Design of Blockchain-based Electronic Health Records for Indonesian Context: Narrative Review

Puspita Kencana Sari
[a]Faculty of Computer Science
Universitas Indonesia
Depok, Indonesia
[b]Faculty of Economy & Business,
Telkom University
Bandung, Indonesia
puspita.kencana91@ui.ac.id

Setiadi Yazid
Faculty of Computer Science
Universitas Indonesia
Depok, Indonesia
setiadi@cs.ui.ac.id

***Abstract*— Healthcare providers in developing countries manage their medical data in Electronic Health Records (EHRs) system in silos with different structures and data formats that causes the problem of data sharing, interoperability, and data security. This paper aims to propose a concept of blockchain-based EHRs that is relevant to the case of developing countries, especially in Indonesia. The research method used is a narrative review of several literature related to the design of blockchain-based EHRs using Smart Contract from 2016-2020. The design proposed permissioned blockchain with several healthcare stakeholders as nodes in the network. Different with most previous research that using proof-based, we propose to use vote-based consensus protocol to execute transaction faster. Based on number of national health insurance policy holders, outpatient, and inpatient visits per year, the storage capacity required to keep the transaction is estimated around 2,7 TB per year with 77 transactions per seconds. This design is intended to be a contribution for EHRs platform architecture in the future.**

Keywords—blockchain, electronic health record, smart contract, healthcare, Indonesia

I. INTRODUCTION

Security and privacy of health data are essentials in providing health services. The development of the Electronic Health Records (EHRs) system by healthcare facilities offers opportunities and challenges to the protection of health data. Data sharing and interoperability among healthcare providers are required for integration as it is a major dimension in health referral system [1]. However, it will also increase vulnerability since many stakeholders will be able to access patient data. On the other side, different data formats among stakeholders makes data integration not easy. EHRs system development by various parties also resulted in large quantity of health data distributed and managed by different providers. The expected outcome of EHRs system to provide comprehensive and continuous health treatment can only be optimized when health data is shared.

EHRs, also called as electronic medical records (EMRs) or personal health records (PHRs), are related to electronic creation, storage, and management of patients' personal, medical or health-related data [2]. Generally, healthcare facilities create, store, and manage patient data into EHRs systems. A record will be created when a patient is admitted to a healthcare facility, when a doctor diagnoses a patient, or when a radiologist generates diagnostic image such as an MRI scan [3]. Data in EHRs can only be accessed by doctors and other health professionals who give medical assessment and treatment to patients in an origin health provider. In addition, health records are useful for health professionals to properly diagnose a disease so that they can administer the medicine and treatment for the disease [4].

When the patients need to be referred to other healthcare providers, the origin provider will make some medical resume from EHRs then give it to the referral provider. The control of data sharing in EHRs is owned by healthcare providers not the patients. Besides patients and doctors, other stakeholders who need to access health data stored in EHRs are health insurance companies or customers, researchers, pharmaceuticals, and public health authorities. Each health provider might have different data formats and mechanisms to organize health data. Demand from patients and healthcare providers for multiple access to have a comprehensive overview of their health condition has also raised data security, interoperability, and privacy issues [5]. Patients also do not have control over their data and hard to access their health records [3]. This problem of access control and data sharing will bring inefficiency in the management of health data. It can also increase costs, both for patients and providers, to have repeated medical examinations and treatments.

In developing countries like Indonesia, healthcare faces common problems such as availability, affordability, accessibility, sustainability services and weak referral system [6]. Pearson & Jordan [7] also revealed that health professionals in developing countries have inadequate access to health information that makes them hard to conduct evidence-based healthcare. It also causes ineffective and inefficient health treatment given to patients. In Indonesia the referral system also has some obstacles, such as different data formats among health information systems and unintegrated health data managed by various stakeholders [8]. These situations complicate data sharing and system interoperability. In addition, Indonesia has not fully implemented the family or primary doctor which is the first point of contact when patients need health treatment. National health insurance system has been established to address this problem where people should start their health treatment from specified first-level healthcare facilities. However, there are still many patients in Indonesia who use other private insurance and get direct health care at referral health-facilities or to ask for second opinions from other physicians in different health facilities. This condition will cause patient data to be unintegrated across many health providers.

