Blockchain technology for managing an architectural model of decentralized medical record

M Harika¹*, S Rahmadika² and D R Ramdania³

₁ Department of Computer and Informatics Engineering, Politeknik Negeri Bandung, Indonesia
₂ Interdisciplinary Program of Information Security, Graduate School PKNU, Department of IT Convergence and Application Engineering, Pukyong National University, Busan, South Korea,
³ Department of Informatics, UIN Sunan Gunung Djati Bandung, Indonesia

*maisevli@polban.ac.id

Abstract. Medical record (MedRec) of the patient is derived from several healthcare providers i.e. hospital, the national provider, and laboratories which contains personally identifiable information test yet referred to therapeutic procedures and medications of the patient. MedRec has been compiled and maintained by several providers thus resulting in separated and disseminated the data among the parties. Mostly, the MedRecs are stored in provider's database and the patients have no control to manage and access their data. Hence, in this paper, we propose a conceptual model for managing the data of medical record using blockchain technology in the peer-to-peer network with several protocols are embedded in the system. The proposed model aims to facilitate the patients in order to manage their data from various providers into a single view. Blockchain offers the promise of an immutable, single source of truth from multiple sources and facilitates a trust as well as validates an identity without the third-party involvement.

1. Introduction

The health care system that involves the patient and the provider gives many advantages such as efficiency, simplicity, and availability of the data related to the condition of the patient as well as treatment, injury, and any other diseases [1]. The providers come from the health professional parties [2], such as doctors, pharmacist, dentistry, nursing, laboratories, hospital, and to name a few [3]. A MedRec of the patient is derived from several healthcare providers that cause the dissemination of data in the multi-format. Currently, the information of healthcare record is separated and stove piped among the health care providers and there is no mutual standard format or common form of the data. The majority form of the health care system is not fully available for the patient when he/she is in need to access their medical record from the providers. The record used to be separated and stove piped among the health care providers and there is no mutual standard format among the providers. Furthermore, in term of maintaining data is paramount for the industry because in many cases, the providers do not directly share the data with the patient [4].
Figure 1. (a) Centralized, (b) Decentralized, (c) Distributed

In this paper, we propose an architecture model for managing the MedRec data of the patient in the peer-to-peer network using blockchain technology and several protocols applied. The data is divided into several data blocks in the overlay network and it is updated and propagated using blockchain technology. The system makes every health care provider and the patient have the same version of the PHI data in a single format. Whenever the providers upload MedRec data to the storage, it should be confirmed by the miners first to check the record and ensure the validity of the data. Once the transaction is confirmed by the miner, the replica data is propagated to the node in the blockchain network as shown in Figure 1.

The paper is organized as follows. Section II briefly discusses the prior research that related to our work, while Section III elaborates the core components of the model such as blockchain, proof-of-work, and so on. In Section IV, an architecture model of decentralized MedRec is presented. Finally, conclusion and the future work is outlined in Section V.

2. Related works
OmniPHR [3] architecture model faces some challenges regarding PHR contexts i.e., how health care providers can access up-to-date data regarding their patients, even though changes occurred elsewhere. The issue about where patients can maintain their health history. There is no guarantee for security model regarding privacy and integration with other systems and there are several challenges to be worked on and answered, ranging from decisions to flexible the model regarding access rules and data replication. A conceptual privacy is applied for health information by using a wearable device with a distributed mechanism based on cloud server distribution of objects with support for security and privacy with CIA protocol and HIPAA [4]. The model privacy framework is applied on a wearable device but did not focus on the operating system i.e. how the system generates the programs from several health care providers and the way they interact to each other via local or wide-area, and there is no information about the general architecture of the system. The hierarchical distributed electronic health record (EHR) model [5] aims to maintain the patient’s data in the health organization and replicate at the same time to other hospitals in their region, ensuring fail tolerance, but the P2P distribution is a future proposal and topics such as security [6,7], privacy, data integrity are beyond the research.

3. Preliminaries

3.1. Essential of blockchain technology
Blockchain technology can support a new generation of transactional applications and streamlined business processes by establishing the trust, accountability, and transparency that are essential to modern commerce. As it has for centuries, commerce relies on trust and verified identity. The blockchain technology is a data structure used to create a decentralized ledger and composed in a serialized manner [8]. A block of the blockchain contains a set of transactions, a hash value forms the previous block, timestamp, block reward, block number etc.

This technology can prevent fraud and corruption, yet it can be used to solve many other problems depending on how people implement and use it. Establishing the trust and transparency that are essential to modern commerce with the guarantee of security based on several cryptographic protocols [8]. The new block can be added to the blockchain if only the miner successfully solves the hash puzzle (proof-of-work) and reach the consensus for every transaction. Typically, a decentralized system such as
blockchain for the peer-to-peer network, there is no any single failure from a middleman because the system gets rid of the third party to control the system.

