Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A BLOCKCHAIN FOR SECURE DATA STORING WITH MULTI CHAIN ON SMART HEALTHCARE SYSTEM

SYAFIQ MUHAMMAD[A], BENFANO SOEWITO[B]

[a,b] Computer Science Department, Binus Graduate Program - Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480

E-mail: syafiq.muhammad@binus.ac.id[a], benfano@binus.ac.id[b]

ABSTRACT

The development of the smart healthcare industry requires them to adapt to new technologies, because every year a lot of data is stolen or used by other parties, because the smart healthcare industry deals with very sensitive data that must be managed in a secure way. Electronic Health Records (EHRs) store various types of personal and sensitive data. there have been many surveys that prove the loss of data stolen and used by other parties. Therefore, we propose a new technology to be used in sensitive data storage in smart healthcare systems, namely blockchain. but we also apply another method in blockchain to store data that is with multi-channel. The advantage of blockchain also is that it provides transparency, security and privacy using consensus-based decentralized data management on top of a peer-to-peer distributed computing system. then the use of the multi-channel method can also make data storage possible with several channels at once where each channel has its own data. By proposing a blockchain technology and multi-channel method, we will experiment and evaluate the results of the experiment.

Keywords: *Blockchain, Smart Healthcare, Hyper Ledger, Multi-Channel,*

1. INTRODUCTION

The current healthcare system are mostly based on centralized servers where multiple entities within the network require permission to access the medical information [1]. This can cause delay in offering the medical services and also potential leakage of the information. One of the challenges with the current healthcare systems is the secure accessibility of the medical data by various entities within the hospital network [2]. However, sharing health data needs a secure and trusted infrastructure as there exists many risks related to privacy, security, and interoperability [3]. Blockchain can be utilized in these cases to achieve the secure accessibility and integrity of the healthcare data. In fact, blockchain as a decentralized and distributed technology can play a key role in providing such healthcare services [1]. Therefore, it is difficult to effectively integrate interoperability between health care systems, which are distributed in application. Because the integration between health care systems can speed up services, and can reduce the error rate in services such as drug administration because medical history. Healthcare organization are focused on their primary mission (i.e helping patients) while cyber security risks not considered [1]. Furthermore, many health care companies use of external third party vendors to manage and run their systems can pose a large number of risks. Instead of attacking large and well-funded organizations with advanced ones cyber capabilities first hand.

The technology of blockchain, with inherited characteristics such as decentralization, transparency and anonymization, was introduced in the cryptocurrency Bitcoin in 2008 (Nakamoto, 2008). According to IBM, 70 % of healthcare leaders predict that the greatest impact of blockchain within the health domain will be improvement of clinical trial management, regulatory compliance and

providing a decentralized framework for sharing electronic health records (EHR). Blockchain technology promises to provide immense opportunities in the healthcare sector such as secure data storing and sharing among various stakeholders, nationwide data interoperability and flexible and quick billing and payment modes [1]. We discuss blockchain in more detail in chapter 2 covering what blockchain is, how it works.

As reported by many practitioners, from 2005 to 2019, the total number of individuals affected by healthcare data breaches was 249.09 million [4]. The total number of healthcare records that were exposed, stolen, or illegally disclosed in the year 2019 was 41.2 million in 505 healthcare data breaches [4]. According to an IBM report, the average cost of a data breach in 2019 was $3.92 million, while a healthcare industry breach typically costs $6.45 million [4]. HIPAA and OCR reports also showed that hacking/IT incidents are the main cause behind healthcare data breaches [4]. The main types of attacks used to breach protected health data are Hacking/IT incidents, unauthorized access/ internal disclosure, Theft/loss, or Improper disposal [4]. In contrast, hacking/IT incidents and unauthorized internal disclosures have shown a marked increases, especially hacking incidents, which have increased very rapidly in frequency in last few years [4].

The health care sector is currently facing difficulties in meeting growing problems, costs, and stringent quality care arrangements. Of course, electronic medical records (EMR) and personal health records (PHR) are extremely sensitive and personally identifiable information (PII). Due to software vulnerabilities, security failures, and human error, these databases are sometimes accessed by unauthorized users. This leads to the exposure of sensitive data in the form of a data breach. Occasionally, insider attackers cause damage to protected health information, resulting in the loss, theft or disclosure of sensitive health care data.
Therefore, there are a lot of healthcare systems that must be explored and implemented, to improve the quality of our lives with technology. From these considerations, in this study we propose architecture the blockchain system for secure data storing on smart healthcare system for replace the database system and traditional paper. And every health institution that wants to access patient data must have permission access from the patient for secured from unauthorized users.

