Security model to protect patient data in mHealth systems through a Blockchain network

Cristhian Alexis Natividad Peña[1], Angel Elí Gutiérrez Díaz[2],
Jimmy Alexander Armas Aguirre[3] and Juan Manuel Madrid Molina[4]

[1]Universidad Peruana de Ciencias Aplicadas, Perú, u201413799@upc.edu.pe
[2] Universidad Peruana de Ciencias Aplicadas, Perú, u201214826@upc.edu.pe
[3] Universidad Peruana de Ciencias Aplicadas, Perú, jimmy.armas@upc.pe
[4] Universidad Icesi, Colombia, jmadrid@icesi.edu.co

Abstract*– On this research paper we propose a security model to protect patient data on mobile health systems (mHealth) through a Blockchain network. This model is implemented under a Blockchain platform that allows collecting, sharing and integrating data in a safe way through a mobile app for mHealth devices, for medical care in Peruvian clinics. This security model consists of three stages: 1. Data collection, 2. Data processing, 3. System monitoring. It should be noted that the patient is autonomous in the management of his information, and that each user requires a single identifier to get access to the data. A test scenario was defined to validate the proposed model. Also, the study was conducted with a group of users through a health mobile app and the used medical data was provided by a hospital in Peru as anonymized research data. During the study, we validated the following topics: access control to the network, access to medical information of authorized users, data integrity on each transaction and performance evaluation of the system under a high user transaction load. Preliminary results show the system average response time is 4.72 seconds for 10,000 users carrying out requests simultaneously.

Keywords—mHealth, Blockchain, wearable devices, security

I. INTRODUCTION

Mobile health (mHealth), according to the OMS, is the remote medical care service supported by mobile devices, such as smartphones, personal digital assistants (PDA) among others [1]. These devices allow doctors to remotely track a patient's clinical condition in real time, in order to take timely actions. MHealth offers services that help patients to get access to their data from any place through an internet connection. Likewise, this service reduces the number of visits to hospitals and the cost of medical attention [2].

Data security generates an impact on the patient's care. The inability of accessing the data could lead to delays in treatment and decision making. In 60 analyzed mHealth apps, 137 security vulnerabilities were found, with remote monitoring apps presenting most of the vulnerabilities (32.12% of the total) [3]. Risk factors established by OWASP were considered [11]; 64% of the found vulnerabilities corresponded to "security decisions through untrustworthy entries", meaning the attacker elevated access and privileges, affecting confidentiality and integrity of the clinical data.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2019.1.1.285
ISBN: 978-0-9993443-6-1 ISSN: 2414-6390

Many different solutions have been developed in order to provide data security in the mHealth system. However, solutions [5] and [8] only use one authentication factor for access to their systems. Furthermore, solution [5] only provides a government-level approach, and it does not take into consideration the behavior of an mHealth system in a private entity. Likewise, solutions [4], [6] and [7] are not scalable for a high level of transactions.

This paper is structured in the following way. We start with a literature review, then we will describe the proposed model and its implementation based on a real scenario. Finally, we present the conclusions, based on the obtained results in the case study.

II. LITERATURE REVIEW

Clinical information of patients is a critical asset that needs to be protected by secure systems in order to avoid access by unauthorized third parties. Previous studies have developed different solutions to the problem of security in patients' data in an mHealth system. Now, we discuss the main security attributes that must be incorporated in an mHealth system.

A. *Security Attributes in an mHealth system*

Table I shows the main attributes found in the literature review. The order of listing does not represent the importance of each one.

TABLE I
SECURITY ATTRIBUTES IN AN MHEALTH SYSTEM

Attribute	Description	Reference
Confidentiality	To keep clinical data private and inaccessible to unauthorized people.	[5], [6]
Integrity	The system must verify that stored data hasn't been changed by third parties, and also that data has been sent by someone trustworthy.	[5], [6]
Availability	Clinical data must be easily accessible to authorized people, whenever they require it.	[6]
Authentication	mHealth infrastructure must have robust authentication mechanisms to ensure identity of uses. In addition, it is recommended to have two or more authentication factors.	[5], [6]

Access Control	Doctors, nurses and patients access the information previously shared by the data owner.	[5], [7], [8]
Data Transfer	Data must be protected during transport, to avoid interception by third parties.	[6], [13]
Auditability	User activity on the system must be traceable.	[5]

B. *Blockchain platforms*

An evaluation of the different Blockchain platforms was carried out in order to identify usability and capacity of each one to secure medical information. Table II shows the main Blockchain platforms. The Ethereum platform allows execution of smart contracts between the participants, though it lacks permissions to access the network and perform transactions, which are visible to all the participants of the network. In contrast, Hyperledger Fabric requires permissions to access web content, and its transactions are visible only to a determined group through the use of encryption algorithms. In addition, Hyperledger Fabric allows reuse of components to facilitate testing. These were the main reasons to choose this platform to support our proposed model.

