Mitigate Long-lasting Ethical Issues in the Healthcare Industry with Blockchain-based Solutions

Tongxin Li *

Khoury College of Computer Sciences, Northeastern University, Boston, MA, United States

* Corresponding author email: li.ton@northeastern.edu

Abstract. As one of the most promising innovations in the recent computing paradigm, blockchain technology has been introduced into many fields such as finance. With the outbreak of the epidemic and the intensification of the global public health crisis, medical care has also undergone rapid revolutionary changes in replacing traditional systems with new technologies. Among them, the ethical issues exposed in the process of transformation are under intense debate. Traditional research and surveys focus on the privacy of patient data management and only include some roles in the medical ecosystem, which cannot meet the existing needs. To this end, based on system thinking, this paper studies blockchain technology and emphasizes its application potential in the field of health care to alleviate some long-standing ethical problems, mainly including manipulation of organ transplantation, counterfeit drugs, and medical insurance fraud. It also discussed the technical challenges and limitations of the implementation of the blockchain-based system and ended with the possibility of reimagining the future.

Keywords: Blockchain; Healthcare; Security; Data Privacy; Smart Contracts; Ethics; Supply Chain.

1. Introduction

The healthcare industry is an ecosystem that includes not only patients and care providers but also other stakeholders interacting and interoperating simultaneously. The complexity of it and the conflict of interests within it create not only efficiency and financial controversies but also leave long-lasting ethical problems to be solved. In this paper, three major ethical issues in the healthcare sector will be discussed: rigged organ transplants, counterfeit drugs, and health insurance fraud. According to a report from WHO, nearly 10% of the organs being transplanted are from the black market and organ trafficking [1]. Conventionally, an organ bank relies on a central database to register patients, donors, and hospitals, manage the records and handle the matching process. The problem with keeping all the sensitive information in one place is that the security and availability of the data are completely relying on the security level of the system. The data could be exposed or tampered with easily by hackers or fraudulent employees [2]. Moreover, the lack of transparency in the system facilitates unethical and criminal activities in the purchase, donation, and matching processes. Also, hospitals might ignore the prioritization list and instead offer organs to the person who is willing to pay the highest [3, 4]. Aggravated by the COVID-19 pandemic, the problem of counterfeit drugs makes drug traceability one of the biggest concerns among current ethical issues [5]. Recent research from Health Research Funding Organization shows that up to 30% of the drugs in the market of developing countries are counterfeit, and according to WHO, in most cases the victims of counterfeit drugs are children [6,7]. Counterfeit drugs entering the market attributes to the complexity of healthcare supply chain, as those drugs could be easily traversed across the distribution channels and among stakeholders without valid documentation [8]. It is rudimental, therefore, to monitor, trace, and control counterfeit products across the healthcare supply chain.

The traditional Health Insurance Claim (HIC) procedures are usually based on legacy computer systems and therefore problematic in terms of transparency and privacy. Since managing records is extremely error-prone and vulnerable to cyber-attacks, fraud occurs when the data itself is easily accessed and altered by unwanted entities. Moreover, as the range of data collected by insurance providers expands, the Health Insurance Portability and Accountability Act (HIPPA) no longer protects from HI providers' unwanted access people's personal health data in fitness applications or

wearable devices like Apple Watch [9]. It leads to concerns because subscribers are gradually losing control over the collection and use of their personal data [10]. Reimaging a new way to detect health insurance fraud is therefore prominent because people's Personally Identifiable Information (PII) could be damaged if the HIC system is exposed to security and privacy issues.

2. Blockchain Technology

2.1 Types of Blockchain

Blockchains could be classified into three categories: public, private, and consortium. Public blockchain provides a fully transparent environment by enabling any person in the network to become a node in the network and access transaction records in the public ledger [11]. Private blockchain, on the other hand, only consists of users authorized by the administrator of the network. Private blockchain is considered more desirable for healthcare providers because it provides a higher level of data privacy and availability. Consortium blockchain combines features from both public and private blockchains.

