I.J. Information Engineering and Electronic Business, 2020, 6, 13-27
Published Online December 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2020.06.02

Analysis of Blockchain Technology Recommendations to be Applied to Medical Record Data Storage Applications in Indonesia

Senny Hapiffah
Widyatama University, Bandung, 40125, Indonesia
Email: senny.hapiffah@widyatama.ac.id

Ardiles Sinaga
Widyatama University, Bandung, 40125, Indonesia
Email: sinaga.diles@gmail.com

Received: 10 April 2020; Accepted: 24 June 2020; Published: 08 December 2020

Abstract: Personal Health Record or we know as the medical record in Indonesia has its regulations relating to ownership, confidentiality and authorization from the authorities to provide medical record entries to their ownership. Not many health facilities in Indonesia that digitize medical record data storage and there are still many health facilities that use third parties to manage medical record data. This raises problems such as data access, data exchange, privacy, security and approval among the people involved in it. In this case, the doctor is authorized to provide the patient's medical record, according to the examination results that have been carried out by the patient.

Blockchain technology or distributed ledger technology seems to offer a solution to some of the problems encountered. Blockchain is a digital ledger of verified transactions that are locked chronologically in an encrypted chain. This platform uses a decentralized approach that allows the information to be distributed and that each piece of distributed information or commonly known as data have shared ownership. Based on these functional needs, Blockchain technology Ethereum can be a solution. Ethereum blockchain provides smart contract features that are *stateful* and *Turing-completeness*, so that it can be used to store data and execute complex operations. This study provides an overview of how blockchain technology can be a solution to problems that arise related to the storage of patient medical record data in Indonesia. While the InterPlanetary File System (IPFS) is used to accommodate file sharing requirements.

Index Terms: Blockchain Technology, Smart Contract, Ethereum, Personal Healthcare Record, Medical Record, Cryptography.

1. Introduction

Since the blockchain was first introduced through bitcoin (electronic money) a few years ago, research regarding blockchain technology has continued to expand the application of blockchain technology in other cases, especially outside the finance industry. Blockchain is known as the safest online financial technology ranked 3 in "*Computer Society's top 10 tech trend to watch in 2018*". This makes blockchain technology being intensively developed. Healthcare is one of the industries where blockchain is expected to have a significant impact. Quoted from the journal healthcare titled "*Blockchain Technology in Healthcare: A Systematic Review*", it is known that research in this field is relatively new but growing rapidly. So, health informatics researchers and practitioners are always struggling to keep up with the progress of research in this field. [1]

Personal Health Record (PHR) or better known as a patient's medical record is a record of personal health history. At present medical record has been based on Electronic Healthcare Record (EHM). Electronic Healthcare Record has the potential to give patients better access, personalized and safe access to their medical data and enable self-care management. Electronic Healthcare Records are usually maintained centrally by health organizations and rule out the integration between different health organizations to see the complete medical history of a given patient [2]. In Indonesia, Medical Record is a file that contains a record of documents about the patient's identity, examination, treatment, actions and other services that have been provided to patients.

In Indonesia, the making of medical records has been regulated in the regulation of the Minister of Health of the Republic of Indonesia number 269/MENKES/PER/III/2008. Medical record data is confidential and should only be written by the doctor or medical person in charge of the patient. But there are still many health facilities that still use third parties. The third party here is the officer who enters the patient's medical record data into the hospital system after the doctor has written it down on the patient file (still in paper form).

As quoted from the journal Frontiers in Medicine with the title "*A Ledger of Me: Personalizing Healthcare Using Blockchain Technology*" mentions if trends emerge around using blockchain technology, or distributed ledger technology seems to offer a solution to some of the problems encountered, especially issues of approval, data exchange (integrated), data access and security. [3]

Besides, William J. Gordon and Christian Catalini, in their journal entitled *"Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability"* want to show that the patient has full control over the data he has (interoperability). Patient-centered interoperability has challenges in terms of security and privacy, technology incentives and governance that must be overcome for this type of data to succeed on a large scale [4]. Gordon and Catalini see that the blockchain has a high likelihood of overcoming interoperability, especially for clinical data transaction volumes, privacy, security, patient involvement and incentives.

However, interoperability is an obstacle to development. This is supported by research conducted by Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman of the Massachusetts Institute of Technology, the United States in the journal entitled *"MedRec: Using Blockchain for Medical Data Access and Permission Management"* said blockchain technology can be used to overcome problems health data access and management approval. [5]

Blockchain technology is famous for cryptocurrency applications such as Bitcoin and Ethereum. Blockchain is a digital ledger of verified transactions that are locked chronologically in an encrypted chain. Ledgers are updated with new transactions each time unit, which allows each computer to access the same ledger together. Transaction chains are blocked and encrypted, to destroy one of the documents in the blocked block, hackers must destroy all transactions in the block and this is difficult to do without the knowledge of the stakeholder in it.

In Indonesia, the application of blockchain technology is being intensively developed. Excerpted from the CIPG Communication and Information study on the Dynamics of Blockchain Development in Indonesia, the Indonesian people's expectations of the blockchain are getting stronger, seen by Blockchain 2.0 was applied in several banks in Indonesia to support process efficiency their business [6]. This was driven by the achievements of several blockchain companies from Indonesia that gained achievements in the international arena, like Online Tax [7] and DattaBot [8].

One application of this technology in Indonesia, as implemented by one of the largest private banks in Indonesia which implements a blockchain as an activity contained within the company itself. Another example is the *digiro.in* system developed by POS Indonesia. This system applies blockchain technology to be used in multicurrency services or can also be referred to as the evolution of current account services which will certainly also be one of the business models that are widely applied at POS Indonesia [9].

In Indonesia, there are not many health facilities that implement technology (especially blockchain technology) in their health care systems, especially for recording patient medical records. According to the viva news page quoted on 23 July 2019, it is known that 78 hospitals have implemented digital technology in storing medical records, and at least many of them have applied the concept of paperless [10]. Although Indonesia is still far behind in the use of technology in the storage of medical records, several technology companies specializing in blockchain technology have immediately assisted the development of blockchain technology as its application to medical record storage and health information technology in Indonesia.

