Ensuring the Durability and Reliability of Data in Smart Health Services Using Blockchain Technologies

Aldina Avdić *, Ulfeta Marovac*, Dragan Janković**
State University of Novi Pazar, Department of Technical Sciences, Novi Pazar, Serbia
** Faculty of Electronic Engineering, University of Nis, Nis, Serbia
apljaskovic@np.ac.rs, umarovac@np.ac.rs, dragan.jankovic@elfak.ni.ac.rs

***Abstract*— The use of modern technologies in all spheres of life offers the possibility of collecting and processing citizens' data in smart cities to improve the quality of their lives through creating smart health services. The collected data should be protected from misuse. This paper describes e-health services in smart cities, as well as the problems of ensuring durability and reliability of patients' data. As a solution to this problem, the use of blockchain technology has been proposed and ways for its application have been given.**

I. INTRODUCTION

Advances in information technology, especially sensor technology and Big Data processing techniques [1][2][3], have made it possible to create the concept of a smart city. Smart city is "a developed urban area that creates sustainable economic development and high quality of life by excelling in multiple key areas: economy, mobility, environment, people, living, and e-government". One of the most important components of a smart city is smart health [4]. S-Health (smart health) encompasses a range of health and medicine services that are realized by combining medical technologies and ICT (information and communication technologies), within smart cities. The data is coming from citizens using crowdsourcing, crowdsensing, from medical information systems and EHR-s (electronic health records), etc. Then they are processed using the ICT infrastructure of the smart city and returned to citizens in the form of new knowledge, dashboards, info tables etc.

Citizens' health can be improved using telemedicine and online services, but the question of privacy, data security, durability and reliability in smart health services is raised.

The research motivation and the problem are following. To use this information for the benefit of citizens and to protect it from abuse by third parties, it is necessary to think about their protection in a specific way. Encrypting this data would prevent its processing for the purpose of e-health services. Conversely, if the data remained in its original form, it would be easy to misuse it.

Patient data can be divided into two groups: personal data (name, occupation, place of residence) and health information (medical history, diagnosis, etc.). The EHRs which cannot be used to reveal a patient's identity can be used to implement various health services in a smart city (i.e., information for epidemic control, vaccination progress etc.). Therefore, they should be in raw form, suitable for further processing, but protected from abuse.

A suitable method for protecting this data should provide next:

(a) protection against attacks and changes by a third party,

(b) the identity of the patient cannot be deduced from the available data, and

(c) that the data that can be used for research is not encrypted.

On the other hand, blockchain technology [5] has been very popular in recent years, and is used to decentralize services and data, and its most famous role is related to the emergence of cryptocurrencies.

The first research question is what the challenges are related to data security and privacy in smart health services. The second research question is can blockchain be used for the purpose of creating efficient smart health services and how. To answer these questions, it was necessary to use the following scientific methods: a method of description and qualitative analysis was applied to the related work and the applications of blockchain technology in healthcare, a simulation of using a blockchain for a smart health service was done, and a method of modeling smart health services based on blockchain has been applied.

The paper is organized in following way. The second section describes related work, which consists of a description of methods for ensuring data privacy and security in a smart city, and a description of blockchain technology, and the application of blockchain technologies in smart health. The following is a description of the integration of blockchain technology and health services through the storage of electronic medical reports, and description of its use cases. Finally, conclusions and directions for further research are given.

II. RELATED WORK

A. Methods for ensuring data privacy and security in smart cities

Statistical disclosure control. Tabular data collected from patients are also called microdata. This method changes the microdata to ensure minimal loss of information, while reducing the possibility of re-identification of users based on data [6].

The W3 privacy model provides privacy protection when location-based services are used. Since such services receive information that someone from a certain location is asking something, it is necessary to disable the tracking of this personal data, but only to answer the question. This model can also be applied to location-based services within smart health [6].

The 5D privacy model is based on the following five dimensions: identity privacy, query privacy, location privacy, fingerprint privacy, and owner privacy. This model represents an extension of the previous model for the last two dimensions. Fingerprint privacy refers to the protection of privacy when appropriate sensor data collection technology is used so that they are not given to a third party and are not misused. Owner privacy refers to the privacy of user data that different city services have about the user [6].

B. Blockchain technology

The term blockchain is associated with cryptocurrencies. The most popular among them is bitcoin, which was first described by a scientist or a group of them under the pseudonym Satoshi Nakamoto in 2008 [7]. At the same time, to protect ownership of cryptocurrencies, blockchain has been proposed to record bitcoin transactions.

Figure 1 shows the structure of the blockchain and the block in the chain. In addition to the block ID number and block creation time (timestamp), each block contains its hash key in the header, as well as the hash key of the previous block and of course the data.

