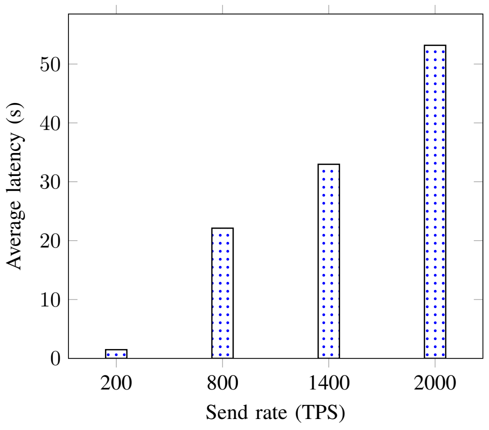

Fig. 6. Average latency vs Send Rate

The sending rate of transactions gives the performance of the blockchain network. As shown in figure 6, when increasing the transaction send rate, the average transaction latency will also increase significantly. This behavior is due to the throughput which represents the amount of completed transactions per second. The number of peers and the processing resources available on the network have a direct impact on this metric.

The results showed that by going from 200 to 2000 transactions in each of the tests, the success rate reached 100% since all the transactions were successful.

*2) Transaction latency:*

Transaction Latency is a network-wide view of the time it takes for the effect of a transaction to be usable on the network. The measurement includes the time between when it is submitted and when the result is widely available in the network. This includes propagation time and any stabilization time due to the consensus mechanism in place.

The measurements are made according to the formula (1) :

$$L_T = (C_t * N_t) - S_t \quad (1)$$

were :

$L_T$ : Transaction Latency
$C_t$ : Confirmation time
$N_t$ : Network Threshold
$S_t$ : Submission time

To take into account these two factors and provide a network-wide view, the latency was measured using all nodes in the system. This metric is calculated per transaction, with reports to provide various statistics on all transactions such as medium, high, low, and standard deviations.

In the blockchain, among the parameters that impact system performance are the block size and the block time.

For the block size test, evaluation was carried out on the blocks of size 5, 10 and 30 in two groups of experiments according to the send rate. The first whose results are displayed at the level of figure 7 consider send rate lower than 1000 transactions per second, so that the second where the results are displayed at the level of figure 8 consider the send rate more than 1000 transactions per second. Note that the latency rate increases linearly with increasing send rate. The results clearly show that under the same conditions, the more the block size is lower, the more the performance is better. For example, for 200 TPS, it was recorded 0.29s for the block size 5, 1.49s for the block size 10 and 3.21s for the block size 30, in the same order of block sizes, it was recorded 2.16s, 4.74s and 13.69s for 400 TPS, 11.81s, 26.42s and 52.85s for 1000 TPS, and 24.1s, 53.21s and 96.35s for 2000 TPS. It is noticed that configuring the block size with a lower transaction rate gives more optimized results. Through this experiment, we also notice that as the transaction rate increases, the latency between a large block size becomes greater than that of a smaller block size.

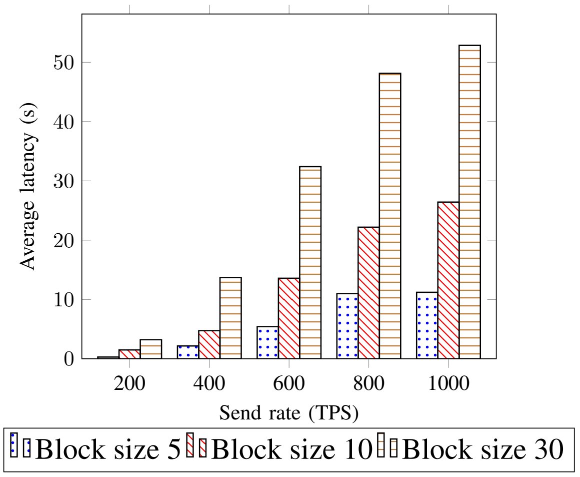

Fig. 7. Average latency with varying block size for lower than 1000 TPS

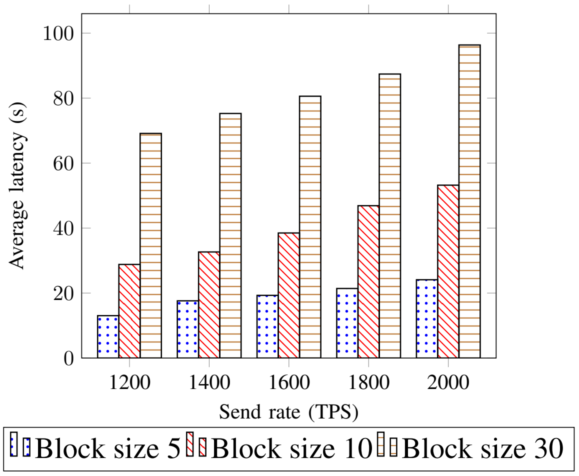

Fig. 8. Average latency with varying block size for more than 1000 TPS

The second parameter that was tested is the block time. In this experiment, the impact of block time on performance was evaluated by varying it between 500ms, 1s and 2s over the two groups of transaction send rates, less than 1000 and more than 1000.