Many medical record-keeping applications developed in Indonesia still use storage in general (other than on blockchain networks, such as MySQL or IBM DB2). This requires that a third party handles the medical record data. As mentioned earlier, the existence of a third party (in this case the party that manages medical record data) can raise the issue of trust. Because medical record data is confidential and valuable data that is only owned by patients, the presence of a third party can lead to the fraud of the medical record data that is stored and managed by such third parties.

In Indonesia, the medical record data that has been written by the doctor in the medical record file will be entered into the patient's medical record data storage application at the health facility by a special medical record administration officer. This raises problems regarding third parties and the validity of the medical record data [11].

According to the regulation of the Minister of Health of the Republic of Indonesia number 269/MENKES/PER/III/2008. Medical records are the property of the patient, written by the doctor or health worker concerned and managed by the health facility. In the process, the medical record file may not be taken home by the patient, and the patient is only allowed to bring home the final information (conclusion of examination results). This is so that there is no cheating on the patient's medical record and that there is no misinterpretation of the patient's medical record information.

The mechanism for storing medical record transaction storage is similar to the cryptocurrency transaction mechanism, where the entire network will record the ongoing data. If the cryptocurrency includes the amount of the transaction and the balance held, the same is the case with medical record records where one's health information will always be recorded every transaction is carried out (ca be in consultation with doctors, medical treatment, etc).

On the other hand, each health facility has a different system between one and the other. This makes the medical record data of one patient can be different in each facility that the patient visited. This raises the problem of data integration between health facilities regarding the patient's medical record data.

From this background, we know that blockchain technology is a technology that can be developed further. For that blockchain technology can also be applied to the medical world, in this paper the authors conclude if the problem raised is:

1. How to overcome the issue of trust in medical record data maintained by third parties? This raises the privacy and security issues of the stored medical record data.
2. Medical record data written by doctors is not directly stored into the system, but by a third party tasked with entering the medical record data into the health facility system. This raises the issue of authorizing the validity of medical record data stored in the medical (approval made by the doctor or medical person concerned).
3. The different systems applied in each health facility and the differences in the patient's medical record data stored, causing data exchange problems between systems that are running in each health facility.
4. Patients cannot see all the medical record information they have. Patients only know the final results of the examination in consultation with the doctor or medical personnel concerned. This raises the problem of access to medical records data by patients, so it is also under applicable regulations.
5. Can blockchain technology be a solution to the problems that arise related to storing medical record data?
6. What are the advantages and disadvantages of blockchain technology in its application to electronic medical records?

OBJECTIVE

The purpose of this research is to find out whether blockchain technology can be a solution for problems that arise related to medical record data storage in Indonesia. This study refers to several studies that have been done before, as a reference to the solutions offered. And to find out what are the weaknesses and strengths of the offered solutions.

SCOPE

Blockchain technology is a technology that can be applied in many fields, one of which is in the health sector. For this reason, in this study, researchers wanted to find out how blockchain technology can be applied to patient medical records. The application of blockchain technology to patient medical record data will be seen from how the medical record data is stored and accessed by the parties concerned. Also, medical record transactions will focus on the interaction of information between doctors and patients without seeing other stakeholders.

METHODOLOGY

This research is a qualitative exploratory study which is a study aimed at obtaining in-depth information about inputs, processes, feedback, and control related to the organization of medical records based on the Regulation of the Minister of Health of the Republic of Indonesia by using the ethereum blockchain feature, namely the smart contract. The stages of this research consist of:

1. *A literature study*, this stage is to look for and study the literature that supports the research conducted. This stage will be discussed in the supporting theory section, which contains supporting literacies in this study.
2. *Analysis of related wor*k, this stage is intended to further examine the problem being faced. Related work analysis is needed to find out whether the solution offered is good and following the problem at hand. In addition to being related to similar research that has been carried out, at this stage, an analysis will be made of good and correct medical records following applicable regulations in Indonesia.
3. *Problem Domain Analysis*, based on the results of literature studies and related work studies, these materials are developed to determine the problem domain and will be adjusted to the needs of this research.
4. *Designing the results of the analysis*, this stage explains the design of the system being built. This design is based on the results of the analysis in the previous stage. The results of this design are expected to be used as a reference at the implementation stage. Design refers to the process requirements and functional requirements. This stage will be explained in the *Result and Implementation* section.
5. *Implementation*, this stage explains the module that will be implemented as a form of realization from the previous planning stage. Here the author will give an overview of what modules might be applied to medical record applications.

2. Literature Review

A. Cryptography

Cryptography provides techniques for the transformation of data to render it useless for unintended receivers of the data [12]. Useless, in this context, means the thwarting of two basic actions; extracting information from the data and

injecting false data or altering the data. This is called the confidentiality- and the integrity-problem respectively. Additionally, one could imagine the case where a sender encrypts and sends a message only to later deny having sent it. Not being able to plausibly deny having sent specific data is another cryptographic goal, called non-repudiation. At its core, cryptography is the theory, but also to a large extent the practice, of preventing and detecting cheating or disallowed access to and usage of data. On the book Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone. (Alfred J. Menezes, 1996)

To achieve authentication and non-repudiation using cryptography, digital signatures are used. In other words, to assure that a specific person/device has sent a specific messagblockchaine, it needs to be digitally signed, just like letters would be imprinted with a special seal and signed by the hand of the sender in former times. A digital signature is a method for digitally signing data with, perhaps, even more, the certainty of identity than a handwritten letter. Formally, this authenticates the message sent, ensures that the sender cannot deny having sent it and also ensures senders identity

There are essentially two types of digital signature algorithms, those that require the original message as input for the verification algorithm, and those that do not. In the latter case, the original message is recovered from the signature itself. Digital signature schemes with appendix rely on hashing algorithms and are more widely used than the alternative message recovery-type since they are less prone to existential forgery attacks.1 Digital signatures with message recovery don't require a priori knowledge of the original message, for verification. It is especially suited for sending short messages since the message can be recovered from the signature itself

B. Personal Healthcare Record

Personal Health Record also is known as a medical record, according to *The Office of the National Coordinator for Health Information Technology*, in his journal entitled "*Personal Health Records: What Health Care Providers Need to Know*" says that Personal Health Records are records that are controlled by individuals (patients) and can include information health from various sources, including several health care providers and patients themselves [2]. PHR is separate from and doesn't replace official records from any health care provider. Another term known in the world of Health Information Technology is the Electronic Health Record (EHR), where information in electronic records is usually entered and accessed by a healthcare provider. And may only have information from one health service provider or group practice.