2.2 Consensus Mechanisms

Transactions are verified and appended to the main network of the blockchain using consensus protocols. One of the commonly used protocols is Proof-of-Work (PoW), a secure algorithm that requires miners to solve a complicated puzzle and whoever wins gets to append the block to the main blockchain network and receive bitcoin reward [12]. The problem of PoW is that it requires large computing power, which leads to a lower processing speed and a high level of energy consumption [13]. An alternative is Proof-of-Stake (PoS), where the possibility of a user earning the permission is corresponding to the number of assets in their wallet. It does not include any puzzle competition, but it is considered more suitable in cryptocurrency applications than healthcare organizations [14].

2.3 Characteristics

Blockchain is a decentralized, immutable network that stores a series of verified transaction data in chronological order. The decentralization of blockchain eliminates a central server and distributes authority among all users in the network, therefore improving the overall service availability of the system. Blockchain also ensures immutability because it stores the transaction data permanently and prevents any user from editing the data. It uses hashing functions, asymmetric key cryptography, and digital signature to verify the integrity of each transaction, which adds another level of data integrity to the system. Smart contract is another feature introduced by Ethereum, allowing developers to implement predefined functions in the main blockchain network, which could be automatically executed later [15]. It eliminates intermediaries and creates opportunities for a more customized, efficient blockchain network, which is promising in not only financial sector but also non-financial sectors such as healthcare [16].

3. Applications of Blockchain in Healthcare

3.1 Organ Transplant

Adopting a blockchain-based organ bank system based on the private Ethereum blockchain could be a more secure and ethical alternative for organ bank system in the future. The blockchain-based system ensures the integrity of the organ matching process because each transaction, in this case the organ transplant request being added to the priority list, is recorded in the immutable ledger, making sure that organ will be given to the person who is on the top of the list. Smart contract provides a higher level of accountability. It assigns roles for different participants so that only organ matching professionals could operate on the priority list, and only transplant sergeants could run the transplant

procedures. Because any abnormal or illegal activity is completely traceable and stored in the immutable ledger as events, all participants take responsibility for their own actions.

The decentralization of the private Ethereum blockchain ensures network availability, which is important especially for an organ bank that needs to respond to a possible organ donation case within 15 minutes any time of the day [17]. Having multiple distributed nodes logging events and activities in the network, one node being attacked by hackers will not interrupt the overall workflow of the organ bank. Given the authentication feature of blockchain, every transaction would need a digital signature from the sender to verify their identity. It would significantly decrease the possibility of Man-in-the-Middle (MITM) attack because the attacker would not be able to access or tamper with the data without being verified or trusted by the organ transplant system.

3.2 Drug Traceability

The blockchain-based drug supply chain would mitigate the problem of counterfeit drugs and improve the accountability, integrity, and quality control of the existing network. By tracking and storing all transactions in the immutable ledger in Ethereum, any suspicious activity during the distribution process would be traceable, and any actor would be held accountable for their actions: drug manufacturers would be responsible for the drugs they produced, and pharmacies would be responsible for every prescription they prescribed, as the log in the blockchain-based system would be able to show the source of the drug obtained by the patient. To minimize human intervention and interest conflicts among various stakeholders in drug supply chain, the smart contract in the system ensures that certain features or operations could only be executed by authorized users. Avoiding unauthorized access and preventing unwanted entities from executing the stored functions are crucial to the healthcare supply chain, especially the fight against counterfeit drugs, because only verified manufacturers can produce drugs and only verified pharmacies can prescribe them to patients.

Because the initiator of a transaction encrypts their message with a private key, and it is considered to be impossible to deduce a private key from a known public key, the transaction itself would not be accessed by attackers, and any attempts from unknown entities to alter that transaction would not be approved. In the case of blockchain-based healthcare supply chain, anyone who attempts to produce or distribute counterfeit drugs in the name of a verified manufacturer would no longer be able to do that.