Figures 9 and 10 plots the experimental results of transaction latency. We note that transaction latency increased linearly with increasing send rate in the first experiment of lower than 1000 TPS. When the send rate increased from more than 1000, the latency was increased modestly. For example, the average latency of 2s block time for 200 TPS was 1,49s but 4s for 1s block time and 10.18s for 500ms block time, and records went up for 1000 TPS to 26,42s for 2s block time, 30.07s for 1s block time and 34.14s for 500ms block time. But from 1000 to 2000 TPS, the rise on records

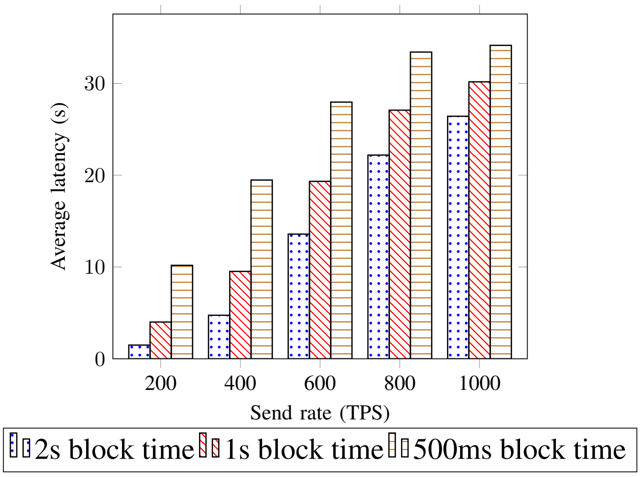

Fig. 9. Average latency with varying block time for lower than 1000 TPS

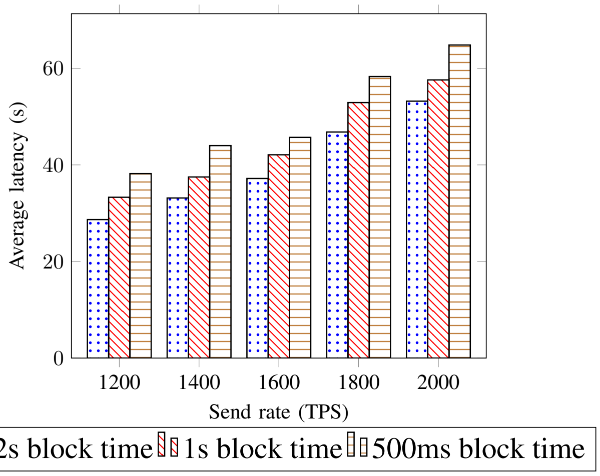

Fig. 10. Average latency with varying block time for more than 1000 TPS

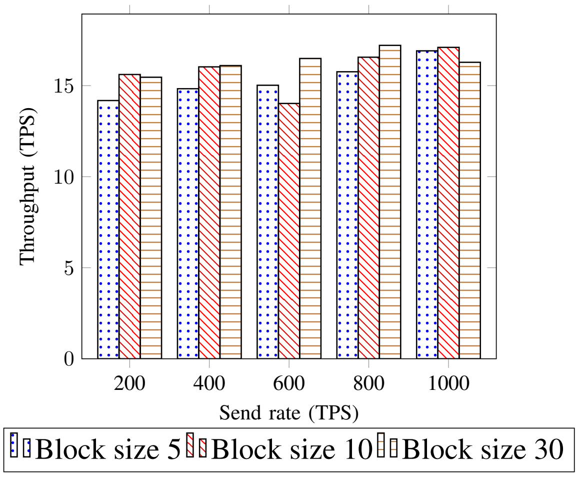

Fig. 11. Transaction throughput with varying block size for lower than 1000 TPS

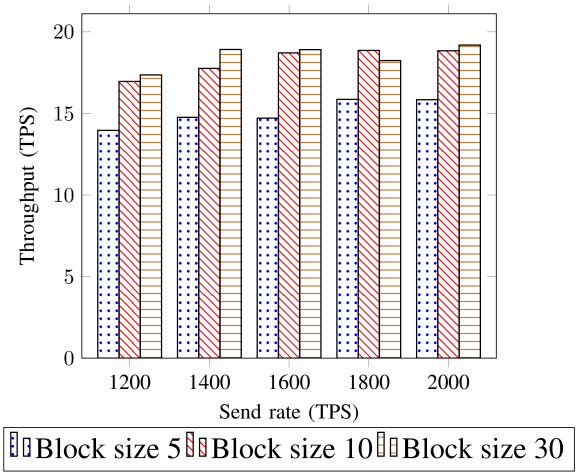

Fig. 12. Transaction throughput with varying block size for more than 1000 TPS

hasn't changed much as for 2000 TPS it was recorded 53.2s for 2s block time, 57,6s for 1s block time and 64.83 s for 500ms block time. The results of this experiment indicate that block time settings have a slight effect on performance. A lower block time shows the worst performance in terms of latency.