In Indonesia the patient's medical record is specially regulated by the Regulation of the Minister of Health of Republic Indonesia number 269/MENKES/PER/III/2008 [13]. In section 1 subsection 1 states that a medical record is a file containing records and documents about a patient's identity, examination, treatment, actions and other services that have been provided to patients. Medical records are written by doctors, dentists or health workers who are responsible for the patient's servants. Medical records can contain supporting documents such as supporting examination, daily observation, and treatment records, and all recording, whether in the form of radiological photographs, imaging and electro recording diagnostic.

C. Blockchain

Blockchain technology was first known through the Bitcoin cryptocurrency application. The alternative definition proposed by Vitalik Buterin. Founder of Ethereum, blockchain is a magical computer where anyone can upload a program and leave the program to be executed on its own, where states now and the previous state in each program are always visible to the public and carry very strong crypto economically guaranteed that programs running on the chain will continue to run properly by following the specified blockchain protocol [14]. While IBM says that the blockchain is a public ledger that cannot be changed to record the history of transactions ("How does Blockchain Work?" 2016). Figure 1 that explains the whole process of a transaction being send from a user on the blockchain network.

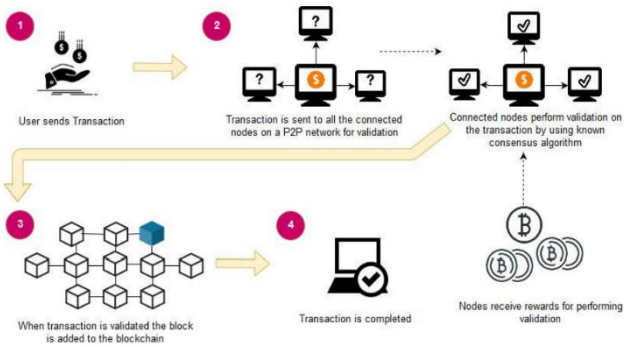

Fig. 1. An Overview of Blockchain Architecture [15]

Blockchain is a distributed computing architecture where computers disconnect nodes if they participate in the blockchain network. Each node has full knowledge of all transactions that have taken place, information is shared. Transactions are grouped into blocks that are added consecutively to distributed databases. Only one block at a time can be added and for new blocks added it must contain mathematical proof that confirms that it follows the order of the previous blocks. Such blocks are connected in chronological order.

D. Ethereum Smart Contract

Smart contracts are, in the context of blockchain, simply logic that is published on a blockchain, can receive or perform transactions like any address (transactions may be rejected or require special arguments to function) and that can act as an immutable agreement. The purpose of the smart contracts is to act as a "computerized transaction protocol that executes terms of a contract" (Szabo, 1994) and was first coined by cryptographer Nick Szabo. [12]

Smart Contract is a special account that stores executed code together with associated data and an account balance on the blockchain. Smarts contract has an address (public key) and created by the transaction. These transactions are used to interact with a contract on the blockchain by sending money to its account balance or by executing code. To execute the contract's code, a call function containing name and parameter being code in binary and sent to the contract in the data field transaction as figure 2. [16]

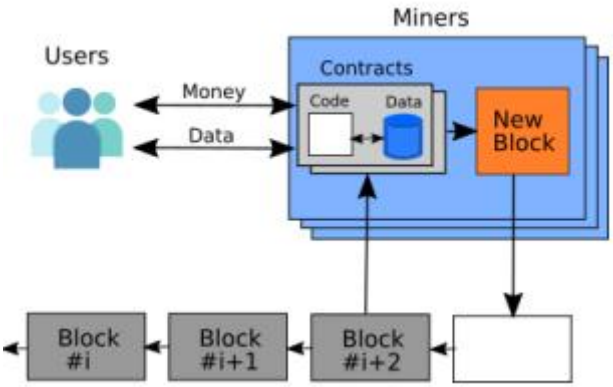

Fig.2. Execution of a smart contract on the blockchain. (Schüpfer, 2017)

Figure 2 illustrated the interaction of external accounts (users) with a contract. Every time a contract receives a message from another contract or a transaction from the user, it can receive *ether* or execute a function that is specified in the data field. In the same way, a contract can send money from its balance to other account or execute the function on other contracts by through broadcasting of messages.

Execution of the code takes place on all mining nodes in the network concurrently which reach consensus over the new state of the contract using a proof-of-work algorithm. The persistent variables of a contract are stored on the storage, a key-value store associated with the contract that is persisted on the blockchain. Access to the storage is very expensive (20000 units of gas per 256-bit word) because it has to be stored on every full node in the network. Intermediate results of computations are stored in the memory, a non-persistent byte-array. The state, as well as the code of a contract, are public and the code of a contract cannot change retrospectively.

Every decentralized application requires more than one smart contract to work well. There is no way to write smart contracts that are safe and scalable except by distributing logic and data into several contracts. *Five types models* help the classification process for designing smart contract structure [17]. In this way the contract is divided into five types:

1. Database contracts

This contract is a contract that functions as data storage. The only logic that is in this contract is *insert*, *update*, *delete* and *permission logic*.

2. Controller contracts

This contract is responsible for operating the database contract. This contract can also perform insert, update, or delete functions into several database contracts.

3. Contract Managing Contracts (CMC)

The purpose of this contract is to regulate the existence of other contracts. With this contract, communication between contracts becomes easier.

4. Application Logic Contracts

This contract contains the specific code of the application being built. In general, if a contract uses controller contracts and other contracts, these contracts are application logic contracts.

5. Utility Contracts

These types of contracts have specific jobs, such as libraries in object-oriented programming languages.

3. System Analysis

This work based on how blockchain technology can be a solution to the problem of PHR application development such as data access, data exchange, approval, security and privacy. And this work is based on providing security and privacy through cryptography-based access control to store data in the cloud and encryption through attributes. Literature survey needed to find and study things that can support developing application.

As explained in the introduction, recently many authors examined the thought of mistreatment clever agents in ambient to produce ability. Some authors explored blockchain technology has a theoretical approach we tend to do some proposing ways to enhance quality and security in PHRs mistreatment. As explain in the journal titled *"Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability"*, published on June 30th, 2018, say that patient-centered interoperability, however, brings with it new challenges and requirements around security and privacy, technology, incentives, and governance that must be addressed for this type of data sharing to succeed at scale. In this paper, writers look at how blockchain technology might facilitate this transition through five mechanisms: (1) digital access rules, (2) data aggregation, (3) data liquidity, (4) patient identity, and (5) data immutability [4].