2. THEORY

2.1 Blockchain

Blockchain is an emerging trend in technology that is influencing the business and society. Blockchain technology has been successfully used in different fields, that includes financial services, public administration, supply chain management, healthcare and many more. A blockchain is a distributed database in which a linear collection of data elements called blocks are linked together to form a chain and these are secured by cryptographic primitives. Blocks records the sequence of transactions and the time when they were recorded in the blockchain. Each block contains the cryptographic hash that points to its previous block, timestamp, and transaction data. Blockchain can be described as an immutable ledger that logs data entries in a decentralized manner. It enables entities to interact without the presence of a central trusted third party. The blockchain maintains a continuously growing set of data entries, bundled together into blocks of data. These blocks are, upon acceptance to the blockchain linked to the previous and future blocks with cryptographic protocols [5]. In blockchain's original form, these data records/blocks are, readable by all, writable by all, and tamper proof by all. This for instance allows decentralized transactions and data management.

A key attribute of blockchain is decentralization. no central authority controls the content added to the blockchain. Instead, the entries passed on to the blockchain are agreed upon in a peer-to-peer network using a various consensus protocols. Blockchains make audit and traceability possible by linking a new block to the previous by including the hash of the latter, and in this way forming a chain of [5]. The transactions in the blocks are formed in a Merkle tree [6] where each leaf value (transaction) can be verified to the known root. This enables the tree structure to verify the integrity of the data by only storing the root of the tree on the blockchain figure 2.1.

Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

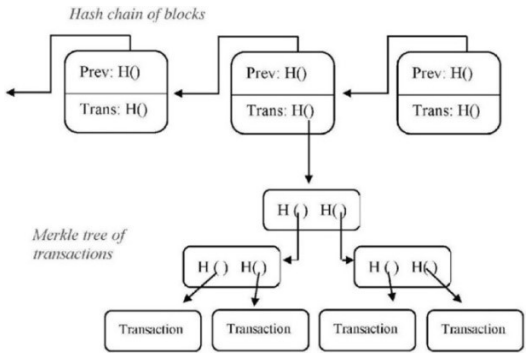

Figure 2.1 Blockchain Merkle Tree tree [6]

Same with Hasselgren, et al. [5] zhang, et al [7] describe the blockchain structure. Miners then compete in solving a computationally expensive cryptographic puzzle, known as "proof-of-work," where a targeted hash value associated with the last valid block in the chain is calculated. The first miner to solve this puzzle receives a reward (i.e., an amount of Bitcoin) and appends their block of validated transactions to the blockchain sequence [7] figure 2.2.

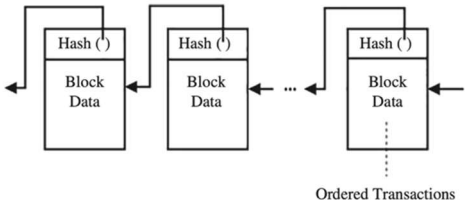

Figure 2.2 The Blockchain Structure: a Continuously Growing and Immutable List of Ordered and Validated Transactions. [7]

In illustrated table [7] there are mainly three types of blockchains: public (permissionless), consortium (public permissioned) and private, the detail can be seen in the Table 1.

Table 2.1 Type of blockchains overview [5]

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Public or restricted	Public or restricted
Immutability	Nearly impossible	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

They have different characteristics regarding who can access, write and read data on the blockchain. Data in the public chain is visible to all and anyone can join in and contribute to consensus and changes to core software. Public blockchain is widely used in cryptocurrencies, and the two largest cryptocurrencies: Bitcoin and Ethereum, are categorized as public chains without permission. A consortium blockchain can be considered partially centralized, with only a select group of entities having access to view and participate in the consensus protocol. In a private blockchain, the network is distributed but often centralized.

2.2 Smart Contract

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

2.3 Smart Healthcare

Smart healthcare was born out of the concept of "Smart Planet" proposed by IBM (Armonk, NY, USA) in 2009 [11]. Smart healthcare is a health service system thatuses technology such as wearable devices, IoT, and mobile internet to dynamically access information, connect people, materials and institutions related to healthcare, and then actively manages and responds to medicalecosystem needs in an intelligent manner [11]. Smart health care also often contains information such as EMR, EHR, and PHR. Electronic medical records (EMR) are digital versions of paper charts in doctor's offices, clinics, and hospitals. EMR contains records and information collected by and for doctors in that office, clinic or hospital and is mostly used by service providers for diagnosis and treatment. Electronic health records (EHR) do all those things and more. EHRs focus on the total health of the patient going beyond standard clinical data collected in the provider's office and inclusive of a broader view on a patient's care [12]. Personal health records (PHRs) contain the same types of information as EHRs diagnoses, medications, immunizations, family medical histories, and provider contact information but are designed to be set up, accessed, and managed by patients. Patients can use PHRs to maintain and manage their health information in a private, secure, and confidential environment [12].

Smart healthcare consists of multiple participants, such as doctors and patients, hospitals, and research institutions [11]. Its an organic whole that involves multiple dimensions, including disease prevention and monitoring, diagnosis and treatment, hospital management, health decision-making, and medical research. Information technologies, for example, IoT, mobile Internet, cloud computing, big data, 5G, microelectronics,and artificial intelligence, together with modern biotechnology constitutethe cornerstone of smart healthcare [11]. From the perspective of patients, they can use wearable devices to monitor their health at all times, seek medical assistance through virtual assistants, and use remote homes to implement remote services; from the perspective of doctors, a variety of intelligent clinical decision support systems are used to assist and improve diagnosis [11].