*3) Transaction throughput:*

The Transaction Throughput measures the flow rate of processed transactions through the blockchain network, in units of transactions per second, during the test cycle.

The measurements are made according to the formula (2) :

$$TP_T = \frac{V_T}{(T_t * V_n)} \tag{2}$$

were :

$TP_T$ : Transaction throughput
$V_T$ : Total validated transactions
$T_t$ : Total time in seconds
$V_n$ : Validates nodes

Transaction throughput is the rate at which valid transactions are validated by the blockchain within a defined period of time. In this experiment, the throughput was calculated by engaging all the nodes of the network. This rate is expressed in transactions per second (TPS).

The various results of the experiments on the transaction throughput are plotted at the level of the figures 11 and 12 for block size variations tests and 13 and 14 for block time variations tests, over the two groups of transaction send rates, less than 1000 and more than 1000 TPS.

According to the results of the same experiments conducted to test the latency, we notice that the results are the same for the throughput. The more the block size is lower or more the block time is higher the more the performances are improved. Yet for the throughput, we notice that the difference by increasing the bock size or time is modest and the throughput remains more or less stable even by increasing the transaction sending rate.

## C. Encryption impact on performance

Three scenarios were implemented and tested:

- Scenario 1: No data encryption neither client side nor blockchain network side (Without enc).
- Scenario 2: Data encryption in client side (Enc C side).
- Scenario 3: Data encryption in blockchain network side (Enc B side).

*1) Average latency:*

The average latency for the first test without encryption recorded: 1.43 seconds for 200 TPS, with a minimum latency