In *"A Model for Blockchain-Based Distributed Electronic Health Record"*, published in 2018 with the problem related to lack of integration Electronic Health Record between health organization, it makes patients and doctors not have the same view of medical records that are ofter stored in the system different health information organizations, proposed a blockchain in a distributed architecture for Electronic Health Record integration called UniRec (Unified Medical Records). [18]

On the thesis worked on by Jonatan H. Bergquist from Uppsala Universitet, *"Blockchain Technology and Smart Contract: Privacy-preserving Tools"*, research on how blockchain technology and smart contracts can be used to securely share and control personal information among parties who do not necessarily trust each other [12]. This will be proven by a proof-of-concept application for the use case of electronic medical records (EMR). The results of the investigation will have clear applicability to many use cases. Like How can the architecture of a blockchain application for privacy-preserving data-sharing between known, but not necessarily trusted, parties look like? They suggest using blockchains for permissions management and for storing pointers to encrypted data, while the actual data is hosted by a trusted, blind escrow service (Zyskind et al., 2015). This thesis proposes the use of smart contracts for developing systems with blockchain.

Blockchain technology is a better way to provide medical records to make secure where it is also known as distributed ledger technology, where it requires no third party to organize, maintain, and manage data in the records. Ethereum is a decentralized platform software platform that has functionality like smart contracts and distributed applications to be built without any downtime, error, fraud or third-party interference. It possesses smart contract functionality, it is a computer code where we can write what kind of operations we want to perform. Blockchain holds the promise to create the new data deal, a greater degree of individual ownership, control and content distribution of personal data, within a system that allows community to benefit from the aggregation of data. [19]

Based on *"MedRec: Using Blockchain for Medical Data Access and Permission Management"* journal from (Azaria, Aekblaw, Tvieira, Lip) Massachusetts Institute of Technology, 2016. Mention about system orchestration: provider adds a record for the new patient as below. [5]

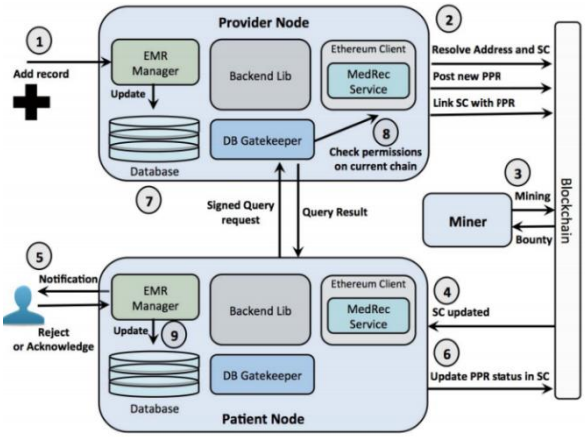

Fig.3. System orchestration: provider adds a record for new patient

Figure 3 illustrated how the provider (in this case is a doctor) adds the new medical record for a new patient. Using the Registrar Contract on the blockchain, the patient's identifying information is first resolved to their matching Ethereum address and the corresponding Summary Contract is located. Next, the provider uploads a new PPR to the blockchain, indicating their stewardship of the data owned by the patient's Ethereum address. The provider node then crafts a query to reference this data and updates the PPR accordingly. Finally, the node sends a transaction which links the new PPR to the patient's Summary Contract, allowing the patient node to later locate it on the blockchain.

ANALYSIS

An analysis is needed to know the process requirements and functional requirements in making medical records. The results of the analysis will be modeled in a smart design as a reference at the implementation stage, starting in terms of architectural design, data and processes for the system to be built. Not much research has been done in Indonesia related to the application of blockchain technology in the storage of patient medical records. This is due to the many adjustments in the format of medical records owned by each health facility.

Analysis conducted refers to the regulation of the Minister of Health of the Republic Indonesia number 269/MENKES/PER/III/2008 and medical record manual book's issued by the Indonesian Medical Council (KKI) in 2006 based on the mandate of Law number 29 of 2004 concerning medical practice section 46 subsection (1) which states that every doctor or dentist in carrying out medical practice must make a medical record. [20]

The process of organizing medical records begins at the patient is received at home sick, continued with data recording activities medical patients by the doctor or dentists or personnel other health services that provide activities directly to patients [20]. The organization of medical records includes:

1. Patient acceptance
2. Recording
3. Management of medical records
4. Retention of medical records
5. Retrieval of medical records

For the results of the analysis of the making of medical records contained in the regulation of the Minister of Health and the manual book, it is known that the contents of the medical records are adjusted according to its type, namely medical records for outpatients, for inpatients and one-day care, for emergency patients and patients in the state of disaster. The medical records at least have the contents as below.

a. Patient's identity;
b. Date and time-examined patient
c. Anamnesis result, at least contain disease history and patient's complaint
d. Physical examination result and medical supporting
e. Diagnosis
f. Management plan
g. Treatment and/or
h. Other services that are given to the patient
i. Clinical odontogram specifically for the dental patient
j. Authentication for medical treatment if needed

The medical record for inpatients and one-day care, at least information added,

a. Clinical observation note and treatment result
b. Discharge summary

The medical record for emergency patient, plus information

a. Patient's condition when arrived in the emergency unit
b. Patient's companion identity
c. Patient's condition summary before leave emergency unit
d. Transportation by a patient to the emergency unit
e. Other service that patient given by medical

The medical record for patients in state of disaster, at least information added,

a. Patient's condition when arrived in the emergency unit
b. Patient's companion identity
c. Patient's condition summary before leave the emergency unit and follow up plan
d. Transportation by a patient to the emergency unit
e. Other services that are given to the patient
f. Type of disaster and location that patient to be found
g. Patient emergency's category and disaster patient number
h. The identity that found the patient

While the procedures for organizing medical records which are regulated in section 5 regulation of the Minister of Health of the Republic Indonesia number 269/MENKES/PER/III/2008, can be seen through the information as below.