EHRs implementation in developing countries are facing various challenges such as interoperability, privacy and confidentiality [9]. Blockchain is currently considered as an emerging technology that offers solutions for various industries, including the healthcare industry. There are some essential features of blockchain technology i.e., distributed databases, peer-to-peer transmission, irreversibility, and pseudonymity [10], that can be used to address issues in healthcare such as privacy and access; completeness of information; costs; and give control to patient for their health data; [11]. Blockchain technology enables and secure EHRs data-sharing mechanisms to support interaction among healthcare stakeholders in the ecosystem [3], [12] and provide a comprehensive, unchangeable medical data and services [13]. Blockchain also puts time-stamp in health records so that after broadcasting into the distributed ledger, it is tamper-proof, and patients can decide who will have what access right [3]. Therefore, the patient will have full control of their data, which is difficult to do with existing EHRs.

Research in blockchain utilization for EHRs system is still rare in developing countries [14]. Most literature about blockchain-based EHRs design comes from developed countries. A previous study in Kenya [15] suggested that blockchain-based EMR can give benefit to many stakeholders in the health sector in developing countries, specifically to improve interoperability and security. Kombe et al. [16] proposed blockchain technology for EHRs in Tanzania using a self-sovereign identity where patient or relatives can control their information stored in healthcare facilities. However, this might not be suitable for patients in some developing countries like Indonesia due to low rate of technology adaptation in healthcare facilities and patient involvement in managing their health data. Therefore, this study aims to propose a design concept of blockchain-based EHRs that is relevant to Indonesia case. The blockchain-based EHRs will utilize Smart Contract to manage access permissions to patient data and permissioned network that built from a consortium of healthcare facilities under national health insurance program. The block in the ledger will store access right for specific user and access log to the patients' records. The study is expected to give both practical and theoretical contributions to improve data sharing and interoperability while maintaining data security and privacy in healthcare services.

The rest of this report is organized into four sections as follows. The next section provides a brief overview of blockchain-based EHRs, including business processes and smart contract utilization. It is followed by a section on our research method and another section on our proposed design for the Indonesia context. Finally, the last section gives the conclusion and limitation of this study.

II. BLOCKCHAIN-BASED EHRS

A. *Mapping of the Business Process to Blockchain Process*

Blockchain proposes some solutions to traditional EHRs system problems related to data sharing, access control, and personal health information security. When a patient visits his primary doctor or specialists in a healthcare provider such as a clinic, community care centre, or hospital, the EHRs system will create a record [3], [13]. The record contains all medical information such as nursing care information, the history of drugs, medical imaging, as well as laboratory examination results. Patient records in EHRs are maintained in a decentralized way in the providers' database and cloud storage. Blockchain guarantees strong anonymity to ensure personalized genuine user access [2] based on specific access rules governed by Ethereum Blockchain Smart Contracts [17].

There are some general usage scenarios of data sharing using blockchain-based EHRs, such as (1) a health provider create or edit the patient record from its database; (2) a provider share patient record from its database to other providers; (3) patient can read his/her health record from provider database[5], [13], [17], [18]; and (4) patient can authorize the sharing of his/her health record between providers [5], [13], [17]–[19]. Meanwhile, Khatoon [17] described a more specific usage scenario on data sharing and access control among healthcare stakeholders such as process for issuing and filing medical prescriptions that involve primary doctor/physician, patient, and pharmacy; sharing laboratory test/results data that involve patients, laboratory/radiology, doctors, emergency clinics, and different partners); and data flow for healthcare reimbursement that involve patient, the insurance company, doctor, consultant, laboratory & pharmacy.