2.4 Hyperledger

Hyper Ledger Fabric is an open source enterprise-grade permissioned open-source distributed ledger technology (DLT) platform, maintained by IBM and Linux Foundation, designed for use in enterprise contexts [13]. Has a highly modular and configurable architecture, enabling innovation, versatility and optimization for a broad range of industry use cases including, as the purpose of this article, healthcare [13]. Fabric is the first distributed ledger platform to support smart contracts authored in general-purpose programming languages such as Java, Go and Node.js, rather than constrained domain-specific languages (DSL) [13].

Fabric can leverage consensus protocols that do not require a native cryptocurrency to incent costly mining or to fuel smart contract execution [13]. The absence of cryptographic mining operations means that the platform can be deployed with roughly the same operational cost as any other distributed system [13]. Hyperledger Fabric CA, is the default Certificate Authority component, which issues PKI-based certificates to network member organizations and their users. The CA issues one root certificate to each member and one enrolment certificate to each authorized user [13].

Consensus implies a process in which the members of a blockchain network agrees whether a transaction is valid or not and to keep consistency in ledger synchronization, lowering the risk of malicious transactions [13]. HLF presents a pluggable consensus approach. The ordering of transactions is delegated to a modular component (ordering service) for consensus that is logically decoupled from the peers that execute transactions and maintain the ledger [13]. Since consensus is modular, its implementation can be tailored to the trust assumption of a particular deployment or solution [13]. The modular architecture presented by HLF allows the platform to rely on well-established toolkits for CFT (crash fault-tolerant) or BFT (byzantine fault-tolerant) ordering and can have

multiple ordering services supporting different applications or application requirements [13].

In Hyperledger Fabric, a ledger consists of two distinct, though related, parts a world state and a blockchain [14]. Each of these represents a set of facts about a set of business objects [14].

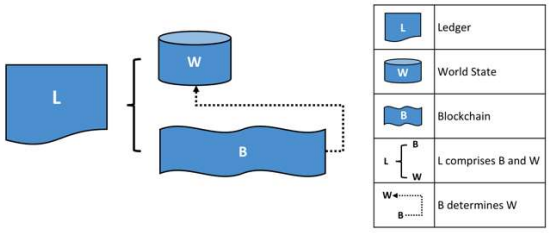

Figure 2.3 The Ledger on Hyperledger Fabric [14].

In figure 2.4 we can see the Ledger L comprises blockchain B and world state W, where blockchain B determines world state W [14]. We can also say that world state W is derived from blockchain B [14].

Firstly, there's a world state a database that holds current values of a set of ledger states [14]. The world state makes it easy for a program to directly access the current value of a state rather than having to calculate it by traversing the entire transaction log [14]. Secondly, there's a blockchain – a transaction log that records all the changes that have resulted in the current the world state [14]. Transactions are collected inside blocks that are appended to the blockchain – enabling you to understand the history of changes that have resulted in the current world state [14].

Some unique features of relative Hyperledger fabric to blockchain framework technologies are:

1. It provides permissions and a modular architecture to execute different transactions in a peer-to-peer blockchain network.
2. A flexible and installable support model helps achieve and reach consensus among stakeholders in the network.
3. Provide mechanisms that support the privacy and integrity of transactions using channels.
4. This allows us to create channels between separate member organizations to communicate achieve the notion of privacy and confidentiality.
5. Transaction processing has less latency compared to other blockchain platforms.
6. Smart contracts can be written in multiple languages such as Go, Java, JavaScript.
7. Supports various types of queries such as keyed queries, range queries, and JSON on chain queries.
8. It provides continuous organizational operations, such as rolling improvement and asymmetrical rolling enhancement version support.

3. RELATED WORKS

Luca Brunese, et al [15] in his journal, proposed to protect the MRI data which is the image stored on the blockchain using the Formal method, and that formal method will verify the MRI data. In recent few years, many authors have explored the idea of using blockchain in a healthcare context. Blockchain technology can help mitigate challenges of current electronic medical records solutions and can create value for treatment process and remote access of patients' medical information and ensuring the protection of healthcare data privacy [16]. Usman and Qamar [16] proposed the use of blockchain with Hyperledger compared to Ethereum because patients medical information are of highly sensitive nature. and All peers that takes part in the consensus mechanism runs a consensus algorithm (Hyperledger use PBFT consensus algorithm) to check whether a transaction is valid or not [16]. different from Usman and Omar, Zhang, et al [7], they prefer to use the Token-Based Permission Model. According to Zheng, the use of smart contracts is less effective [7], because there will be a new contract renewal and must be deployed, and it will cause the system to experience delays in service. But not all have to use a hyper ledger on a blockchain, if there is no sensitive personal information or information, the public blockchain with the smart contract will help acquire digital support, which is often called CALS (Continuous Acquisition and Lifecycle Support), which is a means of supporting sustainable information. for supply throughout the product life cycle. PLM (Product Lifecycle Management) is a product life cycle management technology which is an organizational and technical system that provides the management of all information about a product

and related processes throughout its life cycle, from research and production to decommissioning [17]. in this case healthcare system is very helpful in all aspects such as.