1. After a patient being examined by the doctor, the doctor should write the result to the patient's medical record file
2. Each medical record must have the name, time and signature of the officer who provided health service (in this case doctor or dentist).
3. If an error occurs when recording medical records, records and files must not be deleted in any way. Changes to records of errors in the medical records can only be done by crossed out and the affixing the initial officer concerned.

To describe the various functional requirements that users have on the application, user stories were written and are shown in table 1.

Table 1. User stories defining functional requirements and guiding development

Actor	Role
Doctor	• Examining patients • Write and edit the content of the medical record according to the results of the examination • Authorization of patient examination results on the medical record • Explaining examination result to the patient
Patient	• Check up (consultation regarding his health problem to the doctor) • Got explanation the examination result • Got examination result summary that approved by the doctor

Based on the results of the analysis we can summarize the requirements applied to the system will be built are as follows.

1. Only those permitted to should be allowed to connect to the network.
2. There must be immutable traceability built into the system, where it is possible to see:

a. Who wrote the examination of the results of the medical records
b. Supporting document that including in there.

Immutable traceability means that there must be a history of changes made to medical records and that it must be made very difficult, if not impossible, to alter it post ex.

3. Smart contracts must be exchangeable without needing to remove the entire system or change addresses to contracts with which humans interact.

The transaction that can be used divided into:

- Doctor data transaction
- Patient data transaction
- Medical record data transaction

Each participant (in this case is a patient and doctor) who joined the blockchain network, when register will generate a public key and private key as their identity in conducting transactions. Account data (such as doctor and patient) will be generated using ganache. Medical records transactions carried out by doctor and patient will receive to be a historical record of observer patients, data records can be stored in another block as follows.

1. The doctor writes the examination results in a medical record data transaction in the system
2. The data transaction is entered into a smart contract through a series of logic that contains a business rule between the patient and the doctor. The business rule referred to the doctor sign the medical record data as a valid form of medical record authorization according to the regulation of the Minister of Health of the Republic of Indonesia
3. After passing the smart contract stage, the transaction enters the consensus stage. In *ethereum*, the consensus used is to use the Proof of Work (PoW) technique or commonly called mining. Proof of Work (PoW) is a protocol based also on cryptographic hash function, in which the miners are required to solve a computationally difficult problem to determine the miner whose block is accepted to be added to the blockchain.. At this stage the transaction will check whether it is double spend, whether the size is appropriate and whether the the resulting hashing value is correct.
4. If the mining process is successful, then the new block is stored in the blockchain network.

While other parties (patient) wishing to access block (medical record data) mush have a public key and private key contained in the block. The patient can access a medical records that owned by him.

4. Result and Implementation

Unified Modeling Language (UML)

The Unified Modeling Language is a visual language for specifying, constructing and documenting the artifacts of systems [21]. The UML defines various UML profiles that specialize subsets of the notation for common subject areas. The Unified Modeling Language is a popular dialect for indicating, Visualization, Constructing and archiving the curios of programming framework, and for business demonstration and different non-programming frameworks. Figure 4 describe overview of different users and their interaction whit blackchain network. And table 2 is a description of user interaction with a smart contract system with the following details

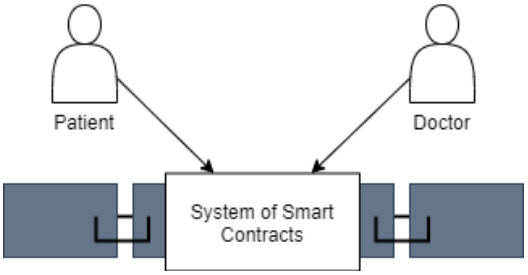

Fig.4. Overview of different users and their interactions with the blockchain and system of smart contracts which exist on the blockchain

Table 2. Detail interaction different users with the blockchain and system of smart contracts which exist on the blockchain

Doctor *data owner*	Patient *data request*
• Secure login • Provide data assets • Discretionary access control • Set smart contract	• Secure login • Makes transaction request

A use case diagram (UML) is a behavioral diagram defined and created from a Use-case analysis. Its purpose is to represent a graphical overview of the functionality provided by a system in terms of actors and any dependencies. The main purpose of a use case diagram is to show how system functions are performed for which actors. The roles of the actors in the system can be depicted in figure 5.

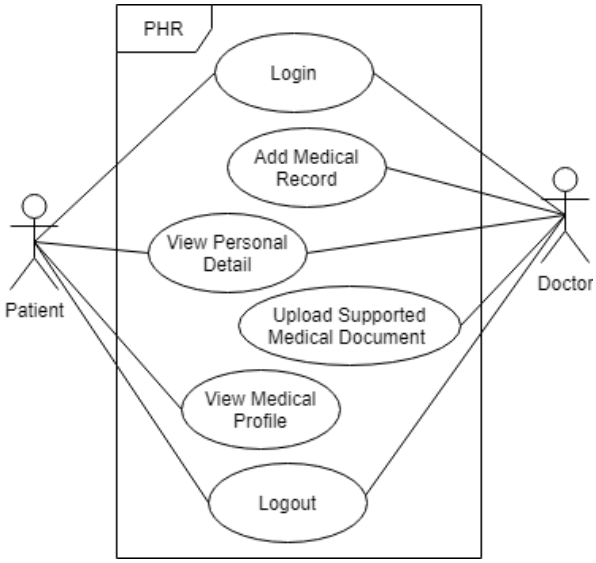

Fig. 5.Use case diagram PHR application

Based on the analysis conducted previously on medical record contents, can be described by medical record data that will be entered into a block for each transaction are as table 3.

Activity diagrams are used to present the business and operating step-wise workflows of an individual system components or items in a system. Procedures for organizing medical records based on previous analysis can be seen in the activity diagram as figure 6.