Figure 1. depicts the new business process in healthcare using blockchain-based EHRs. Provider, patient, and other stakeholders who want to share data must be registered as a platform community and given blockchain addresses to be recorded in the Smart Contract and the agreed access rights. Every time a patient visits a physician in a health provider, the health data will be recorded in EHR and stored in the provider's database. Accordingly, the provider can update the Smart Contract after adding or editing the patient record, and then the patient will be notified for the change and approve or reject it. If another stakeholders, such as a pharmacy, laboratory, health insurance, etc change anything related to the patient, it will be reflected in the Smart Contract with time-stamped log history and the patient will be notified. However, from the best of our knowledge, none of previous research have discussed access or usage scenario for nurses or midwives who are one of the most significant medical personnel in developing countries.

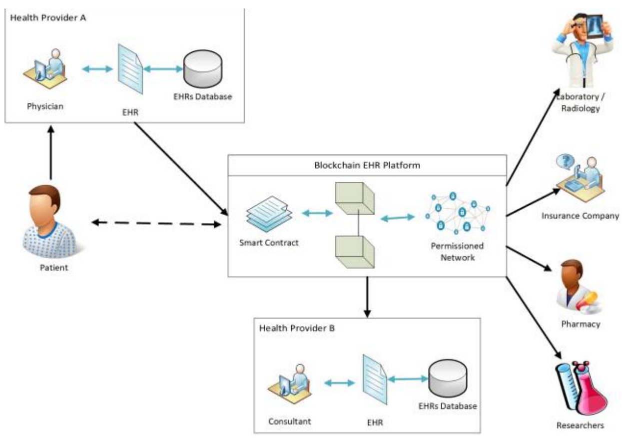

Fig. 1. Business process using blockchain-based EHRs System

B. *Health System in Indonesia*

Since 2013, the Indonesia government has established a National health insurance program as part of the National Social Security System. The Health Social Security Administration (called *BPJS-Kesehatan*) responsible for arranging health insurance for all Indonesian people through this program. Therefore, everyone must be the policyholder of national health insurance and paid for insurance premiums to receive the service. The government will give subsidy for poor people by paying their premium using the national budget. However, people can still use other private insurance as a payer instead of national health insurance by *BPJS-Kesehatan*. About 220 million people already covered as policyholders per June 2020. It will be increased until all populations are included. Since the target is national health coverage, people information regarding *BPJS-Kesehatan* program are disseminated to various stakeholders, such as healthcare facilities, community organizations, or employer's organization [20].

In this study, the design of blockchain-based EHRs using the case of a referral system covered by Indonesia national health insurance. Table I shows the total number of people who are registered as insurance policyholders in national health insurance. It also shows the total number of health facilities visits, including outpatient and inpatient in first-level health facilities and hospitals. We can conclude that a patient visit and claim for their medical treatment payment is 1-2 times per year from that table.

TABLE I. INDONESIA NATIONAL HEALTH INSURANCE COVERAGE

Year	Total number of insurance coverage (in million people)	Total number of health facilities visit (in million case)
2014	133,42	92,3
2015	156,79	146,7
2016	171,93	177,8
2017	187,98	223,4
2018	208,05	233,9

source: National Health Insurance Annual Report 2018

Health system in Indonesia follows federal government structure with three hierarchy level namely district/city, province and national level [1]. Health administration in district and province is relatively independent form the national where the health information system in each level works in different platform with little data sharing[8]. Ministry of Health has developed EHRs system to be implemented freely in different level of health facilities such as SIMPUS for primary healthcare centre and SIMRS for hospital. However, some facilities prefer to develop and managed their own system.

