IJITEB
Vol. 5
No. 1
2023

International Journal of Information Technology and Business

http://ejournal.uksw.edu/ijiteb

Data Security and Privacy on Blockchain Technology

Willson Mangoki[a*]

[a] Magister of Information System, Satya Wacana Christian University, Indonesia

Keywords: blockchain, data security, privacy, healthcare,

Abstract : Healthcare is an aspect that possibly to use of blockchain technology, for example for historical treatment, health insurance and patient medical records. In health services, personal health data will be recorded in the form of a blockchain. This research explains its mechanism and implementation in the healthcare field. On the other hand, this study also discussed the vulnerability caused by the mechanism that applies in the blockchain.

1. Introduction

Digital currency or known as cryptocurrency began to be popularized by Bitcoin. The Bitcoin presence answers the need for a transaction mechanism that does not require a third party as a witness, where transactions are centralized to trusted third parties as applicable in conventional electronic transactions. The main weakness of this centralized mechanism is the possibility of transaction failure, system hacking and system unavailability, in addition to transaction costs and time lags. Cryptocurrency uses a decentralized system, each transaction validated by a computing point (node) in a peer-to-peer network, recorded in the form of blocks that are interconnected and form a blockchain (block chain). The blockchain technology has a similar function to a ledger where each transaction proof will be recorded in each block and cannot be changed. In Cryptocurrency hash functions are used as cryptographic techniques to maintain block integrity. This is one of the main differences between conventional electronic transactions and digital currencies, where transactions based on trust are replaced by cryptographic evidence-based transactions. The first generation of blockchain-based cryptocurrency is like Bitcoin, and modifications and improvements continue to be made in an effort to create another generation of blockhain-based technology. The first implementation of this blockchain technology is called blockchain 1.0. Besides Bitcoin, there are several technologies that use blockhain 1.0 such as Monero [1], DASH[2], and Litecoin [3]. The second generation of blockchain technology (blockchain 2.0) is associated with the introduction of control over proprietary ownership or digital assets based on blockchain (smart properties) and software to regulate how smart properties are controlled and managed (smart contracts) as exemplified by Ethereum [4].

The next development of the blockchain generation (blockchain 3.0) focuses on the application of blockchain 2.0 in the non-financial field [5], [6]. Healthcare does not escape from one aspect of the use of blockchain technology, for example for historical treatment, health insurance and patient medical records. In health services, personal health data will be recorded in the form of a blockchain. Personal health data is a positive object, where security and

* Corresponding authors
e-mail addresses: willson.mangoki@gmail.com

confidentiality must not be known by any party without the consent of the owner of the authority. Keep in mind that one of the working principles of blockchain is distributed or not centralized. Copies of each formed block will be distributed to all connected nodes in the network. In addition, there is a security gap called 51%, where theft or modification of data may occur if hackers can control more than half of the nodes connected in the network. Departing from this, it is important to examine how the mechanisms in the blockchain are applied in health services and how data security and patient privacy are guaranteed by the existence of this technology.

This study aims to discuss the application of blockchain in health services, which are expected to provide a deeper and more scientific understanding of data security and privacy guarantees, especially on personal health data.

2. Blockchain Technology

In research conducted by Cornelis et al [7] used a systematic review method, discussed about the application of blockchain technology in health services. Research describes structurally the development of the blockchain technology which was originally intended for the financial sector, experiencing developments that are likely to be adopted in the non-financial field. The research also identified how much of the blockchain application that has existed to date, case examples that are the object of application and the challenges and limitations faced. In addition, it is also explained that a challenge related to data security and privacy needs to be made which is characteristic of the application of open blockchain-based health services for further research.

Kuo et al [8], in a research related to distributed ladger technology with blockchain for the application of biomedical and health services, introducing blockchain technology, including benefits, loopholes, recent applications, potential threats accompanied by solutions offered in the adoption of blockchain technology.

The focus of this research is to examine the blockhain forwarding in the field of health services that has been investigated to date by looking at it from the perspective of data security and patient privacy as one of the challenges identified in research related to the adoption of blockhain technology.

2.1. Blockchain Component

Details in the blockchain technical are important to discuss in the scope of this research. By understanding the blockchain concept is closely related to data security and privacy which is the main focus. With blockchain technology that is intended for finance which is then adopted in the health sector, it is necessary to understand the procedure and its constituent elements, and how modifications and improfisations are carried out.

The main advantage of the blockchain discussed earlier is the fact that this technology removes the need for trustworthy third parties. Generally in the blockchain there are 2 main components as follows [9]:

- Transaction: Representation of actions triggered by participants.
- Block: A block in a blockchain is a set of data that records transactions and everything that is associated such as workflow timetable, proof of work, and so on.