One of the prominent examples of decentralized currency by relying on blockchain technology is Bitcoin by using proof-of-work to reach the consensus which miners solve the cryptographic hash puzzle before adding the new block in the blockchain system [9]. The mining process among the miner is like a race, the first one who successfully solved the hash puzzle is the winner and then the result will be propagated to the network until reach consensus before the block is added to the new block.

A bitcoin address is an identifier of 26 to 35 alphanumeric characters and the address is computed from an Elliptic Curve Digital Signature Algorithm (ECDSA) public key for which the address owner knows the corresponding private key by using a transformation based on hash function. The network in peer-to-peer can be connected by default [6]. The peers provide incoming TCP connections (port 8333 for Bitcoin).

![Figure 2. Peer-to-peer (triple-entry) transaction.](image1)

![Figure 3. The nodes and query of an overlay network.](image2)

3.2. Peer-to-peer network

In the peer-to-peer (P2P) overlay network of blockchain system, the fundamental problem is related to the how efficient to find a peer that shares a requested message (how to connect from one node to another node). Similar to the overlay network, it is defined as a network which is built on top of another network in the system of a computer network which allows to detect and recover from disconnection or other disturbance. The node in overlay network can be described such as virtual (see Figure 3) [10] or logical networks that correspond to a path for some purposes. The central idea behind overlay networks is tunnelling e.g. packets in the networks are captured and encapsulated to be forwarded to their actual destinations.

The Chord protocol is also needed in order to support the system to propagate the information of transaction to the entire network. The chord protocol has some characteristic such as simplicity in provable the value and performance context, and only need a few nodes related to the routing overlay [11,12], and manage the information system in join and leave the system context. The chord protocol uses some properties as hash function as follows:

- Pre-image resistance can be defining such as $r = 0, 1^r$ message, $r = H(z)$; $z = H^{-1}(r)$.
- 2nd pre-image resistance, let define by message $z$ to find some: $x^*$ s.t. $H(z^*) = H(z)$. It must be very difficult to find the original value.
- Collision resistance, assume there are two messages $m_1, m_2$ and the probability that their hashes are equal $P(H(m_1) = H(m_2))$ must be very small.
The distributed hash table is needed which is similar to the data structure except that it runs in a distributed system rather than in a single process, and the objects are files which have the unique keys. The concern focus related to the hash table is load balancing, in nutshell referred to each host to have about the same number of objects stored, simply the system applied does not want some hosts overloaded with the objects.

4. Proposed model of decentralized medical record

The component model and architecture in the system consists of the patient, data block and several stakeholders in the same overlay network by relying on the blockchain technology to propagate the personal health record data. We defined the health care provider always give the latest update of MedRec data and propagated into our system by using blockchain technology and several protocols applied. The health care providers in the system are divided into five groups namely laboratories, pharmacy, dentist, clinical psychologist and chiropractor as shown in Fig. 4. The MedRec is also divided into data blocks, it means every healthcare providers will upload and propagate their MedRec data result by relying on blockchain (see Fig. 5) in resulting the patient has the ability to access and get a single look of MedRec data. All of the participants in the blockchain network will acts as miners as well who solve the cryptographic hash puzzle to keep the system running simultaneously even though the miner will not get any reward such as cryptocurrency.

Additionally, what actually happens in the resilient overlay network of our system is a distributed key-value store to exchange the topology information between agents as well as introduce extended virtual network IDs, e.g. a 24-bit VNI in case of VXLAN which is supporting over 16 million virtual networks. Overlay network has an ability for self-organized. For example, when a node fails to form any specific reasons, the overlay network protocol should have some prevent action and solutions to solve that kind of problem such as recreating a proper network for the system.

The overlay network has many advantages such as scalability and there is no single point of failure from the middleman. The overlay network aims to decentralize data and locate nodes on the network, managing the location of PHI data. This kind of mechanism has some certain goals, such as providing distribution, replication, security and data integrity. In the overlay network, the data of PHI is divided into small pieces than later are encrypted before the data is propagated to the rest of node in the network.

The simulation result shows that data sharing with proposed conceptual architecture model by relying on the blockchain technology and several protocols applied has 100% successful rate and propagation delay is negligible. This model architecture aims to facilitate the patients in order to collect and manage their PHR data from various providers and healthcare organizations into a single data view with the

**Figure 4.** Decentralized MedRec data among the parties.

**Figure 5.** Propagating the MedRec data to the network.
guarantee of data integrity. The system model should satisfy the cryptography properties (security manner) such as integrity, availability, and confidentiality.