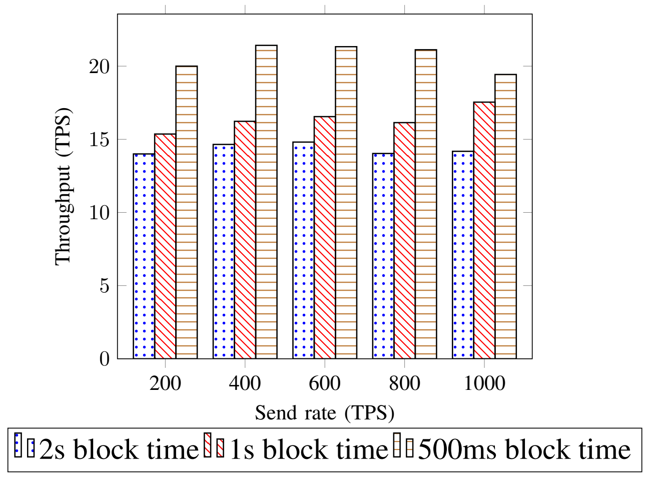

Fig. 13. Transaction throughput with varying block time for less than 1000 TPS

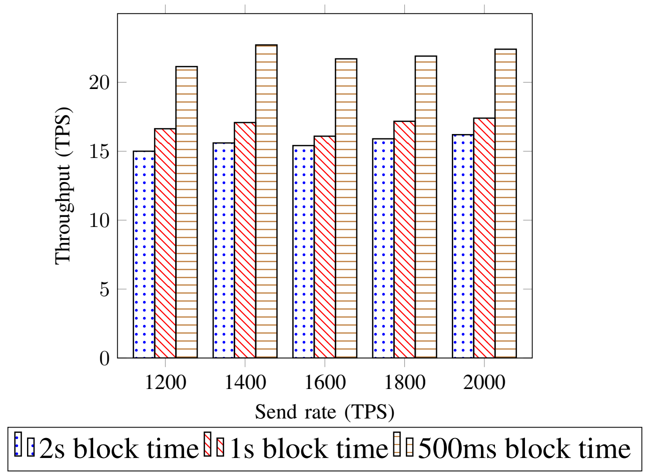

Fig. 14. Transaction throughput with varying block time for more than 1000 TPS

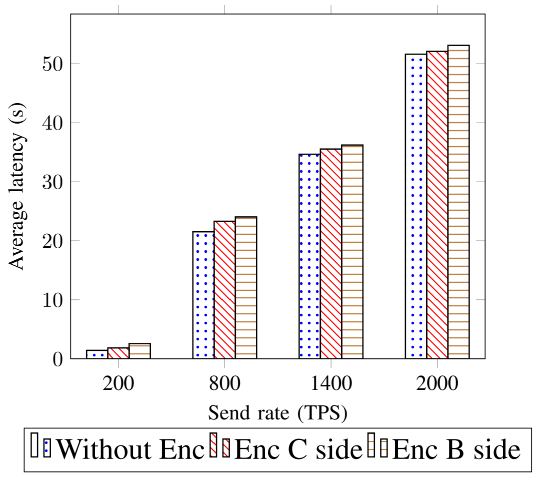

Fig. 15. Transactions average latency with and without encryption

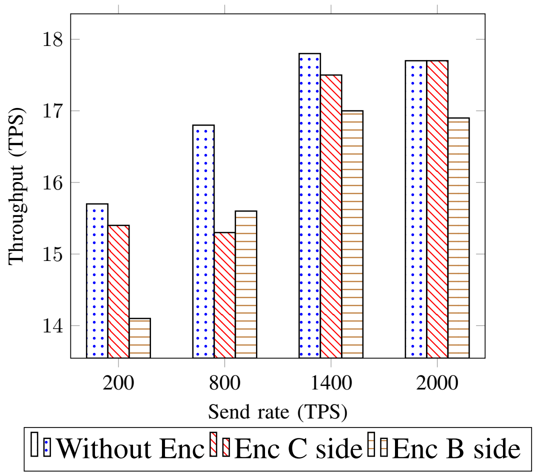

Fig. 16. Transactions throughputs with and without encryption

of 0.66 seconds and a maximum latency of 3.33s; 12.93s for 600 TPS, with a minimum latency of 0.78s and a maximum of 26.49s; 22.7s for 1000 TPS, with a minimum latency of 0.72s and a maximum of 56.75 s; 34.67s for 1400 TPS, with a minimum latency of 0.66s and a maximum of 70.53s and 46.33s for 1800 TPS, with a minimum latency of 0.86s and a maximum latency of 96s. Therefore, for the latency, despite the increase in the number of TPS, the minimum has a good record that does not exceed 0.78 seconds, and for the maximum for the greatest number of transactions is 96 seconds which is good too.

The same can be seen in the results of the average latency for the second test with encryption in client side were it was recorded 1.84 seconds for 200 TPS, 13.18s for 600 TPS, 24.79s for 1000 TPS, 35.55s for 1400 TPS and 47.36s for 1800 TPS, with a minimum latency that varies between 0.45 and 0.86 seconds, and a maximum latency that varies between 2.98 and 100.7 seconds.

Succeeding in having optimized results for our blockchain solution is very important since the solution is intended for developing countries which lack the means and resources to implement and set up sophisticated solutions, especially for this application which will be deployed at the national level and it is necessary to take into account the difficulties of access to the internet as well as the average quality experienced by the networks in these countries.

The latency recorded in the tests is correct and shows that the system will show good results.

*2) Transaction throughput:*

The following average throughput was obtained in the five tests, without encryption it was recorded between 15.7 and 18.3 TPS; with client side encryption it was recorded between 15.4 and 17.3 TPS and with blockchain side encryption it was recorded between 14.1 and 17 TPS.

The same can be said for the throughput recorded during the tests. Since the blockchain is based on networks, succeeding in recording correct and acceptable throughput during transactions remains an essential thing which will decide on the implementation or not of the solution.

*3) Resource consumption:*

For resource consumption, when performing caliber tests for the network, various parameters are measured such as average CPU consumption, memory, inbound traffic, outbound traffic, etc., while CPU consumption of the customer is displayed. Different traffic and memory and processor consumption are shown in figures 17, 18, 19 and 20 considering the orderer, smart contracts (SC) .

The orderer obtains in tests without encryption records of CPU or memory consumption, as well as traffic, less than tests performed using cryptography. We also notice by

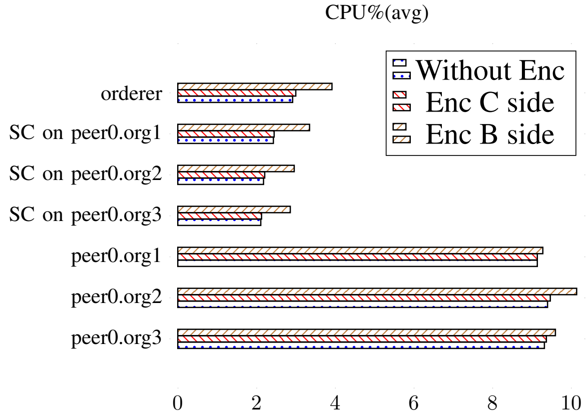

Fig. 17. Average CPU usage time (%)

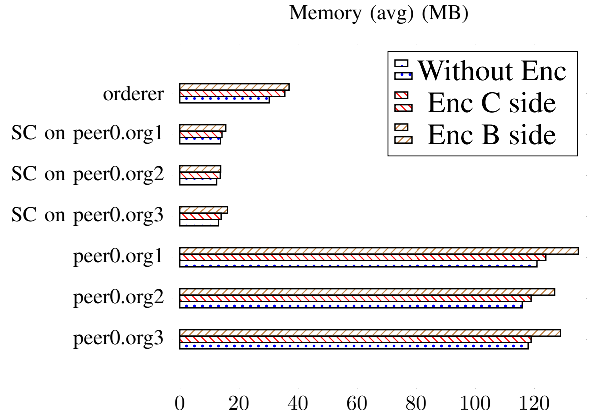

Fig. 18. Average Memory consumption (MB)