3.3 Health Insurance

Blockchain- and AI-based health insurance fraud detection system could be used to mitigate security issues and rebuild trust among insurance providers and subscribers. Given the decentralized framework of blockchain, the system is decoupled from a central server, and it supports distributed Health Insurance Claim (HIC) procedural operations [18]. The cross-node ledger creates a transparent environment and shares the insurance data among all authorized participants within the network [19]. One of the demands of HIC is to prevent alteration of the insurance data, and blockchain satisfy the demand by its underlying feature of immutability. More importantly is to protect the integrity and privacy of subscriber's personal, sensitive data. Not only blockchain encrypts their data through cryptographic technology, but it also allows the exchange of data among parties without revealing patient's identity because their identity is pseudonymized using cryptographic keys [18].

The system also supports smart contract, written as executable function and deployed on Ethereum. Used in identity authorization and insurance payment, the smart contract will be executed as soon as the transaction commits, following standard procedures. It adopts consensus such as Proof-of-Work (PoW), Proof-of-Stake (PoS) and Proof-of-Burn (PoB) to verify each transaction and input, preventing data tampering and allowing insurance subscribers to control their own HIC records and how they are being shared and collected.

4. Challenges and Limitations

Despite the benefits of blockchain technology and its positive implication on the healthcare industry, it is important to discuss its limitation and potential consequences of its implementation to better understand its practical value.

4.1 Immutability

Blockchain secures the data integrity of its transaction by disabling alteration or deletion of its data once the transaction is recorded in its ledger, but it also means that any human-error or inaccuracy in the system could not be manually fixed. For instance, an operation professional who is in charge of inputting the information of drugs into the ledger sent out a transaction but later realized that they made a mistake by entering the quantity as 100 instead of 10. In this case, the blockchain-based drug supply chain management system prevents that person from reentering the quantity of the drug, and the error would be carried to the distribution channel. If the manufacturer made a mistake while inputting drug description, the cascading effect will spill over to the next stage of the supply chain and potentially causes pharmacists to prescribe the wrong drug to patients.

4.2 Data Privacy

The immutability of blockchain transactions also exposes blockchain-based systems to another problem: conflicting with recent data privacy laws, like General Data Protection Regulation (GDPR). According to GDPR, a person reserves the right to control how their data is stored, be aware of the location their data is stored, and alter and delete their data at any time [20]. In the case of health insurance claims, insurance subscribers might refuse to let the system store their personal, sensitive data on blockchain permanently, a request that is not supported by current blockchain technology. As more comprehensive data protection laws and regulations establish and. grow, failing to comply to data protection laws and regulations will result in healthcare providers facing serious legal issues.

4.3 Scalability

Blockchain requires every node to process every transaction in the network, and the consensus mechanism such as Proof-of-Work requires massive amount of computing power to provide data security and validation. However, this feature limits the scalability of the system. That being said, Sharding and Plasma are two solutions to mitigate the efficiency problem by eliminating the need for every node to process every transaction. Whether scalability is going to be an issue depends on the number of drugs being manufactured. Producing drugs in large scale using a blockchain-based system could slow down the manufacture process and increase the level of energy consumption significantly.

4.4 Interoperability

Blockchain might mitigate the dependency problem by not relying on a single central server, but meanwhile it creates a new problem, where two blockchains are not able to communicate with each other. There are attempts to create a standardized blockchain-based solution, but in reality, this issue is likely to be more prominent as major healthcare providers decide to adopt or establish private blockchains to ensure cost efficiency and manage access control. If healthcare centers make the decision to operate on different blockchain platforms, and the platforms employs different consensus mechanisms and verification processes, it would significantly hinder patients' healthcare experiences.

5. Conclusion

This paper investigated ethical challenges in the healthcare sector includes human organ transplant, counterfeit drugs, and health insurance fraud. Based on a systematic mindset, the paper proposed a blockchain-based solution for each of the abovementioned issue and evaluate the potential of its application. The proposed solutions leverage the decentralization, immutability, and smart contract

features of blockchain network to add data security to the existing healthcare ecosystem and make it less vulnerable to internal and external attacks. Nevertheless, some challenges and limitation of the implementation were listed and discussed, encouraging future research and investigation.

References

[1] U. Jain, "Using blockchain technology for the organ procurement and transplant network", 2020.

