Chapter 7

Workshop on Blockchain Use Cases in Digital Health

Philip Christian C. Zuniga, Rose Ann C. Zuniga, Marie Jo-anne Mendoza, Ada Angeli Cariaga, Raymond Francis Sarmiento, and Alvin B. Marcelo

Abstract We present in this chapter discussion of how blockchain can be used in Digital Health. Benefits and risks of using blockchain were presented. Guide questions with sample answers are also presented to deepen the discussion of the topic. At the last section of the chapter, several use cases on how blockchain is used in Digital Health are presented.

Keywords Blockchain · Cryptography · Data security · Data trust

Learning Objectives

- (1) Describe how public and private blockchain works
- (2) Propose and evaluate blockchain use cases in healthcare

7.1 Introduction

Blockchain technology has been known since the early 1990's through the work of Stuart Haber and W. Scott Stornetta. In their work, *How to Time Stamp a Document* (Haber and Stornetta 1991), the authors propose a methodology to time stamp document using cryptography to prevent counterfeiting of crucial documents. The first real implementation of blockchain was done by Satoshi Nakamoto in 2008 (Nakamoto 2008). His work was focused on using blockchain in cryptocurrencies.

Blockchain revolves on the idea of having a decentralized system of storing data, where each participant/node will have a copy of the ledger of transactions done. By doing so, it will be impossible for someone to alter data in the blockchain without informing other participants. This also eliminates the need for a centralized system that handles all the data since all participants would have their own copies (Zheng et al. 2017). Usually, blockchain is very useful in scenarios where there is a strong centralized entity. In this work, we discuss how blockchain can be used in Digital Health.

P. C. C. Zuniga (✉) · R. A. C. Zuniga · M. J. Mendoza · A. A. Cariaga · R. F. Sarmiento · A. B. Marcelo
Standards and Interoperability Lab-Asia, Mandaluyong City, Philippines
e-mail: phil@sil-asia.org

Blockchain is expected to change the way how Digital Health is done. Digital health implementations rely heavily on centralized systems. This can be seen in the need to validate data, in having a regulatory body and in securing patient data. All of these can be transformed by blockchain. In a survey made by the *European Coordination Committee of the Radiological, Electromechanical and Healthcare IT industry*, several areas are identified to be a good pilot use case for blockchain (COCIR 2017).

- (1) Supply Chains
- (2) Drug Verification
- (3) Claims Reimbursement
- (4) Access Control
- (5) Clinical Trials

In this workshop, we will present a framework on evaluating blockchain use cases and examine whether the above-mentioned use cases would also be able to pass the evaluation parameter. We will also present a sample use case for a personal health record system using blockchain.

7.2 A Discussion on Blockchain

There are two main important ideas in blockchain.

1. Blockchain consists of a list of blocks that are cryptographically linked with one another.
2. All participant nodes in the system have a copy of the blockchain.

Each blockchain block generally consists of three main parts: [1] the transaction data, [2] the hash of the previous block and [3] the hash of the current block. Each block is connected since every block contains the hash of the previous block hence would have a way to access the previous block. Instead of storing the blockchain in a single centralized node, copies of the blockchain are distributed to each participant nodes. Participants can add a block, and this block will also be added to the copies of other participants.

Because of these properties, blockchain is immutable. Any modification done on the blockchain will change the hash values of the succeeding blocks, and all the changes in the hash values should be reflected in the copies of the participants. The immutability of the blocks in blockchain ensures that the data saved are authentic as stored by the participant. However, this does not ensure that the correct participants will send the correct data. Blockchain works on this issue either by making other participants validate the data submitted by one participant or by only allowing authorized participants to store data in it.