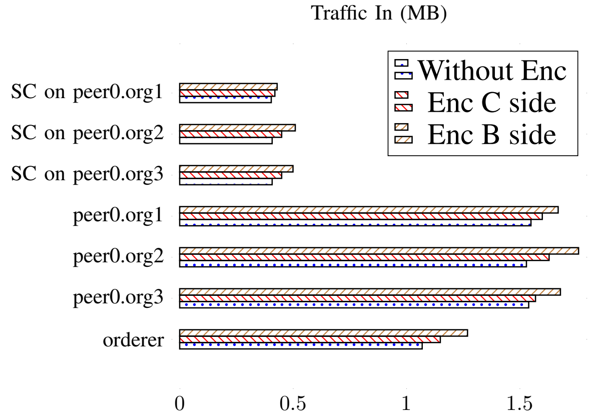

Fig. 19. Input network traffic (MB)

comparing the two tests with cryptography that the records of experiments with cryptography on the blockchain side are higher than the experiences with cryptography on the client side. The latter are almost similar to the recordings for CPU and memory made without cryptography, except traffic, which is quite logical since the results are obtained on the blockchain node side.

That said, for an implementation in developing countries, where the majority of users have low-resource machines, the best solution if we want to add a layer of cryptographic security, to better support it and execute it on the blockchain side.

The system evaluation for the three scenarios shows clearly that adding an encryption layer to the system impact the performances such as latency, throughput, memory and CPU usage. It is clear that the latency is slightly higher when using encryption compared with the average latency when there is no encryption. In the same manner, we remark that throughput is better when there is no encryption and it decreases slightly when encryption is deployed. Also, the memory and CPU load add an extra overhead.

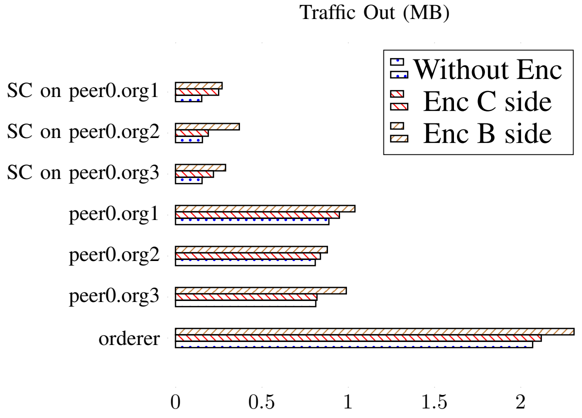

Fig. 20. Output network traffic (MB)

### D. Scalability

To assess the scalability of the proposed solution, the assessment of the scenario when there are multiple organizations or peers in the network is required. The first experiment assessed the impact of the number of peer endorsers on performance. Figures 21 and 22 plot the average latency and transaction throughput of different endorsing peers over different transaction send rates. For transaction latency, as shown in figure 21, the network with 4 endorsing peers has more latency than the network with 2 endorsing peers. But for the throughput in figure 22, the network with 2 endorsing peers has better throughput than the other network with 2 peers.

The second experiment assessed the impact of the number of organizations on performance. Figures 23 and 24 plot the average transaction latency and throughput of different organizations over different transaction sending rates. For transaction latency, as shown in figure 23, the network with more organizations generates more latency than the network with fewer organizations, and the variation in latency is huge. But for throughput as shown in figure 24, even it increased linearly with the increase of send rates. However, transaction throughput in the case of 3 organizations is better than the others, and increased modestly. This experiment indicates that increasing the number of organizations can decrease throughput and increase latency as the network becomes complicated.

The results of the scalability experiments indicate that the number of peer endorsers and organizations has a significant effect on performance. Increasing the number of peers and organizations can have better throughput, but it will increase latency as the volume of network traffic increase.