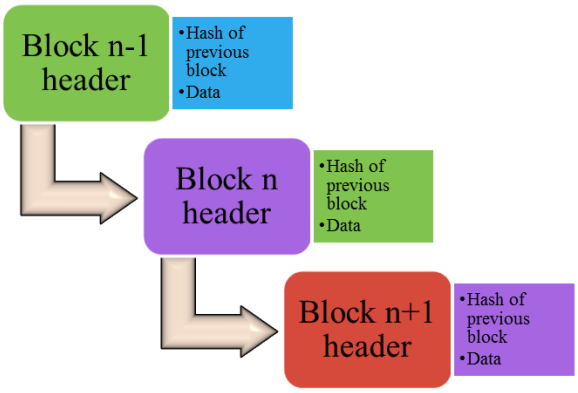

Figure 1. The structure of blockchain

The functioning of the blockchain can be described on the principle of a bitcoin transaction (Figure 2). Blockchain, in this case, is a collection of digital wallets. For example, if we want to transfer bitcoin from wallet A to wallet B, all members of the bitcoin blockchain must know this. A new block is created containing information about the transaction time and information about it. To add a created block to the blockchain, it must be verified by others in the chain. That way the transaction is visible to everyone.

This means that all transaction data is in a database that is publicly distributed to all owners, i.e., this information is publicly available. And the data is sent by users who have a pseudonym, so the information within the block is anonymous [8].

C. Blockchain in smart health

The possibility of using blockchain technology to secure transactions in cryptocurrencies has led many researchers to consider its use in data security and privacy in other areas.

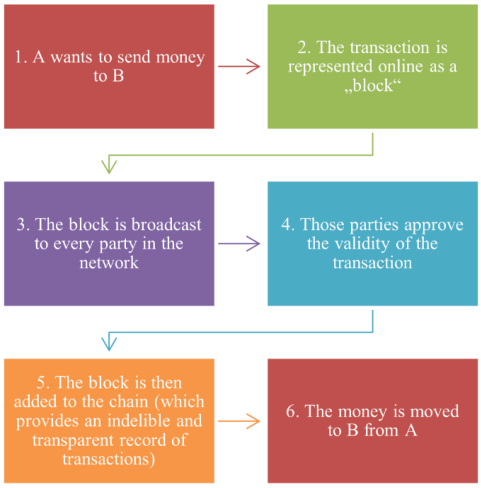

Figure 2. Recording a transaction in a bitcoin blockchain

In [9], the authors described algorithms for using blockchain technology to store private data. In papers [10][11][12][13][14] there are ways to apply blockchain technology in the health system, with an emphasis on electronic health services.

The paper [13] describes an overview of the possibilities of using blockchain technology for decentralization and data protection in smart city services.

The paper [10] describes a prototype of the MedRec system for storing health data and data intended for research based on blockchain.

The related papers present cases of blockchain use in health care through the following services:

1. monitoring the drug supply chain to suppress the abuse of opioid prescribing and prevent patients from becoming dependent on these drugs,
2. data storage for telemedicine services,
3. controlled sharing of sensitive patient data (cancer monitoring, therapy, instructions, etc.),
4. digital identity of the patient and personal health card,
5. information on requests for coverage of costs by health insurance.

III. USING BLOCKCHAIN IN S-HEALTH SERVICES – A SIMULATION AND THE USE CASES

The data in the case of cryptocurrency is the amount of money and transactions, while in our model it will contain information about the patient.

A simulation in Python is done, where the EHRs from Health Center Niš collected by information system MEDIS.NET [15] are stored in the blockchain. The part of the blockchain with these EHR data is given in the Figure 3.

The creating of a blockchain in which the blocks consist of the medical reports, was done, with a modification of the solution given at the [16].

Figure 3. The blockchain structure with EHR data

The simulation was done on a Lenovo G50 laptop that had an i5 processor, 8GB of RAM, with an 256GB SSD hard drive. The measurement required to create the chain, the block, and the transaction was performed and the obtained average time is given in Table 1. Some implementation details are given in the Figure 4.

TABLE I.
EXECUTION TIME OF FUNCTIONS FOR ENTERING AN EHR IN A BLOCKCHAIN

Function name	Average execution time (s)
Creating a blockchain object	1.130000000000575e-05
Creating a blockchain transaction	8.30000000000275e-06
Adding a new block	0.0001152999999999999874