There are some referral information systems widely used in Indonesia, such as SISRUTE from Ministry of Health and P-Care from *BPJS-Kesehatan* [1]. If the patient is covered by national health insurance (*BPJS-Kesehatan*), they must use P-Care. Unfortunately, they cannot check the availability of referral hospital from P-Care instead they have to get it from SISRUTE. Both systems are not integrated, therefore the operator in health facilities must inputs the patient data twice. A patient start by getting health examination from first-level health facilities. When the patient need to be referred, they will send him to a referral health facility such as a public or specialty hospital in the district[1]. The first-level health facility gives printed referral letter and medical resume to patient as the output of referral information system. Then, the patient will bring those documents to referral hospital as assigned in the letter. Patient data stored in EHRs system of first-level health facilities cannot be accessed by referral hospital. The hospital will conduct their own examination and stored patient data in their own EHRs system. It might generate gap of patient data that stored in those different systems. Figure 2 describes the process of health referral system in Indonesia.

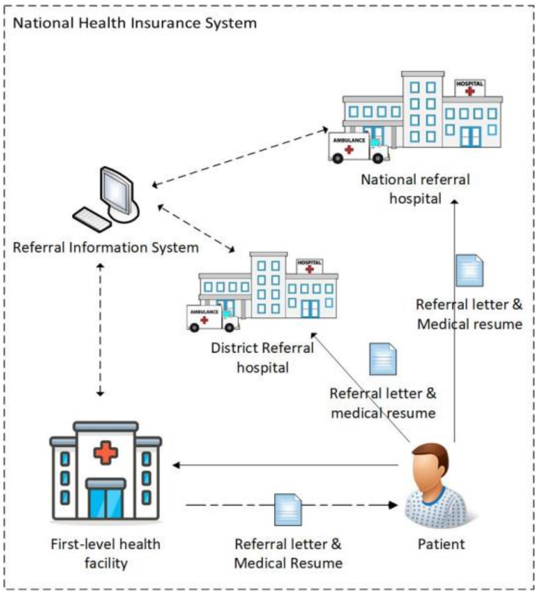

Fig. 2. Health Referral System in Indonesia.

III. RESEARCH METHODS

This study uses a narrative review of several literatures related to blockchain-based EHRs utilized Smart Contract. We use "blockchain" AND "Electronic Health Record" keywords to search the articles in Scopus and Google Scholar repositories. The inclusion criteria are (1) the full text can be accessed by author; (2) written in English; and (3) utilizing Smart Contract.

According to systematic literature review from Holbl et al. [21] & Agbo et al. [2], studies about blockchain applications in healthcare was published since 2016. There are some blockchain-based EHRs applications proposed by previous research with various design and architecture. The pioneer applications designed by Azaria et al. [13] called MedRec that using Smart Contract on the Ethereum Blockchain platform. This concept is similar to FHIRChain [19]; Ancile [18]; and two other applications proposed by Yang et al., [5] and Khatoon [17]. Other commonly used platforms are Hyperledger Fabric Blockchain network [22]; Bitcoin platform [23]; combination of blockchain with digest chain and structured P2P network techniques [24].

In the next sections, we discuss some related works from 2016 until 2020. We take a design from Azaria et al. [13] as a basis to be a comparison of other studies that appear next. We compare some features, such as which stakeholders is involved in the network, mining mechanism, consensus protocol, blocks creation, and contents. Through this review, we expect to determine a suitable design with Indonesian conditions by comparing previous proposed concepts that had been theoretically proofed.

IV. RESULT AND DISCUSSION

A. *Smart Contract for EHRs Application*

A smart contract is a compilation of rule-based declarations written in computer code involving two or more parties [25]. Blockchain-based EHRs utilized smart contracts to represent existing medical records [13]. Like MedRec proposed by Azaria et al. [13], Yang et al. [5] also proposed a smart contract for EHRs. In both concepts, there are two parts in the smart contract. The first part is called Summary

Contract [5], [13] consists of a list of providers who store patient's health record, and the reference to the second part that store more detailed patient-provider relationship, time-stamp, and status. The second part is called Record Relationship Contract [3] or Patient-Provider Relationship [13]. This part stores metadata of a record includes ownership, access policies, contract update status, a value to determine mining bounties, and hashed logs of all read and write events [3], [13].