Table 3. Structure data of medical record JSON

Attribute name	**Description**	**Null able**
datetime	Examination date and time	Not null
patientType	Type of patient such as outpatients, inpatients and one-day care, emergency patients and patients in state of disaster	Not null
anamnesisResult	At least contain patient's disease history and patient's complaint	Not null
physicalExaminationResult	Patient examination result in that day	Not null
Diagnosis	Doctor's diagnosis	Not null
managementPlan	The next plan after examination	Not null
Treatment	Treatment that doctor give for the diagnosis	Not null
otherService	Other service that patient needed such as advice to the lab, image processing (x-ray, rontgen, etc)	Not null
clinicalOdontogram	Odontogram clinical result just for dental patient	Null

clinicalObservationNote	Clinical observation note during the treatment in hospital or clinic. Just for inpatient type	Null
dischargeSummary	Examination summary before patient can be home soon. Just for inpatient type.	Null
patientCompanionId	Patient companion's identity that bring patient to emergency unit.	Null
patientFoundedId	Identity to the person that found the patient in disaster situation.	Null
transportation	Type of transportation that bring the patient to the emergency unit, such as ambulance.	Null
patientSummaryUGD	Patient's examination summary during emergency service in emergency unit.	Null
disasterType	Type of disaster that experienced by the victims. Just for patient in state of disaster.	Null
disasterLocation	Location of the disaster.	Null
patientDisasterLocationFounded	Patient's location to be found. Specific area of the disaster.	Null

As mentioned before, blockchain is a decentralized, distributed, and public ledger that is used to record transactions on many computers so that the records (data assets - medical records) cannot be changed retroactively without changing all subsequent blocks and consensus on the network. This makes only the input process that can be done by the user. If there is an incorrect input (medical record data that is not appropriate as the blur x-ray results), then the user can re-input the medical record data. The medical record data will be stored historically on each block in the blockchain network. Based on MedRec prototype and analysis result, flowchart about how medical record data stored in the blockchain as figure 7

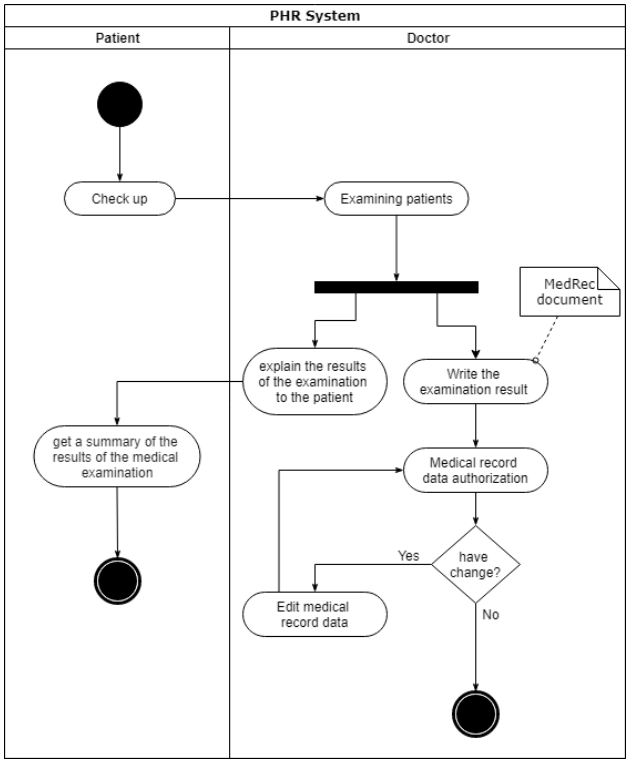

Fig.6. Activity diagram of valid medical record procedure

Figure 7, illustrates how medical record being made. The first doctor will create a medical record on application, doctor writes every patient's examination result information. That medical record or we call data assets will be processed as metadata transaction. Transaction metadata is a section of data that gets added to a transaction after it is processed. Any transaction that gets included in a ledger has metadata, regardless of whether it is successful. The transaction metadata describes the outcome of the transaction in detail. Then file medical record will be uploaded to the IPFS network [22]. IPFS (InterPlanetary File System) is used to accommodate file sharing requirements so that transactions can be done with minimum gas usage and minimum time [23]. After file being uploaded in the IPFS network we get a content address.

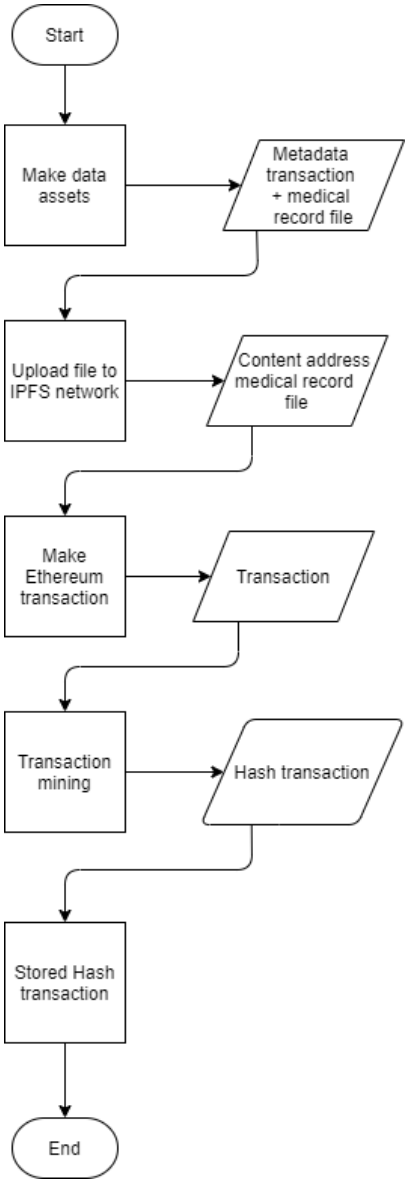

Fig.7. Flowchart on how medical record being made

The next step is the ethereum transaction. Ethereum transactions require **addresses** and **private keys** [24]. The public addresses are stored and the transactions to and from them are visible for anyone to see. The private keys are used to unlock these addresses to make a transaction. Ethereum transactions are processed through the **Ethereum Virtual Machine** (EVM). The EVM mainly executes smart contract interactions, where every time someone interacts with the contract, all nodes are required to agree that the transaction took place. Where the miners validate blocks and track the ownership, then the EVM executes a **pre-programmed contract** according to the rules of the transaction. Ethereum is still a **record of all past transactions**, in that all the history of the blockchain is stored and validated through consensus. However, Ethereum's node operators also **record a history of smart contract interactions** that have occurred on the Ethereum network.

In each ethereum transaction, the following components come into play [24]:

- Input address: the address which the transaction will be sent from
- Amount: the amount in ETH(ether) that will be sent
- Gas price
- Gas limit
- Output address: the receiving address
- Private key: used by the input address owner to sign the transaction

The gas limit and gas price are used to calculate the fee, which is given to the miner who validates your transaction. In this case, the miner will be made a kind of bot that will automatically do mining (infinite loop) every time a transaction comes in.