[2] M. He, A. Corson, J. Russo and T. Trey, "Use of forensic DNA testing to trace unethical organ procurement and organ trafficking practices in regions that block transparent access to their transplant data", SSRN Electron. J., 2020.

[3] D. P. Nair, Organ is Free Transplant Cost is Problem, 2016, [online] Available: https:// timesofindia. indiatimes. com/ life-style/ healthfitness/health-news/ Organ-is-free-transplant-cost-isproblem/ articles how/ 54014378.cms.

[4] P. Ranjan, S. Srivastava, V. Gupta, S. Tapaswi and N. Kumar, "Decentralised and distributed system for organ/tissue donation and transplantation", Proc. IEEE Conf. Inf. Commun. Technol., pp. 1-6, Dec. 2019.

[5] Shortage of Personal Protective Equipment Endangering Health Workers Worldwide, Jun. 2020, %5 bonline %5d Available: https:/tinyurl.com/v5qauvp.

[6] Guardian, 10% of Drugs in Poor Countries Are Fake Says WHO, Jun. 2017, [online] Available: https:/www.theguardian.com/global-development/2017/nov/28/10-of-drugs-in-poor-countries-are-fake-says-who.

[7] D. Bagozzi, 1 in 10 Medical Products in Developing Countries Is Substandard or Falsified, Jun. 2017, %5bonline%5d Available: https:/www.who.int/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified.

[8] A. Marucheck, N. Greis, C. Mena and L. Cai, "Product safety and security in the global supply chain/ Issues challenges and research opportunities", J. Oper. Manage., vol. 29, no. 7, pp. 707-720, Nov. 2011.

[9] C. Thapa and S. Camtepe, "Precision health data/ Requirements challenges and existing techniques for data security and privacy", Comput. Biol. Med., vol. 129, Feb. 2021.

[10] M. Eling and M. Lehmann, %22The impact of digitalization on the insurance value chain and the insurability of risks%22, Geneva Papers Risk Insurance-Issues Pract., vol. 43, no. 3, pp. 359-396, Jul. 2018.

[11] R. Saranya and A. Murugan, "A systematic review of enabling blockchain in healthcare system/ Analysis current status challenges and future direction", Mater. Today Proc., pp. 1-12, Jul. 2021.

[12] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J.A. Kroll, E.W. Felten Sok/ research perspectives and challenges for bitcoin and cryptocurrencies 2015 IEEE Symposium on Security and Privacy, IEEE (2015), pp. 104-121.

[13] P. Pandey, R. Litoriya Implementing healthcare services on a large scale/ challenges and remedies based on blockchain technology Health Policy Technol., 9 (1) (2020), pp. 69-78.

[14] A. Li, X. Wei, Z. He Robust proof of stake/ a new consensus protocol for sustainable blockchain systems Sustainability, 12 (7) (2020), p. 2824.

[15] W. Viriyasitavat, L. Da Xu, Z. Bi, D. Hoonsopon Blockchain technology for applications in internet of things—mapping from system design perspective IEEE Int. Things J., 6 (5) (2019), pp. 8155-8168.

[16] A. Hasselgren, K. Kralevska, D. Gligoroski, S.A. Pedersen, A. Faxvaag Blockchain in healthcare and health sciences—a scoping review Int. J. Med Inform, 134 (2020), Article 104040.

[17] Electronic Health Records Can Improve the Organ Donation Process, Dec. 2021, %5bonline%5d Available: https:/hbr.org/2021/12/electronic-health-records-can-improve-the-organ-donation-process.

[18] C. C. Agbo, Q. H. Mahmoud and J. M. Eklund, "Blockchain technology in healthcare/ A systematic review", Healthcare, vol. 7, no. 2, pp. 56, 2019.

[19] R. Saranya and A. Murugan, "A systematic review of enabling blockchain in healthcare system/ Analysis current status challenges and future direction", Mater. Today, Proc., pp. 1-12, Jul. 2021.

[20] European Parliament and Council of European Union (2016) Regulation (EU), Aug. 2020, %5bonline%5d Available:https:/eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.