Badr, et al [18] in his journal, propose a novel protocol to achieve a perfect privacy preserving for the patient namely Pseudonym Based Encryption with Different Authorities (PBE-DA) by applying the concept of Blockchain on the healthcare communication entities in an e-health platform [18]. In PBE-DA, the logic for key generation and authentication is moved from the Internet of things (IoT) nodes to the corresponding gateway (GW), thus relieving the IoT device from the computational burden associated with the generation of cryptographic data [18]. PBE-DA will be used to create a patient virtual identity that could help in preventing the reverse of access chain in the EHRs environment through hiding the main patient identity from cloud providers [18]. The first level in its architecture is considered to be the Fog layer or access to connect patients with their IoT devices via its gateway system. At the second level, we analysed the communication or distribution of the ledger among EHR members.

IoT includes two concepts: "Internet" and "Thing", where "Internet" refers to "The world-wide network of interconnected computer networks", based on a standard communication protocol, while "Thing" refers to "an object not precisely identifiable" [19]. Smart healthcare is a health service system that uses technology such as wearable devices, IoT, and mobile internet to dynamically access information, connect people, materials and institutions related to healthcare, and then actively manages and responds to medical ecosystem needs in an intelligent manner [20]. Therefore, the reach of the ideas presented here regarding wearable healthcare devices and using blockchain technology are further reaching than we show or can imagine here [21]. Dwivedi, Srivastava, Dhar, & Singh in his journal they proposed using smart contracts with platform bitcoin and they use double encryption of data using lightweight encryption algorithms (ARX ciphers) and public encryption schemes. ARX is a class of cryptographic algorithms which uses three simple arithmetic operations: namely modular addition, bitwise rotation, and exclusive-OR. In both industry and academia, ARX cipher has gained a lot of interest and attention in the last few years [21]. These algorithms are made of simple operations Addition, Rotation and XOR and support a lightweight encryption for small devices [21].

Yang, et al [22] in his journal proposed an off-the-chain consortium blockchain scheme for collaborative medical decision-making that includes the security of blockchain and privacy of personal data [22]. PoF ensures the integrity of a collective medical decision and privacy of stakeholders by storing previously stored decisions and identities by blockchain [22]. While preserving the identity of stakeholders, PoF follows a two-layer security measure. Firstly, the identities of patients, doctors, cured patients, and insurance companies are locally stored, and secondly, the hash of those are stored in a block [22].Sharing of medical data in the present day is observed to be slow, incomplete, insecure, and provider-centric. These barriers prevent the interoperability of data and are a consequence of the lack of foundational, structural, and semantic inoperability [23]. Lack of trust among healthcare providers, concerns regarding the privacy protection of the shared data, and concerns regarding the scalability of large datasets have restricted the use of mobile technology in the field of medical data exchange [23]. Concerns of data privacy on the blockchain can be addressed with the help of proxy patterns, which can improve the interoperability while maintaining patient privacy [23]. Scalability of healthcare data can be maintained with the help of system patterns such as the publisher-subscriber pattern, which can detect changes in the relevant data sets [23]. By applying blockchain technologies with appropriate markers, the safety of the patient data can be ensured during the transmission of data [23].

In this context you can see what has been done [18] and [22] in developing the blockchain system is very strong, because they solve problems that can be covered by blockchain like privacy, integrity and authorization. Meanwhile, what is done by [16] is about sharing EMR data storing, and regarding patient data access control, patients have

full control of their medical records, as they can decide who can add new medical records and can view their previous medical records. Meanwhile, what is being done [21] focuses on blockchain-based IoT with security and privacy model.

4. RESEARCH METHODOLOGY

In this study, there are stages of research as shown in Figure 3, which will focus on how to make data secure using blockchain with multi-channel that focus on patient, hospital, financial insurance and not focus on medical lab, and pharmacist. Traditional smart health care systems rely largely on outdated methods for storing, maintaining, and protecting patient data which can limit collaboration opportunities among health care providers and participants. This increases the cost of the system which can greatly affect the effectiveness of patient care. However, a lack of awareness, technological immaturity, and unavailability of security and privacy standards prevent smart healthcare participants from unlocking the full potential of blockchain technology. Technological advances on the Internet of Things (IoT) can help the smart health care sector to remotely monitor patient health through precise biomedical sensors. Biomedical sensors can continuously monitor and store health data on high-performance edge servers that help analyze a patient's health condition. Health data can be linked to vital indicators, such as diagnose and symptoms. However, inaccurate data captured via a malfunctioning device can lead to medical errors. To solve this problem satisfactorily, decentralized blockchain technology uses smart contracts to register and verify biomedical sensor permissions to store EHR in the ledger.