One of prominent attack that might be occurred in this system is eclipse attack which is kind of attack from an adversary by control and manipulating the network, then make the node only connect with the adversary's node. Eclipsing entails blinding the view of the victim from the blockchain and requires that the adversary isolate the honest node out of the network by monopolizing all of the victim’s outgoing and incoming connections. It can be described when the adversary’s node controls the network and the honest node (βh) has less mining power than the adversary (βa) (βh < βa). The rest of the node has 30% mining power in the same blockchain network. For example, the honest node has 30% mining power, whilst the adversary has 40% mining power and the rest of the honest node (rational miner) has 30% mining power as shown in Figure 6.

Figure 6. Mining power of different pool in the blockchain.

In relation to the architecture model, a component needs future work such as translator component of the data blocks and a service module. This component allows to convert and equalize communications with the heterogeneous health system. Regardless, the proposed system based on the simulations results seems very promising to maintain the MedRec data from several health care providers into a single view. A complexity is also inherent in the system because blockchain technology involves an entirely new vocabulary and for the network size. Although the application can be dependent on other the application theoretically, it is very difficult to tightly couple the application practically.

Selfish mining is also a kind of attack that might arise the blockchain system. Since this attack is discovered in 2014 by Eyal and Sirer [11], it becomes one of the most widely researched topics by the experts in various fields. The selfish mining attack shows that Bitcoin is not incentive-compatible as assumed. The attacker can gain the reward if 0 ≤ α ≤ 0.5. The key idea of this attack is to find the block as fast as the miner can and keeping the block secret which is invisible to the public network and deliberately forking the chain. Selfish mining can gain disproportionate reward in the pool by deviating from the reference client. Even though in this system miner does not get any reward, but we still consider that the attacker still wants to disrupt the network for any reasons in order to control the entire blockchain network for their benefits.

The preimage attack is also called as pre-mined block propagation delay attack in order to overcome the case when the victims are waiting for n confirmation before they are accepting a transaction through the pre-mining and on purposes for delaying propagation of n + 1 created block to generate a fork and make attacker’s blockchain becomes longer than before. This attack on cryptographic hash function is also referred to the activity of the malicious to attack and find the hash value from the message of personal health information data embedded in the system.

5. Conclusion
Blockchain technology combined with several protocols is applied in the system in order to propagate the MedRec data which is derived from healthcare providers. We categorized the health care provider into five groups, namely laboratories, dentist, clinical psychologist, chiropractor and pharmacy which
propagate and generate the key before upload their PHR data in the blockchain network. The simulation result shows that data sharing with proposed conceptual architecture model by relying on the blockchain technology and several protocols applied has 100% successful rate and propagation delay is negligible. The system still needs some of the control function for individual providers to set any configurations once the attack is detected to ensure the credibility of data.

Acknowledgments
Authors wishing to acknowledge Research and Publication Centre of Politeknik Negeri Bandung that supports and funds this research publication.

References
[1] Krawiec R J, Housman D, White M, Filipova M, Quarr F, Barr D, Nesbitt A, Fedosova K, Killmeyer J, Israel A and Tsai L 2016 Blockchain: Opportunities for Health Care Heal. Inf. Technol. 14
[2] IBM Global Business Services Public Sector Team 2016 Blockchain: The Chain of Trust and its Potential to Transform Healthcare – Our Point of View NIST Work. Blockchain Healthc.
[3] Roehrs A, da Costa C A and da Rosa Righi R 2017 OmniPHR: A distributed architecture model to integrate personal health records J. Biomed. Inform. 71 70–81
[4] Safavi S and Shukur Z 2014 Conceptual privacy framework for health information on wearable device PLoS One 9
[5] Xia C and Song S 2013 Resource allocation in HDEHR system based on bi-level multi-swarm PSO 34
[6] Rahmadika S, Ramdania D R and Harika M 2018 Security Analysis on the Decentralized Energy Trading System Using Blockchain Technology J. Online Inform. 3 44
[7] Rahmadika S and Rhee K H 2018 Blockchain technology for providing an architecture model of decentralized personal health information Int. J. Eng. Bus. Manag. 10 1–12
[8] Karame G and Li W 2016 Blockchain Beyond Bitcoin 1–5
[9] Prusty N 2017 Building Blockchain Projects Develop real-time practical DApps using Ethereum and JavaScript (Packt)
[10] Nakamoto S 2013 Bitcoin: A Peer-to-Peer Electronic Cash System 1–9
[11] Doval D and O’Mahony D 2003 Overlay networks: A scalable alternative for P2P IEEE Internet Comput. 7 79–82
[12] Wan C, Tang S, Zhang Y, Pan C, Liu Z, Long Y, Liu Z and Yu Y 2019 Goshawk: A novel efficient, robust and flexible blockchain protocol Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 11449 LNCS 49–69