In a block there are several layers as follows [10]:

- Data: Depends on the service where the blockchain is applied, for example transaction records or medical records.
- Hash: When a transaction is recognized, a hash code will be formed that will be distributed to all nodes, formed by a function called the Markle Tree.
- Timestamp: When a block is created.
- Other information: Such as block signatures, nonce values, or other data described by the user.

To run the operation, first the user will initiate transactions, transactions. Transactions recorded are then distributed to all connected nodes, for validation and verification.

Verification and validation involve the Consensus method, in the form of approval of messages from the majority of nodes in the community. When approval is made, there are several protocols that will be used such as proof-of-work (PoW) and proof-of-stake (PoS). PoW involves the cost and time spent so that in the process it will consume considerable power and computing power [11], while PoS compares the values that are owned by a node with 1% other nodes [12]. Furthermore, if all nodes in the community have agreed, a new block will be formed by including the hash of the previous block. The block is then associated with an existing block that forms a blockchain. The process of forming a blockchain can be seen in Figure 1.

Fig. 1. Blockchain operations

2.2. Types of Blockchain

The use of blockchain is tailored to the services that are applied. This type of service for applying blockchain determines the access sensitivity of nodes in a community. Based on node access rights, the blockchain is classified into 3 types, namely:

- Public Blockchain; where everyone can check transactions and verify them, and all nodes can participate in consensus..
- Blockchain Consortium; where access or authority of a node can be determined based on certain kerja.
- Private Blockchain; where access will be limited to a blockchain, and not all nodes have the same authority to access data.

3. Blockchain on Healthcare

As explained earlier, the blockchain has great potential to be developed in applications in various fields, one of which is healthcare. In this study, various available sources were collected using Google Scholar to help find references that are relevant to the existing discussion. Search uses the query search technique so that search results are more specific and match keywords. The keywords used in search are blockchain, healthcare, and e-health.

The application of the blockchain concept in the healthcare field has been studied in several studies, both of which specifically discussed [7] as well as explaining various fields in general [13]. In the field of healthcare, in previous research [14], blockchain applied fields in healthcare has been identified, include: 1) data sharing, 2) health records, 3) access control, 4) audit trail, 5) supply chain, 6) others. In addition, a blockchain based application was also stated [15][16] [17] where the application can be done on platform devices. In terms of media itself, blockchain-based data storage can be used by several options such as distributed storage [9] or either cloud networking [18].

After reviewing these studies, several identical concepts can be generalized related to blockchain development in the healthcare field. There are 3 parties involved in forming the blockchain "community" namely patients, healthcare providers (HC), and communities (miners / nodes in the network / relatives of patients) who are on the type of blockchain adopted. From the research that has been developed, some concepts of the application of blockchain are obtained in healthcare applications. As seen in Figure 2, a brief description of how to access data on the blockchain containing medical records is given.

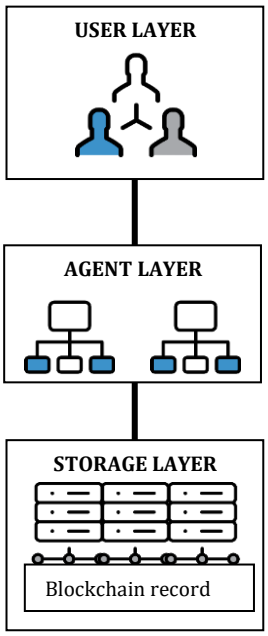

Fig. 2. Access model HC Blockchain-based Concept

The user layer represents data accesses such as doctors, patients, and analyst data. The user initializes the access request for the medical records contained in the storage layer. This request will be processed through the agent layer. Layer Agent checks the user's access rights to a block, where only users who are declared to have valid access rights can access the data. At the storage layer, all medical records will be recorded in the form of a blockchain. This overlay function is to provide the requested data via the agent

layer. For the agent layer and storage layer to be connected in a cloud-network.

The application of blockchain to healthcare in addition to the security aspect which is considered better, is also intended to reduce the cost and time of administration for doctors so that more time is available for patients and discussion about patient health data. Note that to access and share the patient's medical record takes a long time [19].

4. Discussion and Conclusion

4.1. Security and Privacy

The authors should ensure that every reference cited in the text is present in the reference list and every reference in the list should be cited in the text. The reference should be numbered in the order of their appearance in the text.

The security aspect of the blockchain is very dependent on the intended application to be achieved. The part of the blockchain adopted in previous research includes storing data to a patient in the form of a block, which is then placed on a cloud-based storage service. Furthermore, a patient's medical records based on the results of the medical record will be entered as data in a block. To validate a new block, it involves a number of nodes that are part of the community.