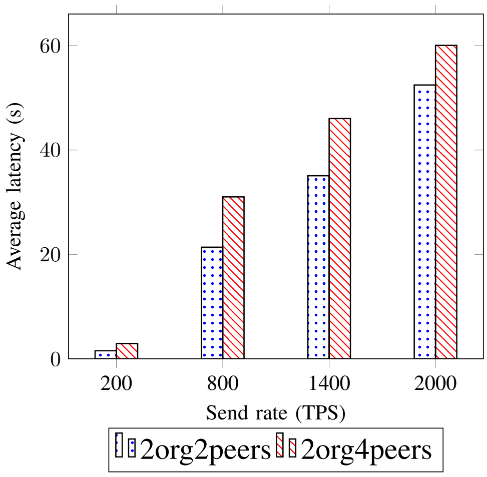

Fig. 21. Average latency with varying number of peers

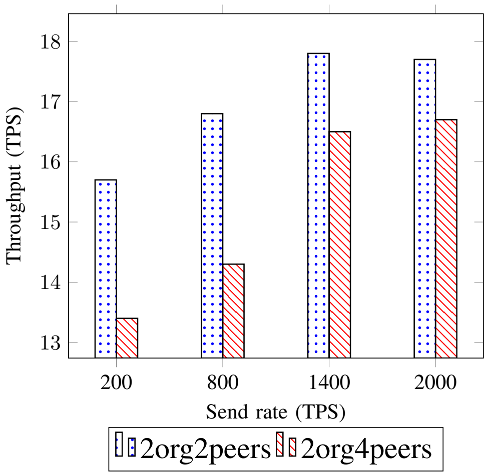

Fig. 22. Average throughput with varying number of peers

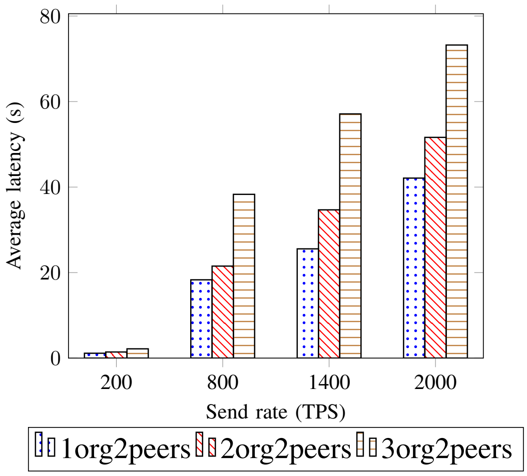

Fig. 23. Average latency with varying number of organizations

## VI. Results evaluation

Testing blockchain performance is a complicated exercise because several factors can affect the performance of the blockchain network. Especially for the case of our study where the proposed solution must operate in good standards in an environment with low resources, the case of developing countries. For that, a comprehensive assessment is studied to analyze every configurable network component that impacts blockchain performance.

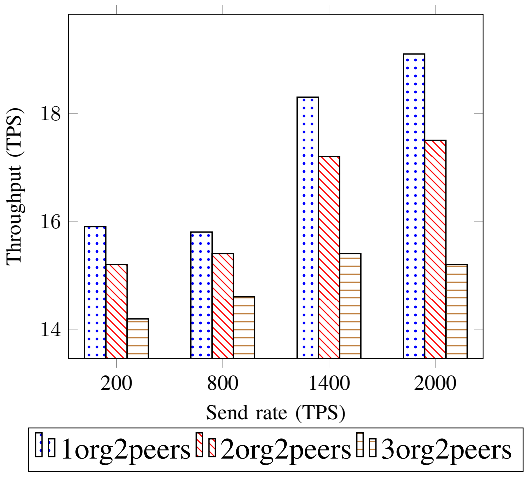

Fig. 24. Average throughput with varying number of organizations

Observing the results of the experiments, we find that for a solution based on the blockchain, several parameters can be optimized to obtain good results. Thus, the scalability of the system will not present a limit. In the case if resources are not a matter the solution can be deployed on cloud so that resources scale automatically as needed

Also, using encryption increase the data privacy and decrease the system performance, this degradation can be significant in production system with thousands of users and transactions. For limited budget organizations, encryption can be omitted.

It is observed that the basic network generates more transaction latency than the network with optimizations, transaction latency and transaction throughput increases linearly with increasing send rate in both cases but the network with one or several optimized parameters show better results than the basic network. These results clearly show that network performance using the optimized configuration can be significantly improved.

## VII. Conclusion

The objective of this study was to design an interoperable and secure information sharing system for health systems in developing countries based on blockchain technology.

The proposed system makes it possible to solve the problems of interoperability, confidentiality and integrity of patient data by offering an alternative or an annex to existing health systems, by offering strict and automatic management of access control.

To achieve this objective, these various works were carried out: an analysis of the challenges of existing electronic information systems and in particular for deployment in developing countries; a study of blockchain-based applications currently available for health information systems; a needs analysis for an application to be adapted to the environment of developing countries; development of a blockchain-based system for healthcare providers comprising the different actors of the healthcare system, including doctors, pharmacies and insurers; an immutable and tamper-proof system that provides secure data, with a reduced likelihood of cybercrime.

A comprehensive assessment is studied through a series of experimentation to analyze every configurable network component that impacts blockchain performance. The evaluation results showed that the proposed optimizations can significantly improve the performance of the blockchain solution.

## References

[1] T. Heart, O. Ben-Assuli, and I. Shabtai, "A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy," *Health Policy and Technology*, vol. 6, no. 1, pp. 20–25, Mar. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2211883716300624

[2] "Healthcare System Types: A Conceptual Framework for Comparison - Wendt - 2009 - Social Policy &amp; Administration - Wiley Online Library." [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-9515.2008.00647.x

[3] "EMR vs EHR – What is the Difference?" Jan. 2011. [Online]. Available: https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference

[4] F. White, "Primary health care and public health: foundations of universal health systems," *Medical Principles and Practice: International Journal of the Kuwait University, Health Science Centre*, vol. 24, no. 2, pp. 103–116, 2015.