In recent years, the development of smart healthcare with blockchain has focused on its architecture such as security threats, data integrity, interoperability, access control the Smart Healthcare system architecture that I created is a blockchain consortium which is jointly managed by related institutions such as the governance, hospitals, financial institutions. This requires related institutions to cooperate in policy making and be supervised by the government. Making a blockchain ecosystem for healthcare must be gradual, in the first stage starting with hospitals that work together, of course assisted by experts in its implementation, because today's health institutions have problems implementing a proper health care system architecture. the hospital will be assisted and supervised by the government in making its policy, in the second stage starting from financial institutions such as finance institutions. In creating the ecosystem, the same architectural standards are made for each node. In the fabric architecture, a permissioned consortium blockchain network is created in which all participating healthcare stakeholders and their end users are identified and registered by health authorities use membership services component using certificate issuing authority.

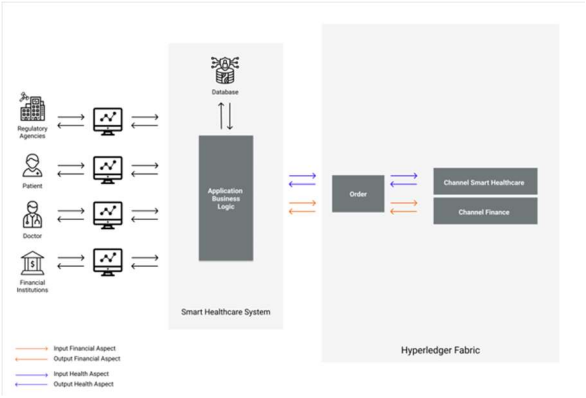

Figure 3.4 Proposed architecture hospital and financial institutions

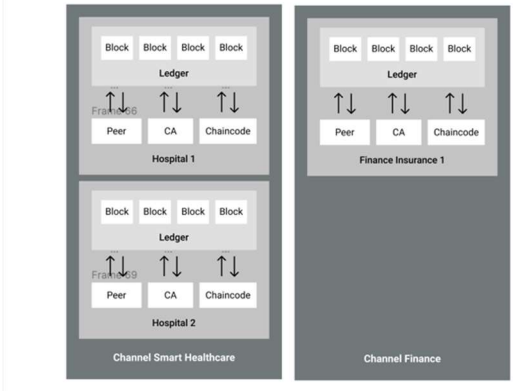

Figure 3.5 Proposed architecture governance

In figure 3.2 it can be seen that the image describes each system in hospitals and financial

institutions the same and its ability to only create and view data on the smart healthcare system, of course with the patient's permission. Figure 3.2 explains that the architect governance smart healthcare system has differences, where there is a feature to add users with the roles of patients, doctors and people in financial institutions, of course, this is under the supervision of the regulatory agencies team. in the governance smart healthcare system there is a notification feature for requests for access rights to view patient data, and patients can agree or reject it.

In cloud computing there are several parts of the application business logic which to set would be the custom rules or algorithms that handle the exchange of information between a system and user interface, the business logic application will also receive data from the internet first before being forwarded to another service, business logic application will manage the response to the web application with some predetermined standards and will facilitate communication between the two. business logic application can be divided into several microservices so that the division of tasks is based on business functionality, the division of modules is based on business functionality. Application business logic is also integrated into a regular database that stores data for application needs such as sessions time or static data such as provinces, cities, districts.

As we are using permissioned blockchain all the users must be registered before being given access to the system with the hyperlegder fabrics. Why use hyperlegder fabrics have promising future in blockchain framework, Hyperledger can also implement multi-chain code which has multiple blockchains in one system. Example in figure 8 doctor will input symptoms, diagnosis, treatment and medicine the pasiens with specific ID. With helper from channels features the Hyperledger can added data on multiple blockchain. Channels are the state store of an blockchain network which hold the application data generated during the lifecycle of the system. It's used to store information like patients data, financial data and more. In a hyeperledger fabric network there can be multiple channels to provide privacy and security to the parties involved. Channel configuration is managed by the configtx.yaml file. Using this file we generate a channel.tx file and then create channels using it. The chain code is installed on all peers participating in the channel, while the chain code is deployed on the channel. Channel contains all communication configurations between peers.

System Admin, which in our platform is health administration, will register the users of the system. When a user gets registered in the blockchain network he/she is provided with login credentials i.e. User ID and Secret key which he/she can use to login to the system. The client application generates a symmetrical pair of private / public keys and patient keys and assigns them to the patient. Patients can now use this identification material to enter the system. The Healthcare Provider process flow will also be the same as for the patient. Healthcare Providers will be given an ID and private key to gain access to the system. Sign the Healthcare Provider into the system and start examining the patient. He can add new medical records for patients and can view previous medical records only after he has received permission from the patient. Healthcare providers can also send requests for authorization to patients to gain access to their medical records. Once allowed by the patient, he or she can view the previous records and add new notes for that patient.