Dagher et al. [18] divided Smart Contracts into six different types according to the functions performed. They are Consensus Contract, Classification Contract, Service History Contract, Ownership Contract, Permissions Contract, and Re-encryption Contract. Every contract has specific data fields according to their functions and can have interaction to perform specific operations. Meanwhile in FHIRChain [19], Smart Contract store reference pointer to EHRs database as a secure token when providers and patients want to access specific records. In addition to smart contracts, each block also stores other data such as transactions, access control lists, the hash of location data, owner identity, and the hash of previous blocks [17].

Some mechanisms can be applied in the block creation. All logs of events that have happened to the health records, such as read/write of existing records or create new records, will be collected, hashed, and added to the new block [5], [13], [19]. After a pre-agreed update time, the new block will be appended to the blockchain according to a consensus mechanism [3]. All providers extend their blockchain by adding the new block with updated data in Smart Contract. However, not all network nodes will be involved in consensus to create new blocks as miners.

Yang et al. [3] only propose health providers to be registered in a permissioned blockchain. Some of them are authorized to be miners to validate the block, and other health stakeholders are outside the network. The provider selected to create a new block will be granted a certain amount of significance as an incentive. Meanwhile, Azaria et al. [13] propose that miners can be other healthcare stakeholders, such as researchers, public health authorities, etc. Miners can also come from trusted parties in the network consortium [19] or randomly selected using an algorithm as voter nodes [18].

Financial reward can be paid in cryptocurrency like Ether as proposed by previous studies [13], [17], [19]. Azaria et al. [6] also offer access to aggregate health data as an incentive for health stakeholders who finished the task to validate the transaction. Yang et al. [5] proposed a new incentive mechanism using a concept of "significance" as the main factor for selecting the provider responsible for creating a new block. In the beginning, each provider's significance value is calculated according to the records maintained by each provider. Providers who manage more records have higher significance values, which are less likely to be delegated to be miners. After completing a task, the selected provider gets the reward a certain amount of significance. The significance distribution changes with each new block added to the ledger.

Different consensus protocols can be used in blockchain-based EHRs, including one such as Proof of Work, as used on BitCoin. MedRec [13] and FHIRChain [19] use this protocol. Other platforms propose using different consensus protocols such as Proof of Interoperability [5] and the QuorumChain algorithm [18]. Both protocols have similarities where miner selection is based on specific criteria and procedures each time the mining process is carried out. Thus, the miner nodes are not fixed and can be different in each cycle. Yang et al. [5] used the concept of significant value to determine the provider in charge of carrying out the computational process. In comparison, Ancile platform [18] use an algorithm called QuorumChain to determine the voter node as a miner. The block can utilize a specific standard data format where data must conform to structural and semantic constraints to be verified to reach consensus [5], such as FHIR standard in FHIRChain [19]. This can help to overcome the problem of different data formats from various providers.

A transaction in the blockchain is created when a user/provider read or update a record, including the query and the return value [5], [13]. In FHIRChain [19], the transaction also includes events related to exchanging and consuming secure token to access the record. Those events would alter smart contracts based on established authorization policy [17]. Table II summarizes the proposed design from previous research.

B. Design of blockchain-based EHRs for Indonesian Case

The proposed design is similar to blockchain-based algorithms discussed earlier, where health data are stored in two ways, on-chain and off-chain. The provider's database (off-chain) still stores the electronic medical record and other data such as medical images, laboratory results, and so on. While the on-chain ledger only contain data ownership and permission agreements, including references to the patient's records in the database. It is also secured so that even though the data is distributed on the network, the patient’s privacy is protected.

During a patient visit to the health provider many access to the EHR will happen, namely the receptionist who will check the patient's identity; nurses in the nurse station; the doctor who examines the patient; and pharmacist for taking prescription. If the patient uses health insurance, the insurance company also needs access to the patient's EHRs. Most researcher mention that patients themselves do not have access right to the EHRs system directly. When the patient permits to access his medical record, it could be through the medical personal.