[5] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, p. 102407, Feb. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212619306155

[6] T. E. P. A. T. C. O. T. E. UNION, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Apr. 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," *IEEE Access*, vol. 5, pp. 14 757–14 767, 2017, conference Name: IEEE Access.

[8] A. Roehrs, "OmniPHR : a Blockchain based interoperable architecture for personal health records," Aug. 2019, accepted: 2019-10-04T16:43:32Z Publisher: Universidade do Vale do Rio dos Sinos. [Online]. Available: http://www.repositorio.jesuita.org.br/handle/UNISINOS/8867

[9] S. I. Khan and A. S. L. Hoque, "Privacy and security problems of national health data warehouse: a convenient solution for developing countries," in *2016 International Conference on Networking Systems and Security (NSysS)*, Jan. 2016, pp. 1–6.

[10] N. Tariq, A. Qamar, M. Asim, and F. A. Khan, "Blockchain and Smart Healthcare Security: A Survey," *Procedia Computer Science*, vol. 175, pp. 615–620, Jan. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920317890

[11] M. Talal, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, M. A. Alsalem, C. K. Lim, K. L. Tan, W. L. Shir, and K. I. Mohammed, "Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors: Multi-driven Systematic Review," *Journal of Medical Systems*, vol. 43, no. 3, p. 42, Jan. 2019. [Online]. Available: https://doi.org/10.1007/s10916-019-1158-z

[12] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight Three-Factor Authentication, Access Control and Ownership Transfer Scheme for E-Health Systems in IoT," *Future Generation Computer Systems*, vol. 96, pp. 410–424, Jul. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X18331297

[13] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Information Quarterly*, vol. 34, no. 3, pp. 355–364, Sep. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0740624X17303155

[14] H. Zhao, Y. Zhang, Y. Peng, and R. Xu, "Lightweight backup and efficient recovery scheme for health blockchain keys," in *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*. IEEE, 2017, pp. 229–234.

[15] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in *2016 2nd International Conference on Open and Big Data (OBD)*, Aug. 2016, pp. 25–30.

[16] F. F. Ozair, N. Jamshed, A. Sharma, and P. Aggarwal, "Ethical issues in electronic health records: A general overview," *Perspectives in Clinical Research*, vol. 6, no. 2, pp. 73–76, 2015. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4394583/

[17] "About Health Level Seven International | HL7 International." [Online]. Available: http://www.hl7.org/about/index.cfm?

[18] "Health Information Privacy," Aug. 2015, last Modified: 2021-04-06T17:50-04:00. [Online]. Available: https://www.hhs.gov/hipaa/index.html

[19] N. Faruk, N. T. Surajudeen-Bakinde, A. Abdulkarim, A. A. Oloyede, L. Olawoyin, O. W. Bello, S. I. Popoola, and T. O. C. Edoh, "Rural Healthcare Delivery in Sub-Saharan Africa: An ICT-Driven Approach," *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, vol. 15, no. 3, pp. 1–21, Jul. 2020, publisher: IGI Global. [Online]. Available: www.igi-global.com/article/rural-healthcare-delivery-in-sub-saharan-africa/251830

[20] "Towards Implementing a Nationwide Electronic Health Record System in Nigeria: Medicine & Healthcare Journal Article | IGI Global." [Online]. Available: https://www.igi-global.com/article/towards-implementing-nationwide-electronic-health/54730

[21] M. O. Akanbi, A. N. Ocheke, P. A. Agaba, C. A. Daniyam, E. I. Agaba, E. N. Okeke, and C. O. Ukoli, "Use of Electronic Health Records in sub-Saharan Africa: Progress and challenges," *Journal of medicine in the tropics*, vol. 14, no. 1, pp. 1–6, 2012. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4167769/

[22] A. R. Ahlan and B. I. Ahmad, "User Acceptance of Health Information Technology (HIT) in Developing Countries: A Conceptual Model," *Procedia Technology*, vol. 16, pp. 1287–1296, Jan. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212017314003727

[23] R. Ssembatya, A. Kayem, and G. Marsden, "On the challenge of adopting standard EHR systems in developing countries," in *Proceedings of the 3rd ACM Symposium on Computing for Development*, ser. ACM DEV '13. New York, NY, USA: Association for Computing Machinery, Jan. 2013, pp. 1–2. [Online]. Available: https://doi.org/10.1145/2442882.2442911

[24] T. Suzuki, J. Hotta, T. Kuwabara, H. Yamashina, T. Ishikawa, Y. Tani, and K. Ogasawara, "Possibility of introducing telemedicine services in Asian and African countries," *Health Policy and Technology*, vol. 9, no. 1, pp. 13–22, Mar. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221188372030006X

[25] F. F. Odekunle, S. Srinivasan, and R. O. Odekunle, "Why Sub-Saharan Africa Lags in Electronic Health Record (EHR) Adoption and Possible Strategies to Increase EHR Adoption in this Region," *Journal of Health Informatics in Africa*, vol. 5, no. 1, pp. 8–15, Nov. 2018, number: 1. [Online]. Available: https://www.jhia-online.org/index.php/jhia/article/view/147