It is evident that the time for entering the data into the blockchain is not greater than the time for entering the data into any database, and the simple implementation is an additional argument for integration in health services. This is not the case with public platforms intended for this purpose, where the confirmation of the transaction takes 6 to 10 minutes.

```
class Blockchain(object):
    def __init__(self):
        self.chain = []
        self.pending_transactions = []

        self.new_block(previous_hash="The previous hash.", proof=100)

    def new_block(self, proof, previous_hash=None):
        block = {
            'index': len(self.chain) + 1,
            'timestamp': time(),
            'transactions': self.pending_transactions,
            'proof': proof,
            'previous_hash': previous_hash or self.hash(self.chain[-1]),
        }
        self.pending_transactions = []
        self.chain.append(block)
        return block

    @property
    def last_block(self):
        return self.chain[-1]

    def new_transaction(self, doctor, patient, anamnesis):
        transaction = {
            'doctor': doctorID,
            'patient': patientID,
            'anamnesis': anamnesis,
        }
        self.pending_transactions.append(transaction)
        return self.last_block['index'] + 1

    def hash(self, block):
        string_object = json.dumps(block, sort_keys=True)
        block_string = string_object.encode()
        raw_hash = hashlib.sha256(block_string)
        hex_hash = raw_hash.hexdigest()
        return hex hash
```

Figure 4. The part of implementation details of the integration of the EHR data in the blockchain

The block stores the data about the patient, but only those data based on which it is not possible to conclude about the identity of the patient. In this case, the health insurance number represents the name of the block in the chain, but it can also be some other information that can be used as the patient's pseudonym. Also, these are medical reports that contain only textual data about the patient, but not images such as radiological images, which would make it difficult to store the data.

In addition to storing the electronic medical reports in a blockchain, three use-cases of smart health services could be enabled in a more efficient way by storing data in a blockchain:

1) Services in which an individual patient is supported by an intelligent health infrastructure. For example, a service in which elderly patients can use smart bracelets or a mobile application to press an auxiliary button, and through sensors on IoT devices can send current parameters of body temperature, blood sugar levels, heart rate, pressure and this could be noted in the patient's card. The latest, as well as earlier patient data, can be used, for example, to detect impending problems and to suggest ways to prevent different types of strokes through machine learning. Here, the patient's private data sent to the smart city's health infrastructure would be stored in a blockchain.

2) Services that use large amounts of data to draw conclusions about the health of the smart city population. For example, the data from all patients could be used to visualize data on infection during an epidemic or

vaccination based on EHR data. Also, the data on epidemics, (e.g., such as numbers of infected, dead, and patients on respirator during a corona virus disease pandemic) could be stored in a blockchain, thus avoiding changes and doubts about its accuracy.

3) Another interesting application of blockchain is the storage of data on organ donors.

IV. Conclusions and Future Work

The paper provides an overview of the challenges in privacy and data security within the smart health service.

The example shows that blockchain technology can be used in smart health services for ensuring durability and reliability of patient data stored in EHRs.

The features of blockchain technology should be used to ensure the durability and reliability of patient data, whether from EHRs or from sensors on wearable or mobile devices, or other health services which require the data privacy.

Acknowledgment

This paper is partially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia under projects III44007 and ON 174026.

References

[1] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The internet of things is the backbone," *IEEE Consumer Electronics Magazine*, vol. 5, 2016, pp. 60–70.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things journal*, vol. 1, 2014, pp. 22–32.

[3] M. Batty, "Big data, smart cities and city planning," *Dialogues in Human Geography*, vol. 3, 2013, pp. 274–279.

[4] A. Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, and A. Martinez-Balleste, "Smart health: a context-aware health paradigm within smart cities," *IEEE Communications Magazine*, vol. 52, 2014, pp. 74–81.

[5] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," *e-Health Networking, Applications and Services (Healthcom) 2016 IEEE 18th International Conference on IEEE*, pp. 1–3.

[6] A. Martinez-Balleste, P. A. Pérez-Martínez and A. Solanas. The pursuit of citizens' privacy: a privacy-aware smart city is possible, IEEE Communications Magazine, vol. 51, 2013, pp. 136–141.

[7] N. Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

[8] https://bitcoin.org/bitcoin.pdf

[9] G. Zyskind, and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," *Security and Privacy Workshops (SPW)*, 2015, pp. 180–184.

[10] A. Ekblaw, A. Azaria, J.D. Halamka and A. Lippman, "A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data," *In Proceedings of IEEE open & big data conference*, vol. 13, 2016, pp. 13.

[11] L.A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States: ONC/NIST. 2016.

[12] S. Angraal, H. M. Krumholz and W. L. Schulz, "Blockchain technology: applications in health care," *Circulation: Cardiovascular Quality and Outcomes*, vol. 10, 2017.

[13] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology. High Performance Computing and Communications," *IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on. IEEE*, pp. 1392–1393.

[14] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, "Blockchain technology use cases in healthcare," *In Advances in computers*, vol. 111, 2018, pp. 1–41.

[15] A. Milenković, D. Janković, M. Stojković, A. Veljanovski, and P. Rajković, "Kolaboracija mobilnih senzorskih aplikacija i medicinskog informacionog sistema," *INFOTEH-Jahorina*, vol. 13, 2014, pp. 879–884.

[16] https://github.com/mchrupcala/blockchain-walkthrough