Blockchain can be categorized as *public* or *private* blockchain. For public blockchains, anyone can send data to the blockchain, but this data will need to be validated by other participants. Private blockchain on the other hand is a limited form of blockchain as only a select member can send data to the blockchain. Another category for blockchains, which is also similar to the earlier classification are permissioned and permissionless blockchain. Permissioned blockchain requires certain permissions before a participant submits a data on blockchain. A permissionless blockchain on the otherhand allows participants to add data to the blockchain without the necessary permissions. In usual blockchain models, public blockchains work with permissioned models, since everyone can add data to the blockchain, and thus permissions must first be checked if the data can be added. On the otherhand, private blockchains usually work with permissionless blockchains, since there is an assumption that users in private blockchains are already authenticated and authorized, hence no additional validation step is done.

Guide Questions:

- (1) What benefits of blockchain can be used to leverage against Centralized Systems?
- (2) Are there any trade offs in using blockchain?
- (3) What are the advantages/disadvantages of permissionless/permissioned or public/private blockchain?

Suggested Answers:

- (1) Three benefits can be identified when using blockchain as compared to Centralized systems. Blockchain does not require back-ups since every participant have a copy of the chain. It is not a single point of failure component, and there is no single source of truth.
- (2) The main trade off in using blockchain is the computational overhead due to the need to synchronize data with other participants. If validation of data is needed (i.e. Proof work/Proof of stake) then it will add significant computational overhead too.
- (3) There is less computational overhead when using permissioned or private blockchains since the validation stage can be removed. There are also less participants since these participants would require authentication/permission credentials. Public/permissionless blockchain allows everyone to push data to the chain. This is more open; however, validation of data will still be required.

7.3 When to Use Blockchain?

Blockchain is a solution that can solve many issues in data management and data storage. However, it is not a solution to every problem. There are overheads to using blockchain, and it is important that its used is maximized to make it a viable alternative to existing systems. In this section, we will present some properties of a use case that will benefit greatly from blockchain.

1. Data sharing is required. A blockchain based approach is viable if the use case requires participants to share data to other entities. Data sharing allows the content of the data to be validated and authenticated by other users. Since data is immutable in blockchain, it will be easier for the receiving entity to validate the data since there is a presumption that this data was not altered illegally.
2. Multiple parties modifying a single database. Another use case property that benefits from blockchain is when multiple parties need to modify a single database. Since modifications done in blockchain are broadcasted to all participants, the data provenance is kept and recorded.
3. Trust on the data. Given that data is shared and multiple parties modify the data, it is important that participants can still trust it. Without blockchain, it will be not inherent for the data integrity to be maintained, and additional steps are needed to ensure the integrity. In blockchain, given that there are ways to validate the data or authenticate the participants first, data stored in the blockchain can always be assumed as true. Also unlike existing systems where a centralized database becomes the single source of truth, in blockchain, any copy of the chain that is with any of the participants can be a trustworthy source of truth.
4. Security is of utmost importance. Use cases where security is important benefits greatly in blockchain since data may be encrypted (data privacy), it may not be modified without informing other participants (data integrity), and participants need either to prove validity of data (authentication) or would need to have the proper credentials before submitting data (authorization).

Guide Questions:

- (1) Will a general healthcare workflow of sharing of patient data benefit from blockchain?

Suggested Answer:

Usually, healthcare workflows require multiple parties accessing and modifying patient data. This may include: doctors, pharmacists, nurses, lab technicians, and even insurance providers. Patient data can also be shared to multiple entities either as individual data (i.e. insurance) or aggregated with the population (i.e. disease surveillance). Also, validity/correctness of the data is important as practitioners should believe that data written by other doctors on the patient's well being is correct. Or insurance agencies must be able to confirm that the medical abstract provided by doctors truly reflect the status of the patient.

It is also important to note that health data is currently the most prized data by hackers. Recent studies have valued the cost of a single health record to up to 400 USD, [5] and this is higher than the per record cost of financial or commercial data. This implies the need of securing health data.

Given how current health care information systems work, and given the trend where patient data is shared across different stakeholders, it follows that blockchain

is really something that can improve how health information systems, particularly health information exchanges, work.