For one outpatient visit to health facilities, the medical record will be accessed at least five times (by the nurse, doctor, pharmacist, insurance, and receptionist), so that it needs five transactions to the blockchain. Meanwhile, it needs more transactions for inpatient visits since the doctor and nurse should monitor and update the patient’s condition every day. If we assume that inpatient visits required at least three days, the number of transactions will be three times more than the outpatient visit. According to the number of insurance policyholders from national health insurance in mid-2020, the national health system has coverage of 221.021.174 (221 million) people. If one patient, on average, visits two times a year, the total number is about 442 million visits per year. Based on the national health insurance annual report 2018 in Table II, the number of inpatient visits to health facilities is about 5% from total visits per year. Therefore, the number of inpatient visits will be 22,1 million, and outpatient visit is 419,9 million.

According to Xia et al.[23] the estimation of block size is 679 Bytes, including block data and transactions with size 578 Bytes. A transaction consists of a consensus transaction and user transaction with the total size is 114 Bytes [23]. For outpatient visits, it will consist of five transactions per visit. It will require around 239 GB for storage. Inpatient visit consists of 3 times more transactions than an outpatient visit so that the total storage will be 37 GB. The total storage requirement is 276 GB per year or 750 MB per day on average. Based on the Ministry of Health Regulation No.269 of 2008, health facilities should keep the medical record for five years and medical resume at least ten years since the last day visit. Therefore, it will require storage capacity to keep the transaction around 2.760 GB or 2,7 TB per year.

TABLE II. COMPARISON OF BLOCKCHAIN-BASED EHRS DESIGN

Platform Design	**Blockchain-based EHRs**				
	[5]	[13]	[19]	[18]	[17]
Prototype name	N/S	MedRec	FHIR Chain	Ancile	N/S*
Network type	Private Permissioned	Private	Permissioned	Permissioned	N/S*
Nodes	Health provider	Health provider, patients, researcher, public health authorities	Clinician, healthcare organization	Patient, health provider, third parties (insurance, etc)	Patient, doctor, pharmacy, laboratory, health insurance
Miner	Selected health provider	Health provider or other stakeholders	Some trusted parties in consortium	Voter node (selected by algorithm)	N/S*
Incentives	Significance value	Access to aggregate health data OR crypto-currency	Crypto-currency	Not given	Crypto-currency
Consensus protocol	Proof of Interoperability	Proof of Work	Proof of work	Quorum Chain protocol	N/S*
Block content	2 types Smart Contract represent data ownership and viewing permissions	2 types Smart Contract represent data ownership and viewing permissions	Smart Contract store reference pointer to EHRs database as secure token to access record	6 types Smart Contract that have specific functions	2 types Smart Contract represent data ownership and viewing permissions
Transaction	Events to record (update patient-provider relationship)	Events to record (update patient-provider relationship)	Events related to exchanging and consuming secure token	N/S*	Events to record (altering smart contract)
Patient's access right	Request for health record	Request for health record, change access permission	No access at all	Request for health record, change access permission	Request for health record

*N/S: not specified

Storage Requirement = number-of-visit X number-of transactions-per-visit X total-size-of-transaction

Storage for outpatient = 419,9 million x 5 transaction x 114B

= 239 GB

Storage for inpatient = 22,1 million x 15 transactions x 114B

= 37 GB

Total Storage = (239 GB + 37 GB) X 10 years = 2.760 GB

For performance evaluation, we calculated the total number of inpatient and outpatient transactions per year is around 2.431 million transactions, so it involved 6.66 million transactions per day. For blockchain EHRs in Hyperledger, transaction rate per seconds (TPS) is 50 – 250 with 2 second block time, depends on number organizations and peers involved [22]. Since number of transactions per day is 6.66 million, it only requires around 77 TPS. Therefore, this concept has good enough performance.