Patients can view their medical records by logging into the system using their login credentials. Patients have full control over their medical records, because they can decide who can add new medical records and can view previous medical records. They can authorize Healthcare Providers to allow them to view their medical records and add new records. A fabric network can have multiple channels. Channels allow organizations to use the same network while maintaining segregation between multiple blockchains. Only channel members (peers) are allowed to view transactions made by any member in the channel. In other words, the channel partitions the network to allow visibility of transactions only to stakeholders. Only channel members engage in consensus, while other network members see no transactions in the channel. Peers can maintain multiple ledgers. And colleagues can connect to multiple channels.

Channel configuration is managed by the configtx.yaml file. Using this file we generate a channel.tx file and then create channels using it. The chain code is installed on all peers participating in the channel, while the chain code is deployed on the channel. The channel contains all the communication configurations between peers. It holds a list of peers along with who supports, anchors, co-leaders. When a client communicates with the network using the SDK, the SDK first gets a list of all the support partners to which transaction requests should be sent. Using this list, the SDK sends a transaction request to the peer. Peers participating in multiple channels simulate and make transactions to different ledgers. The subscriber is also part of the channel.

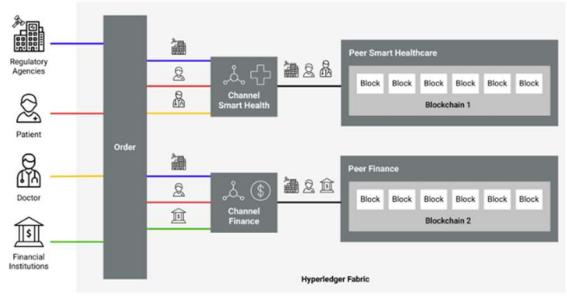

Figure 3.4 Access data on blockchain

In Figure 3.4 we can see access and connection to the blockchain which has 2 channels: health and financial with this division defined in the hyperledger fabric, with this it can handle data stolen by unauthorized access/internal disclosure.

5. Implementation

5.1 Prerequisites

Before getting started, it may be necessary to check if you have installed all the Prerequisites on the platform on which you will be developing blockchain applications and/or operating them. The system should have installed tool such as docker, docker-compose, node, npm, golang, curl and angular cli. Please follow the detailed steps on the official website of each tool. After all the tools are installed, then install hyperledger fabric by executing the command below:

curl -sSL https://bit.ly/2ysbOFE | bash -s

This command will download the initial hyperledger fabric project, and several docker images such as fabric-baseos, fabric-ca, fabric-ccenv, fabric-orderer, fabric-peer, fabric-tools. The command will also download the platform-specific binaries you need to set up your network and place them in the clone repo you created above. It fetches the following platform-specific binaries: configtxgen, configtxlator, cryptogen, discover, idemixgen order, peers, fabric-ca-client, fabric-ca-server. The binaries that will be executed to run the hyperledger fabric. After all completed please setup the terminal environment for add PATH environment variable for each binary. E.g:

export PATH=<path to download location>/bin:$PATH

5. 2 Design Network

The first thing to understand is to identify what we are going to create, in this case we will create three organizations (Org1, Org2, and Org 3), and one peer on each organization. Org1 will act as Hospital 1, Org2 will act as Hospital 2 and Org3 will act as Financial Institution 1. Two channels are established (Channel Smart Health and Channel Finance), such that Channel Smart Health is for Org1, and Org2, and Channel Finance is only for Org3, we can see on figure 3.5.

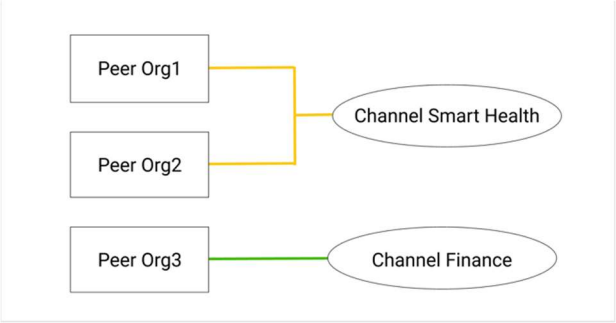

Figure 3.5 Design Network

5.3 Configuration Network

The configuration artifact consisting of asset transaction which consists of application and chain code. This application is used as a bridge between application business logic and chain code, both of which can be written in Java, JavaScript and Golang. Then after the asset transactions, we also have to

create a network artifact which usually consists of configtx.yaml, docker-compose which we will use, crypto-config.yaml and a shell script that is used as a deployment. For configtx.yaml. There are several steps that must be considered:

1) In configtx.yaml there are several important points to note on the variable "Organization" which must be defined Org1, Org2, Org3. Another thing to pay attention to is the "Profile" variable where you have to define "ChannelSmartHealth", "ChannelFinance", and set Organizations on each channel namely ChannelSmartHealth for Org1, Org2 and ChannelFinance for Org3.
2) In cryptogen.yaml we can define OrderOrgs and PeerOrgs for each organization.