7.4 Challenges in Using Blockchain

Despite the benefits obtained in using blockchain, there are still many identified challenges, both technically and legally, in using blockchain. The following are the primary challenges:

1. Scalability Issues

Since increase in the number of participants lead to increase in the number of transactions, scalability has been one of the leading issues in the use of blockchain. It is projected that there is an exponential growth in the number of transactions in Bitcoin. The scalability issue in blockchain stems from the fact that each participant receives a copy of the blockchain hence an increase in the number of participants increases the number of transactions and the number of blockchain copies that need to be updated every time a new transaction is made.

2. Data Migration

Using blockchain is premised to an assumption that the data that will be used are already in digital format. Migrating from a system that is totally manual is a lot harder when the migration is towards a blockchain based solution as data will need to be structured such that it can be processed by blockchain.

3. Registration of New Participants

Another premise in blockchain use is that all participants in blockchain must have a copy of the chain. This will create additional complexity when participants (either facilities, health workers or patients) are added to the chain since they would need to download all the data in blockchain to have an updated copy. This challenge is also a direct effect of the scalability issue in blockchain.

4. Security

Another implication of the property mentioned in the earlier challenge, is that since everyone has a copy of the blockchain, eventually it will be easier to hack on someone's blockchain copy. Instead of having a well-funded third party to attack, data hackers can hack on individual holders of blockchain records.

5. Data Protection Regulations

Many countries have adapt a data protection regulation pertaining to the right of individuals to request for a deletion/revision of their records stored in digital and non-digital media. Examples of these data protection regulations are the Data Protection

Act (Philippines) or the General Data Protection Regulation (GDPR) in Europe. These provisions are somehow opposite to blockchain's immutability property. Data protection regulation is seen as one of the biggest challenges to blockchain use.

Guide Questions:

- (1) Are there technical work-around to the immutability property of blockchain versus the right to be deleted by persons?

Suggested Answers:

- (1) Two possible ways of working around on this issue are
 - a. Participants don't store personal data in blockchain, but rather just use the chain as index to where the actual data are stored. Actual data may be stored in normal databases with CRUD functionalities.
 - b. Another possible workaround is the thrashing of data. Blockchain data are encrypted and if a person wants to delete or make his/her data useless, then a key destruction mechanism can be done, where the key that was used to encrypt the message will be destroyed, or be rendered useless. Once this is done, then the data stored in the blockchain will be practically unreadable.

7.5 Blockchain Use Cases in Health Care

In this section, three use cases of blockchain in Healthcare will be presented. For each use case, guide questions will be provided.

Use Case 1: Simple EHR Workflow

In a single health facility, all health transactions are uploaded to the blockchain. Using smart contracts, the designated personnel will be informed if a particular task is assigned to him. Example:

- (1) Doctor X requests for an X-Ray on Patient Y from Radiologist Z.
- (2) The request is stored in the blockchain
- (3) Radiologist Z is informed that such a task is assigned to him.
- (4) Radiologist Z performs an X-Ray on Patient Y
- (5) Radiologist Z stores result of X-Ray in blockchain
- (6) Doctor X is informed that the result is already available.

All the transactions are stored in the blockchain. Transactions are stored in the blockchain because there are many participants that are modifying the health/medical records of a patient.

Guide Questions:

- (1) Who are the participants in the blockchain?
- (2) What kind of blockchain design can be used?
- (3) What are the potential issues in this design?

Suggested Answers:

- (1) The participants of the blockchain are the different health providers in a facility. All participants should have a copy of the blockchain.
- (2) A private/permissionless blockchain may be used since the health providers in the facility is a controlled population, and authentication credentials can be easily provided.
- (3) The biggest issue with this design is that actual health data is stored in the blockchain. Another potential issue is scalability since all transactions done in the hospital will be recorded in the blockchain hence increasing its length.