Due to the need for processing speed, majority network type in previous researches [5], [18], [19] prefers to use permissioned blockchain. Anyone may join the network after a proper identity check. In permissioned blockchain, not all nodes will perform specific functions, such as to be a miner. The nodes consist of healthcare providers, health insurance, laboratory/radiology, and pharmacy. Patients and health professionals who interact in a health provider will be recorded in the smart contract based on access right consent with the provider. When other parties request for access to their data, patients will get notifications. Access will be granted automatically if those parties already include access to the right consent.

Proof-based consensus algorithm like Proof-of-Work is commonly used in blockchain implementation. As seen in Table II, EHRs system [13] [19] also adopt this algorithm. However, according to Nguyen & Kim [26] and Gramoli [27], consortium and permissioned blockchain more suitable to adopt vote-based consensus algorithm, like Practical Byzantine Fault Tolerance (PBFT). This algorithm is suitable for EHRs system design since node identity are managed, security threat less serious, and less decentralization [26]. Proof-of-Work has some limitation such as network delay, mining power distribution, and double-spending attack that can be minimized using PBFT [27]. Therefore, we proposed to use this algorithm and Hyperledger Fabric as platform that apply this kind of consensus.

A group of specific nodes will be assigned as miners. It is similar to the design of Dagher et al. [18] and Zhang et al. [19]. As mining reward, the stake holders can share the operating cost to be paid to the miners in the form of cryptocurrency. Smart contracts and viewing permissions are store in the blocks, and transactions record all the event related to patient's health care. Table III summarizes the proposed design for blockchain-based EHRs in Indonesia.

V. CONCLUSION

Based on the review of previous studies, we propose a design for blockchain-based EHRs with consideration for some specific needs for developing countries like Indonesia. The proposed system utilizes Smart Contract on Hyperledger Fabric platform that used for operation in defining data ownership and granting access based on viewing permissions. From the best of our knowledge, this kind of research is still rare. This study proposed a design concept that can be used for further research on blockchain based EHR platforms. Based on our calculation, requirement of storage capacity to keep the record for ten years is about 2,7TB with transaction time is 77 TPS. For future work, we recommend to study about acceptance and readiness of this technology in various types of health facilities since they have different conditions and capabilities in providing computation resources.

TABLE III. PROPOSED DESIGN BLOCKCHAIN-BASED EHRS

Network type	Permissioned blockchain
Nodes	Health providers, health insurance, laboratory/radiology, pharmacy
Miner	A group of specific nodes
Incentives mechanism	Cryptocurrency
Consensus protocol	Vote-based consensus protocol (Practical Byzantine Fault Tolerance)
Block content	Smart Contract that represent data ownership and viewing permissions
Transaction	Events happened to record (update patient-provider relationship contract)
Patient's role/access right	Request for health record, change access permission

REFERENCES

[1] P. W. Handayani, I. R. Saladdin, A. A. Pinem, F. Azzahro, A. N. Hidayanto, and D. Ayuningtyas, "Health referral system user acceptance model in Indonesia," *Heliyon*, vol. 4, no. June, pp. 1–33, 2018.

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

[3] S. Khezr, A. Yassine, and R. Benlamri, "Blockchain Technology in Healthcare : A Comprehensive Review and Directions for Future Research," *Appl. Sci.*, vol. 9, pp. 1–28, 2019.

[4] W. Jatrniko, D. M. S. Arsa, H. Wisesa, G. Jati, and M. A. Ma'Sum, "A review of big data analytics in the biomedical field," in *International Workshop on Big Data and Information Security, IWBIS 2016*, 2016, pp. 31–39.

[5] G. Yang, C. Li, and K. E. Marstein, "A blockchain-based architecture for securing electronic health record systems," *Concurr. Comput. Pract. Exp.*, no. Special Issue, pp. 1–10, 2019.

[6] I. P. Chudi, "Healthcare problems in developing countries," *Med. Pract. Rev.*, vol. 1, no. 1, 2010.