The security of this patient data is protected by a mechanism provided on the blockchain such as hashing where medical records that have been made can be ascertained the authenticity and correctness, and protect against the threat of data manipulation. It should be noted that this data has been distributed to nodes in the network so that to change the contents of a block need to change the copy that is owned by the majority of existing nodes. Furthermore, a new block containing medical records cannot be connected to the previous block if there is manipulation which then changes the hash value of the previous block recorded in the block. To protect the confidentiality of existing data, the PKI mechanism can be used for the confidentiality of a patient's identity. Furthermore, this mechanism will be discussed in the protection of patient privacy.

However, protection mechanisms such as hashing and PKI do not guarantee that the patient's medical records will be completely safe from intruder threats. Some of the threats that may arise over the application of this blockchain include cooperative attacks caused by the existence of a consensus mechanism. The attack in the form of tempering the content in the block is very possible with the majority agreement of the node (51%). To prevent this, consider the type of blockchain that will be applied, which will greatly affect the access of each node on a block. Then the problem that then arises is the user's privacy in this case the patient. The identity of a patient or owner of a block can be exposed, it is possible by analyzing network traffic or blockchain itself, because it is public [20]. Related to the use of cryptographic mechanisms on the blockchain, it still needs to be reviewed in the future considering the development of computing devices at a more advanced level so that it is not impossible to use machine learning in solving decryption.

4.2. Conclusion

Blockchain as distributed lagder can be a solution for technology development in the healthcare field. This will speed up the process of access and sharing of patient medical data for doctors. In addition, this can also reduce the administrative costs that must be incurred for making a medical record document. In terms of patients also benefit from access to their own health records.

For overall application, the security aspect needs to be a major concern considering patient data that is confidential and sensitive. Restricting access to a block can provide a solution to a problem that might be caused by a transparency system in blockchipers. Furthermore, the type of blockchain used needs to be reviewed before its application in order to reduce the risks that can be caused by existing mechanisms such as consensus.

For future research, further studies are needed regarding the use of storage-networking that has not been discussed in this paper.

References

[1] “The Monero Project.” [Online]. Available: https://getmonero.org/the-monero-project/. [Accessed: 06-Jul-2019].

[2] “Dash Official Website|Dash Crypto Currency—Dash.” [Online]. Available: https://www.dash.org. [Accessed: 06-Jul-2019].

[3] “Litecoin—Open Source P2P Digital Currency.” [Online]. Available: https://litecoin.org. [Accessed: 06-Jul-2019].

[4] “Ethereum.” [Online]. Available: http://ethereum.org. [Accessed: 06-Jul-2019].

[5] J. Yli-huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where Is Current Research on Blockchain Technology ?— A Systematic Review,” pp. 1–27, 2016.

[6] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain Technology Innovations,” 2017.

[7] C. C. Agbo, J. M. Eklund, and Q. H. Mahmoud, “Blockchain Technology in Healthcare : A Systematic Review,” *Blockchain*

Technol. Healthc. A Syst. Rev., 2019.

[8] T. Kuo, H. Kim, and L. Ohno-machado, "Review Blockchain distributed ledger technologies for biomedical and health care applications," *J. ofthe Am. Med. Informatics Assoc.*, vol. 24, no. September, pp. 1211–1220, 2017.

[9] M. H. Miraz and M. Ali, "Applications of Blockchain Technology beyond Cryptocurrency," *Ann. Emerg. Technol. Comput.*, vol. 2, no. 1, pp. 1–6, 2018.

[10] I. Lin and T. Liao, "A Survey of Blockchain Security Issues and Challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

[11] S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," 2008.

[12] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros : A Provably Secure Proof-of-Stake Blockchain Protocol," 2019.

[13] E. Karafiloski, "Blockchain Solutions for Big Data Challenges A Literature Review," no. July, pp. 6–8, 2017.

[14] M. Hölbl, M. Kompara, and A. Kamišali, "A Systematic Review of the Use of Blockchain in Healthcare," 2018.

[15] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications."

[16] L. C. B and V. Cinque, *Blockchain-Based Logging for the Cross-Border Exchange of eHealth*. Springer International Publishing, 2018.

[17] 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*, 2016, pp. 25–30.

[18] C. Esposito, G. Tortora, H. Chang, and R. Choo, "Blockchain : A Panacea for Healthcare Cloud-Based Data Security and Privacy ?," no. February, pp. 31–37, 2018.

[19] M. Jabed, M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "Blockchain versus Database : A Critical Analysis," in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 1348–1353.

[20] M. Conoscenti, D. Torino, A. Vetr, D. Torino, and J. C. De Martin, "Blockchain for the Internet of Things : a Systematic Literature Review," 2016.