Use Case 2: A Health Maintenance Organization (HMO) Claim Blockchain Workflow

In this workflow, there will be 5 identified transactions:

- (1) Facility and HMO agrees to a contract of service
- (2) Patient is enrolled in HMO
- (3) Service is rendered by Facility to the Patient
- (4) Facility makes a Claim from the HMO
- (5) HMO pays claim.

Smart contracts can be assigned in the process. An example of smart contract use is to check whether there is an existing contract of service between the HMO and the Facility, and whether a patient is enrolled in an HMO, and whether service is provided to the patient, whenever a facility makes a claim from an HMO.

Guide Questions:

- (1) Who are the participants in the blockchain?
- (2) What kind of blockchain design can be used?
- (3) What are the advantages of using blockchain in this workflow?
- (4) What are the potential issues in this design?

Suggested Answers:

- (1) The participants are the facilities, HMOs and the patients. Each may not need to have the contents of the whole blockchain (patients won't need the transaction nodes that are attributed from other patients).
- (2) Since patients are participants, a public blockchain may be used. But since patients won't push data to the blockchain, it is possible that a permissionless blockchain is used since facilities and HMOs would need to be pre-registered/provided with authentication credentials before submitting data to the blockchain.
- (3) Blockchain provides more sources of truth, and can be used offline. This is because all participants have a valid copy of the chain, it is easier to validate the truthfulness of transactions (rather than having a central entity to validate).
- (4) Scalability will be a big issue since the chain will contain transactions by all patients in the locality,

Use Case 3: Design for a Patient Centric Health Information Exchange using Blockchain

In this workflow each patient will have his/her own blockchain recording all the transactions done in a health facility or with a healthcare provider. The blockchain will not store his/her health records, but rather it will only keep a pointer to the location of the associated health record. The health records will be kept in the Health facilities. Health facilities as participants in the blockchain will have a copy of the blockchains that are assigned to the patients.

Guide Questions:

- (1) Who are the participants in the blockchain?
- (2) What kind of blockchain design can be used?
- (3) What are the potential issues in this design?
- (4) Will the design scale up?

Suggested Answers:

- (1) Patients, facilities (where the patients have been seen) are participants. Each patient has his/her own blockchain. Facilities have the blockchain of all patients that were seen in the facility.
- (2) A private/permissionless blockchain may be used since each patient would be given credentials to his/her own blockchain, and facilities would have permissions when submitting data.
- (3) The actual sharing of health data may be an issue since health data is not in the blockchain
- (4) The design will scale up, since a blockchain will only increase in length, as a patient goes to a health facility. It is not expected that a lot of transactions will be stored in a chain since on average a person goes to a health facility only around 7 – 10 times a year. For each person, this amount of data is manageable.

7.6 Conclusion

Blockchain is seen as the most important technology that has been developed after the internet. It is set to change how data are stored and secured. As shown in this chapter, Healthcare is one of the areas that would benefit from blockchain. It has been discussed how the various properties of Healthcare use cases can fit into blockchain. But, despite the promises and the benefits of using blockchain, it is also quite noted that there are existing challenges. It is thus crucial that, before any blockchain solution is implemented, a suitable design and architecture phase must be first performed.

Acknowledgements SIL-Asia is powered by the Asia eHealth Information Network with support from the Asian Development Bank. The funds of the **laboratory** primarily came from the People's Republic of China Poverty Reduction and Regional Cooperation Fund. Additional support was provided by the World Health Organization, the Norwegian Aid Agency and UNICEF.

References

- European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry. (2017). Beyond the hype of blockchain in healthcare, *COCIR*.
- Haber, S., & Stornetta, W. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3.
- Healthcare Data Breach Costs Higher than Any Industry. (2017). Retrieved February 20, 2019, from <https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/>.
- Nakamoto, S. (2008). Bitcoin a peer to peer electronic cash system. *Cryptography Mailing Lists*.
- Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, *Consensus, and Future Trends*. <https://doi.org/10.1109/BigDataCongress.2017.85>.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.