[7] A. Pearson and Z. Jordan, "Evidence-based healthcare in developing countries," *Evidence-based Healthc.*, vol. 8, pp. 97–100, 2010.

[8] T. Sitompul, W. Senyoni, J. Braa, and Yudianto, "Convergence of Technical and Policy Processes : A Study of Indonesia ' s Health Information Systems," in *IFIP Advances in Information and Communication Technology*, no. 551, 2019.

[9] N. Azliza bt Nik Ariffin, A. bt Ismail, I. Kamaruddin Abdul Kadir, and J. Iza Ahmad Kamal, "Implementation of Electronic Medical Records in Developing Countries: Challenges & Barriers," *Int. J. Acad. Res. Progress. Educ. Dev.*, vol. 7, no. 3, pp. 187–199, 2018.

[10] T. Justinia, "Blockchain technologies: Opportunities for solving real-world problems in healthcare and biomedical sciences," *Acta Inform. Medica*, vol. 27, no. 4, pp. 284–291, 2019.

[11] M. A. Engelhardt, "Hitching Healthcare to the Chain : An Introduction to Blockchain Technology in the Healthcare Sector," *echnol. Innov. Manag. Rev.*, vol. 7, no. 10, pp. 22–35, 2017.

[12] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "Blockchain platform for industrial healthcare : Vision and future opportunities," *Comput. Commun.*, vol. 154, pp. 223–235, 2020.

[13] 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 MedRec:*, 2016, pp. 25–30.

[14] A. Chib, M. H. Van Velthoven, and J. Car, "mHealth Adoption in Low-Resource Environments : A Review of the Use of Mobile Healthcare in Developing Countries," *J. Heal. Commun. Int. Perspect.*, pp. 1–32, 2014.

[15] G. Kamau, C. Boore, E. Maina, and S. Njenga, "Blockchain Technology: Is this the Solution to EMR Interoperability and Security Issues in Developing Countries?," in *2018 IST-Africa Week Conference (IST-Africa)*, 2018, p. Page 1 of 8-Page 8 of 8.

[16] C. Kombe, A. Sam, M. Ally, and A. Finne, "Blockchain Technology in Sub-Saharan Africa : Where does it fit in Healthcare Systems : A case of Tanzania," *J. Health Inform. Dev. Ctries.*, vol. 13, no. 2, pp. 1–19, 2019.

[17] A. Khatoon, "A blockchain-based smart contract system for healthcare management," *Electron.*, vol. 9, no. 1, 2020.

[18] G. G. Dagher, J. Mohler, M. Milojkovic, and P. Babu, "Ancile : Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, no. February, pp. 283–297, 2018.

[19] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain : Applying Blockchain to Securely and Scalably Share Clinical Data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, 2018.

[20] Y. A. Setyoko and R. Yasirandi, "Security Protection Profile on Smart Card System Using ISO 15408 Case Study: Indonesia Health Insurance Agency," in *6th International Conference on Information and Communication Technology (ICoICT)*, 2018.

[21] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," *Symmetry (Basel).*, vol. 10, no. 470, pp. 1–22, Oct. 2018.

[22] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4 . 0 applications," *J. Inf. Secur. Appl.*, vol. 50, pp. 1–13, 2020.

[23] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS : Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," *Information*, vol. 8, no. 44, pp. 1–16, 2017.

[24] B. Shen, J. Guo, and Y. Yang, "MedChain : Efficient Healthcare Data Sharing via Blockchain," *Appl. Sci.*, vol. 9, pp. 1–23, 2019.

[25] C. G. Harris, "Consensus-Based Secret Sharing in Blockchain Smart Contracts," in *International Workshop on Big Data and Information Security, IWBIS 2019*, 2019, pp. 79–84.

[26] G. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," *J Inf Process Syst*, vol. 14, no. 1, pp. 101–128, 2018.

[27] V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 760–769, 2020.