5.4 Setup Docker Compose

Hyperledger fabric in release 2.3 uses docker in its virtual machine setup, there are a few things to be aware of in setup:

1) Create Image hyperledger/fabric-order
2) Create Image hyperledger/fabric-peer for each organization
3) Create image hyperledger/fabric-ca for each organization and order
4) Create image hyperledger/fabric-tools
5) Create image couchdb will depens_on on image each organization

5.5 Setup Shell Script for Deployment

Shell script is used for several commands that are executed in the order we want, there are some that we must pay attention to in the order of execution in running Hyperledger in shell script:

1) cryptogen generate --config=# crypto-config.yaml --output="organizations". The cryptogen will generate each organization and 1 order.
2) After creating key we must be register key on fabric-ca-client. With comand “fabric-ca-client register --caname --id.name #namepeer --id.secret #nameSecret --id.type peer --tls.certfiles #root certificate file”
3) docker-compose ${COMPOSE_FILES} up. For the image we want to build.
4) After build up image on ca we can excute configtxgen -profile for each channel. In this step generate initial container tx and block for each channel.
5) After execute configtxgen, we must be execute “peer channel join” for making peer joining to channel.
6) After the peer joins the channel, we have to apply the lifecycle chaincode with the “peer lifecycle chaincode” command. In the chaincode lifecycle there are things that must be considered in order: install, queryinstalled, approvalformyorg, checkcommitreadines, commit and querycommitted, make sure all organizations agree on the initial chaincode to be implemented.
7) After to apply the lifecycle chaincode, we have optional execution for invoke chaincode using initial data, with command “peer chaincode invoke -o --isInit”, in this command we must define certificate file.
8) After all completed we can query, or submit transaction with application asset.

5.6 Application Asset & Smart Contract (Chain code)

In Hyperledger we modify a smart contract defines the executable logic that generates new facts that are added to the ledger. Both smart contract and ledger heart hyperledger fabric blockchain system. In application asset we can write with Java, JavaScript and Golang for connect to specific network resources. And Smart Contract we can use to create business model on ledger or blockchain. In this case we must be create 4 contracts i.e.: doctor-contract, patient-contract, admin-contract, finance-contract. Where each role will have different privileges.

5.8 Backend and Web Application

In backend and web app I use node js with express and angular for web app. And make sure in application assets we use javascript or node to create bridge between backend and Hyperledger. On the node we can join the Hyperledger network with the fabric-network library and deploy ca with the fabric-ca-client library. In the backend we have to define the flexibility of which channel we will connect. For

deployment we can use command "npm start" for node and "ng serve" for web application.

5.9 Data Collection

Data collection in this study was carried out by discussing the architecture and model of the recommendation system as well as application design with an object-oriented design approach in this case using UML with Sequence Diagrams. In figures 3.2 we can see the microservice blockchain where the microservice blockchain as a system that has the logic to pass data and determine what functions will be called in the hyperlegder fabric. In figures 3.2 there are also orange and blue arrows which represent the flow of financial and health data which are separate functions, it is the hyperlegder that determines which blockchain will be stored. In figure 4.1 we can seen application bussines logic handled all request and part of logic. In Figure 4.1 we can see that the business logic of the application handles all requests from web. Also part of the logic of the smart healthcare system and the microservice blockchain has state logic to call specific functions on the hyperledger to store data on the blockchain, figure 4.1 we can see the data storage on blockchain. The initial data in this experiment is in the form of a dummy. with the initial data, the system will implement role-based data access control, then there will be initial data testing where doctors and brokers will access patient data, and the expectation is that the data stored for the smart health channel will not be seen by the broker, and the data stored for channel finance is not seen by the doctor.

Patient
patientId
firstName
lastName
age
phoneNumber
emergancyContact
address
bloodType
allergies
diagnosis
symptoms
treatment
followUp
permissionGranted
modifyBy
password

Finance
patientId
firstName
lastName
age
phoneNumber
emergancyContact
address
bloodType
diagnosis
symptoms
treatment
insurenceType
totalClaim
permissionGranted
modifyBy
password

Figure 3.6 Data patients

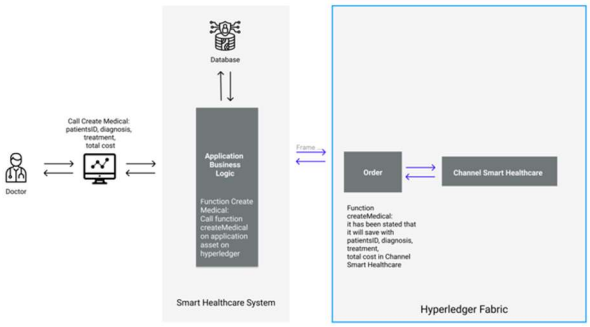

Figure 3.7 Workflow create data patients in channel healthcare

In the process of multi-channel, business logic can be separated, and in this case, I separate 2 institutions: finance and health, from this application bussines logic, blockchain microservices and hyperledger have specific functions for both input and output. In Figures 3.7 it can be seen that each action of the user role doctor and financial institution has a separate function

6. CONCLUSION

In this paper, we propose an architecture with a multi-channel blockchain, why do we propose this architecture? because the smart health care system

will have two channels, where the channel has its own data, and the hyperledger fabric with multi-channel has more optimal multi-channel data security with certificate authority services where each peer or node has a certificate authority that will only recognize the specified channel, and that's not all hyperledger also has a smart contract that will adapt the desired business model which makes managing data control more secure. therefore it is appropriate to build a multi-channel business model in terms of Smart Healthcare and finance which will be secure control of EHR, EMR or PHR data.