ADVANTAGES

- Blockchain could make medical records more accessible to the doctor during an emergency.
- Decentralize data storage, providing health facilities and service providers are no longer assigned to handle their patient data.
- Immutable data storage, makes no data can be lost or corrupted.
- Interoperability, all the data will be stored in a single format, ensuring process integrity and a simpler ecosystem and a trustless exchange.
- Without a third party handling medical record data, becoming a blockchain as the best solution for privacy and security issues of ownership of data assets.

DISADVANTAGES

- Blockchain is a new technology, it's still in its nascent stage and needs more research to integrate it into existing core systems. Much research and development are needed, especially in Indonesia on the application of blockchain technology in building medical record applications.
- Immutable smart contract, as there are clear advantages of having a permanent and irreversible record, at the same time, there is a bitter flipside for this. For example, if there is a defect with code that can harm the system, it also cannot be fixed and creates an opportunity for the attacker to exploit the same defect repeatedly in the future. Over time, the ability to correct mistakes will become more complex..
- If a data asset error occurs during the input process, it requires the user to re-input the data. This will make historical data more and more due to the nature of the blockchain that cannot be changed or deleted.

IMPLEMENTATION

Based on analysis result and system design above, know if a module is needed for application development mention as below,

1. *addMedicalRecord*, this module is designed so that a smart contracts can be used to register a new medical record as a non-fungible token. The patient's basic medical records are stored along with the IPFS hash that contains the file uploaded containing the lab results or other medical records of the patient.
2. *viewMedicalRecord*, this module is designed to let the user view medical records of a patient stored in the application. The view records function is used both by doctors and patients. The patient can view his records by the system authenticating that the patient views only his own medical records. For this purpose, the system uses the public account address of the patient to ensure that only the relevant medical records are shown to the patient.
3. *accessRequestMedicalRecord*, this module is designed for each of the above-mentioned transactions, certain users would need to have access to. For example, only the doctor or nursing staff can make changes in the records of the patient or add them. So, add and update records would only be accessible to these entities. Moreover, the patient can view his medical records but won't be given access to add or update them.

The system that is prepared for medical record data storage applications will depend on the technique used. In this study, the technique used is to use smart contract *ethereum*. From research conducted by Albert Palau who analyzed the hardware requirements for *ethereum* mining techniques are as follows [25]:

1. To get a full validated Ethereum node without storing +1TB of SSD, we must use Parity (*Parity Ethereum* is the fastest and most advanced *Ethereum* client.) at the moment because it's the only client permitting pruning while is syncing the full blockchain
2. Requires a fairly large SSD, because it makes an intensive use of random writes to disk.
3. Requires a large type of CPU because it makes an intensive use of syscalls which interrupt the CPU a lot. At least the CPU is used for special gaming software, such as Intel i5.
4. A SSD able to perform: 68 MB/s of random writes and 30.9 MB/s of randoms reads on average. +112GB of capacity (24/09/2018).
5. 13–14GB of RAM

These requirements are not the minimums. According to research conducted, with the above hardware, we will get a block synced per minute average of 340.2. And we will eventually get synced with a rate of 4.29 and above but it will take more time. Further and special research is needed to find out the appropriate system requirements for medical record applications. Given the amount of data that will be stored into the blockchain network in a certain time unit.

5. Conclusion

Based on literature review and analysis related to a medical record that has been done, it can be concluded that, blockchain technology can be applied to minimize privacy and data access issues with the presence of public keys and private keys as identities and authorization of medical records. Also, blockchain technology is immutable and each block has cryptography hash makes it easy to detect the presence of sabotage. But there are also drawbacks, because having a permanent and irreversible record, at the same time, there is a bitter flipside for this. For example, if there is a defect with code that can harm the system, it also cannot be fixed and creates an opportunity for the attacker to exploit the same defect repeatedly in the future.

In Indonesia, there are not many health facilities that implement a direct system for storing medical records. Many health facilities still use a third party (the officer who enters the medical record file into the system, not the doctor or health worker in charge of the patient). For this reason, digitizing the process of making medical records with authorization in accordance with the regulations of the Ministry of Health of the Republic of Indonesia is the main solution to this problem.

Although there have been developments related to the application of medical records in Indonesia, however, the presence of third parties handling medical records can cause issues related to the privacy and security of medical record data assets. Blockchain is present as one solution in dealing with the issue.

With the use of blockchain technology and the smart contract *ethereum* feature, the implementation of medical records can be carried out following applicable legal aspects, namely the smart contract feature based on the regulation of the minister of health of Republic Indonesia and the medical record's manual book. And without the need for a third party to handle the data, making blockchain technology the best solution to the problem.

File requirements needed supporting documents for digital medical records to support patient examination results. The file-sharing process can be done through the smart contract alone or with the help of other technologies such as IPFS. IPFS is a decentralized file-sharing technology that can facilitate file sharing needs on the network.

For the future, we need to improve the analysis of stakeholders that include in medical records areas such as healthcare providers, insurance companies, nurses, etc. Other than that, as explained in this study, that is as a signature is changed into digital form. The division application is used as a reference to prove the legality of digital signatures in Indonesia. However, analysis and development need to be done more deeply so that later the signature of SiVION can be validated.

Also, the many healthcare institutions in Indonesia make the format of medical records in each healthcare institution different from one another. It is adapted to the system they are using, although generally it is still based on the provisions of the minister of health regulation as explained earlier. For this reason, it is necessary to analyze the integration of patient medical record data, so that the integration of distributed PHR among healthcare institutions can support physicians for a more accurate diagnosis since more information about the patients would be available.

References

[1] C. C. Agbo , Q. H. Mahmoud and J. M. Eklund , "Blockchain Technology in Healthcare: A Systematic Review," Healthcare Journal MDPI, vol. 7, no. 56, pp. 1-30, 2019.

[2] "Personal Health Records: What Health Ccare Providers Need To Know," Official Website of The Office of the National Coordinator for Health Information Technology (ONC), [Online]. Available: https://www.healthit.gov/sites/default/files/about-phrs-for-providers-011311.pdf.