[26] A. Sandford, "Coronavirus: Half of humanity on lockdown in 90 countries," Apr. 2020, section: news_news. [Online]. Available: https://www.euronews.com/2020/04/02/coronavirus-in-europe-spain-s-death-toll-hits-10-000-after/ -record-950-new-deaths-in-24-hou

[27] M. B. Tahir and A. Masood, "The COVID-19 Outbreak: Other Parallel Problems," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3572258, Apr. 2020. [Online]. Available: https://papers.ssrn.com/abstract=3572258

[28] S. Bahl, R. P. Singh, M. Javaid, I. H. Khan, R. Vaishya, and R. Suman, "Telemedicine Technologies for Confronting COVID-19 Pandemic: A Review," *Journal of Industrial Integration and Management*, vol. 05, no. 04, pp. 547–561, Sep. 2020, publisher: World Scientific Publishing Co. [Online]. Available: https://www.worldscientific.com/doi/abs/10.1142/S2424862220300057

[29] "Leave no one behind: Strengthening health systems for UHC and the SDGs in Africa." [Online]. Available: https://www.afro.who.int/publications/leave-no-one-behind-strengthening-health-systems-uhc-and-sdgs-africa

[30] M. K. Domapielle, "Adopting localised health financing models for universal health coverage in low and middle-income countries: Lessons from the national health insurance scheme in ghana," *Heliyon*, p. e07220, 2021.

[31] H. J. AlMossawi, N. Kak, Y. Pillay, R. Matji, and S. Joshi, "Universal health coverage-inclusion of tb in national health insurance programs and recommendations for expansion of coverage of tb services in lmics," *Journal of Lung Health and Diseases*, vol. 3, no. 3, 2019.

[32] A. Rghioui, "Managing Patient Medical Record using Blockchain in Developing Countries: Challenges and Security Issues," in *2020 IEEE International conference of Moroccan Geomatics (Morgeo)*, May 2020, pp. 1–6.

[33] Y. H. Ho, Z. Cheng, P. M. F. Ho, and H. Chan, "Mobile intercloud system with blockchain," in *Proceedings of the international Multi-Conference of engineers and computer scientists*, vol. 1, 2018.

[34] C. E. Ngubo, P. J. McBurney, and M. Dohler, “Blockchain, iot and sidechains,” in *Proceedings of The International Multiconference of Engineers and Computer Scientists*, 2019.

[35] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, Jun. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519300864

[36] PricewaterhouseCoopers, “Fighting counterfeit pharmaceuticals: New defenses for an underestimated - and growing - menace.” [Online]. Available: https://www.strategyand.pwc.com/gx/en/insights/2017/counterfeit-pharmaceuticals.html

[37] T. Heston, “A Case Study in Blockchain Healthcare Innovation,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3077455, Nov. 2017. [Online]. Available: https://papers.ssrn.com/abstract=3077455

[38] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” in *2016 2nd International Conference on Open and Big Data (OBD)*, Aug. 2016, pp. 25–30.

[39] “Medicalchain whitepaper,” Oct. 2017. [Online]. Available: https://medicalchain.com/en/whitepaper/

[40] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data,” *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, Jan. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2001037018300370

[41] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, “MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data,” in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, ser. Lecture Notes in Computer Science, G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, Eds. Cham: Springer International Publishing, 2017, pp. 534–543.

[42] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, “BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records,” in *2018 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.

[43] “SimplyVital Health.” [Online]. Available: https://www.f6s.com/simplyvitalhealth

[44] “Robomed a revolutionary medical blockchain project.” [Online]. Available: https://robomed.io/blog/robomed-a-revolutionary-medical-blockchain-project/

[45] V. Buterin *et al.*, “Ethereum white paper,” *GitHub repository*, vol. 1, pp. 22–23, 2013.

[46] G. Prisco, “The Blockchain for Healthcare: Gem Launches Gem Health Network...” Apr. 2016. [Online]. Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network/-with- philips-blockchain-lab-1461674938

[47] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain,” *IEEE Access*, vol. 5, pp. 14 757–14 767, 2017, conference Name: IEEE Access.

[48] “Healthureum.” [Online]. Available: http://142.93.209.31/

[49] A. Poston, “About hashed health.” [Online]. Available: https://hashedhealth.com/about/

[50] C. McFarlane, M. Beer, J. Brown, and N. Prendergast, “Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.0,” p. 19.

[51] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,” *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[52] C. Kombe, “A secure and interoperable blockchain-based information sharing system for healthcare providers in developing countries,” Ph.D. dissertation, NM-AIST, 2020.

[53] J. Mattke, C. Maier, A. Hund, and T. Weitzel, “How an Enterprise Blockchain Application in the U.S. Pharmaceuticals Supply Chain is Saving Lives.” 2019. [Online]. Available: https://aisel.aisnet.org/misqe/vol18/iss4/6