The use of Hyperledger Fabric to create a blockchain with multi-channel is the right thing because Hyperledger can be configured architecture to match the desired business model. while hyperledger fabric is growing very fast in its features, one of which can be configured with multi-channel, and hyperledger is also very welcome with virtual machine technology such as docker which makes its dynamic configuration. The hyperledger fabric configuration supports certificate authorities to create access controls for their respective channels, which will store sensitive data such as EHR, EMR or PHR.

REFERENCES

[1] Brunese, Luca; Mercaldo, Francesco; Reginelli, Alfonso; Santone, Antonella, "A Blockchain Based Proposal for Protecting Healthcare Systems through Formal Methods," 2019.

[2] F. Amato, G. De Pietro, M. Esposito and N. Mazzocca, "An integrated framework for securing semi-structured health records," 2015.

[3] N. Tariq, A. Qamar, M. Asim and F. A. Khan *Blockchain and Smart Healthcare Security: A Survey,* 2020.

[4] A. H. Seh, . Zarour, . Alenezi, . K. Sarkar, Agrawal, R. Kumar and . A. Khan, "Healthcare Data Breaches: Insights and Implications," 2020.

[5] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review".

[6] R. C. Merkle., "A Certified Digital Signature. Conference on the Theory and Applications o Cryptology," Springer, 1989.

[7] P. Zhang, J. White, D. C, Schmidt, G. Lenz and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," 2018.

[8] M. Richards and N. Ford, Fundamentals of Software Architecture, O'Reilly Media, Inc., 2020.

[9] Y. Wang, "Modular Design," 2018.

[10] K. Clark and C. Y. Baldwin, "The Option Value of Modularity in Design: An Example from Design Rules, Volume 1: The Power of Modularity," 2002.

[11] S. Tian, W. Yang, J. M. L. Grange, P. Wang, W. Huang and Z. Ye, *Smart healthcare: making medical care more intelligent,* 2019.

[12] HealthIT.gov, "Health IT Buzz," 2 May 2019 [Online]. Available: https://www.healthit.gov/faq/what-are-differences-between-electronic-medical-records-electronic-health-records-and-personal.

[13] T. Guimarães, A. Moreiraa, H. Peixotoa and M. Santos, "ICU Data Management - A Permissioned Blockchain Approach," 2020.

[14] Hyperledger Fabric, "hyperledger fabric," 22 June 2021. [Online]. Available: https://hyperledger-fabric.readthedocs.io/.

[15] L. Brunese, F. Mercaldo, A. Reginelli and A. Santone, *A Blockchain Based Proposal for Protecting Healthcare Systems through Formal Methods,* 2019.

[16] M. Usman and U. Qamar, *Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology ,* 2020.

[17] K. K.A, K. G.S, R. I.V and K. P.B, *Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation ,* 2018.

[18] S. Badr, I. Gomaa and E. Abd-Elrahman, "Multi-tier Blockchain Framework for IoT-EHRs Systems," 2018.

[19] U. -. K. S. Agency, in *Internet of things in 2020*, 2010.

[20] S. Tian, W. Yang, J. M. L. Grange, P. Wang, W. Huang and Z. Ye, "Smart healthcare: making medical care more intelligent," 2019.

[21] Dwivedi, Ashutosh Dhar; Srivastava, Gautam Dhar, Shalini; Singh, Rajani, *A Decentralized*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Privacy-Preserving Healthcare Blockchain for IoT, 2019.

[22] Yang, Jinhong; Onik, Md Mehedi Hassan; Lee, Nam-Yong; Ahmed, Mohiuddin; Kim, Chul-Soo, *Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making,* 2019.

[23] Clim, Antonio; Zota, Răzvan Daniel; Constantinescu, Radu, *Data exchanges based on blockchain in m-Health applications,* 201

[24] Hasselgren, Anton; Kralevska, Katina; Gligoroski, Danilo; Pedersen, Sindre A.; Faxvaag, Arild, "Blockchain in healthcare an health sciences—A scoping review," 2020.

[25] Clark, Kim; Baldwin, Carliss Y, "The Option Value of Modularity in Design: An Example from Design Rules, Volume 1: The Power of Modularity," 2002.

[26] Mitchell M. Tseng; Yue Wang; Roger J. Jiao; "Modular Design," 2018.