[3] G. Leeming, J. Cunningham and J. Ainsworth, "A Ledger of Me: Personalizing Healthcare Using Blockchain Technology," Frontiers in Medicine, vol. 6, pp. 1-2, 2019.

[4] W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to," Computational and Structural Biotechnology Journal, p. 1, 2018.

[5] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in International Conference on Open and Big Data, Cambridge, Massachusetts, 2016.

[6] Direktorat Jenderal Aplikasi Informatika Kemkominfo, Big Data, Kecerdasan Buatan, Blockchain, dan Teknologi Finansial di Indonesia: Usulan Desain, Prinsip, dan Rekomendasi Kebijakan, Jakarta: Kementrian Komunikasi dan Informatika Republik Indonesia, 2018.

[7] G. Suroyo and T. Diela, "Indonesia looks to blockchain to fix its dodgy data challenges," Reuteurs, 4 May 2018. [Online]. Available: https://www.reuters.com/article/us-indonesia-blockchain/indonesia-looks-to-blockchain-to-fix-its-dodgy-data-challenges-idUSKBN1I503R. [Accessed 4 April 2020].

[8] Datta Bot, "What is Dattabot," PT Mediatrac Sistem Komunikasi, [Online]. Available: https://dattabot.io/what-is-dattabot/the-business/. [Accessed 4 April 2020].

[9] Techfor ID, "Penerapan Blockchain di Indonesia," Technology For Indonesia, 16 December 2019. [Online]. Available: https://www.techfor.id/penerapan-blockchain-di-indonesia/. [Accessed 4 April 2020].

[10] Tim Viva, "Tiap RS di Indonesia Akan Terapkan Sistem Medical Record Digital," Viva, 23 July 2019. [Online]. Available: https://www.viva.co.id/gaya-hidup/kesehatan-intim/1168504-tiap-rs-di-indonesia-akan-terapkan-sistem-medical-record-digital. [Accessed 30 April 2020].

[11] "Standar Profesi Perekam Medis dan Informasi Kesehatan," Universitas Dian Nuswantoro, [Online]. Available: https://dinus.ac.id/repository/docs/ajar/STANDAR_PROFESI_PEREKAM_MEDIS_DAN_INFORMASI_KESEHATAN_13.pdf. [Accessed 4 April 2020].
[12] J. H. Bergquist, "Blockchain Technology and Smart Contracts: Privacy-preserving Tools," Uppsala Universitet, Uppsala, 2017.
[13] Kementrian Kesehatan Republik Indonesia, Peraturan Menteri Kesehatan RI Nomor 269/MENKES/PER/III/2008, Jakarta: Kementrian Kesehatan Republik Indonesia, 2008.
[14] V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper, 2014.
[15] A. Shahnaz, D. U. Qamar and . D. A. Khalid, "Using Blockchain for Electronic Health Records," IEEE Access, pp. 2-3, 2019.
[16] F. Schüpfer, "Design and Implementation of a Smart Contract Application," University of Zurich, Zurich, 2017.
[17] Monax, "Solidity explainer," [Online]. Available: https://monax.io/docs/tutorials/solidity/solidity_1_the_five_types_model. [Accessed 14 March 2020].
[18] T. Quaini, A. Roehrs, C. A. da Costa and R. da Rosa Righi, "A Model For Blockchain-based Distributed Electronic Health Records," IADIS International Journal, vol. 16, pp. 66-79, 2019.
[19] A. Khatoon, "A Blockchain-Based Smart Contract System for Healthcare Management," MDPI Journal Electronic, vol. 9, no. 94, pp. 1-23, 2020.
[20] Sjamsuhidajat; Siregar, Abidinsyah; Murniah, Dad; Alwy, Sabir;, Manual Rekam Medis, Jakarta Selatan: Konsil Kedokteran Indonesia, 2006.
[21] C. Larman, Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development, Third Edition, Boston, Massachusetts: Addison Wesley Professional, 2004.
[22] F. Ridhwanallah, "Analisis Penerapan Smart-Property Untuk Jual Beli Rumah Memanfaatkan Blockchain Ethereum," Politeknik Negeri Bandung, Bandung, 2019.
[23] K. Kwatra, "What is IPFS?," Protocol Labs, 15 March 2018. [Online]. Available: https://medium.com/wolverineblockchain/what-is-ipfs-b83277597da5. [Accessed 14 March 2020].
[24] B. Conrad, "Ethereum Transactions – How do They Work?," BlockT, 5 October 2017. [Online]. Available: https://blokt.com/guides/ethereum-guides/eth-transactions. [Accessed 2020 March 2020].
[25] A. Palau, "Medium," Medium, 24 September 2018. [Online]. Available: https://medium.com/coinmonks/analyzing-the-hardware-requirements-to-be-an-ethereum-full-validated-node-dc064f167902. [Accessed 26 June 2020].
[26] Peyrott, Sebastián, An Introduction to Ethereum and Smart Contracts, Bellevue, Washington: Auth0 Inc., 2017.
[27] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[28] B. N. Kumar Rao, B. B. Kumar Rao and V. J, "Block chain Based Implementation of Electronic Medical Health Record," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 8, 2019.
[29] T. VIVA, "Tiap RS di Indonesia Akan Terapkan Sistem Medical Record Digital," 23 July 2019. [Online]. Available: https://www.viva.co.id/gaya-hidup/kesehatan-intim/1168504-tiap-rs-di-indonesia-akan-terapkan-sistem-medical-record-digital. [Accessed 2 May 2020].

Authors' Profiles

Senny Hapiffah, obtained a Diploma Degree (A.Md) in Computer Science and Engineering from Bandung State Polytechnic (POLBAN). She has more than 2 years of experience in the Area of Computer Science and Engineering as a programmer. Research interests include Software Engineering and image processing. Currently she is working as a programmer in one of the startup companies in Bandung, Indonesia

Ardiles Sinaga, is currently serving as a Lecturer on the Department of Informatics at Widyatama University and Binus University, Indonesia. In 2013, he is completed his S2-Magister in Telkom University on Informatics Departement. He can be contacted at sinaga.diles@gmail.com

How to cite this paper: Senny Hapiffah, Ardiles Sinaga, " Analysis of Blockchain Technology Recommendations to be Applied to Medical Record Data Storage Applications in Indonesia", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.12, No.6, pp. 13-27, 2020. DOI: 10.5815/ijieeb.2020.06.02