TABLE II
BLOCKCHAIN PLATFORMS

	Description	***References***
Hyperledger Fabric	Hyperledger Facbric is designed to develop apps or solutions with a modular architecture. It uses container technology to host chaincode, also known as smart contracts, i.e. logic of the system. Hyperledger Fabric was launched by Digital Asset and IBM as part of a hackathon [14].	[8], [17], [18]
Ethereum	Ethereum is a decentralized platform that executes smart contracts. It is a project developed by the Etherum Foundation, which is a Swiss organization with a team of developers all around the world. This platform allows design and creation of cryptocurrencies. Code in the Ethereum network may be executed for a fee [14]. This platform is adaptable for public networks.	[5], [19]
Multichain	It helps organizations to quickly develop and implement business solutions based on blockchain. The mining process is done via proof-of-work.The developer can decide either to create a private Blockchain network for being able to decide who can connect to the network and who can make transactions, or can choose to create a public blockchain. Customized cryptocurrencies can also be created [16].	[20]

C. *Data security solutions in an mHealth system*

Models for data assurance applied to an mHealth infrastructure have been proposed [8], [17]. Fig. 1, proposes a model for safe personal data exchange focused on the user, in order to improve interaction and collaboration in an mHealth system [8]. This model proposes a mobile health app based on Blockchain using a channel scheme and a membership service for identity management. Data is retrieved from a permanent database in the cloud synchronized to the Blockchain network, in order to protect the integrity of the information of each patient. Moreover, it uses a method of data processing based on trees, with the purpose of managing huge quantities of data.

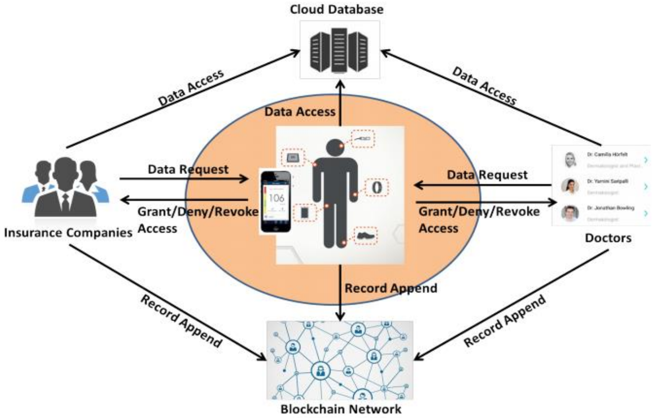

Fig. 1 Model Personal Mobile Health Data Sharing

Other solution, on Fig. 2, proposes a structure of an mHealth system for management of cognitive behavioral therapy in patients with insomnia, made tamper-resistant through the use of Blockchain technology, which allows auditability and reliable computing through a decentralized network [17]. Electronic medical records registered in the

Blockchain network through this solution were resistant to manipulation attacks.

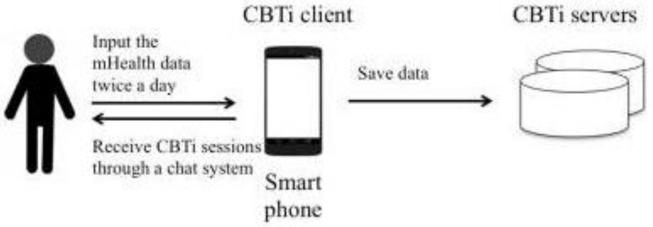
CBTi client
CBTi servers
Input the mHealth data twice a day
Save data
Receive CBTi sessions through a chat system
Smart phone

Fig. 2 The structure of the mobile health system for cognitive behavioural therapy for insomnia

In the same solution, on Fig. 3, the authors propose an architecture based on virtualization in Linux, using Docker and Hyperledger Fabric. The system consist of 4 validation peers (VP) and a membership service (MS). A peer is in charge of the functionality of all the Blockchain network, the membership service is in charge of the authentication to the system and each peer has a database replica [17].

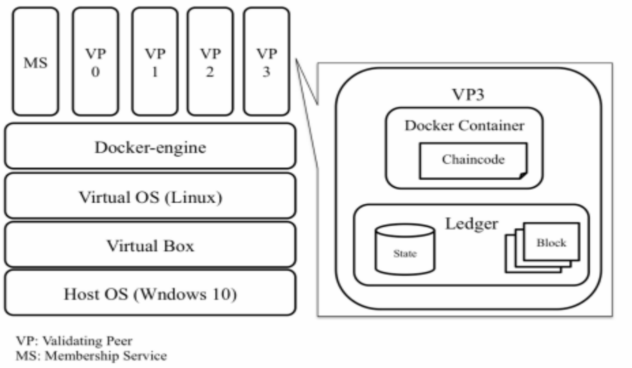

Fig. 3 Virtual computing environment

III. SECURITY PROPOSAL TO PROTECT PATIENT'S DATA IN MHEALTH SYSTEMS THROUGH A BLOCKCHAIN NETWORK

A. *Model Description*

On Fig. 4, we propose a model that allows maintaining the security when collecting and sharing patient' data through mHealth devices. This proposal will allow patients to manage access for visualization and treatment of their data by the medical personnel from the health entity. Three stages were conducted to compose the proposed model: First, patient data collection through mHealth devices; second, data processing in the Blockchain network in Cloud to guarantee privacy and security; and third, system monitoring and performance evaluation.

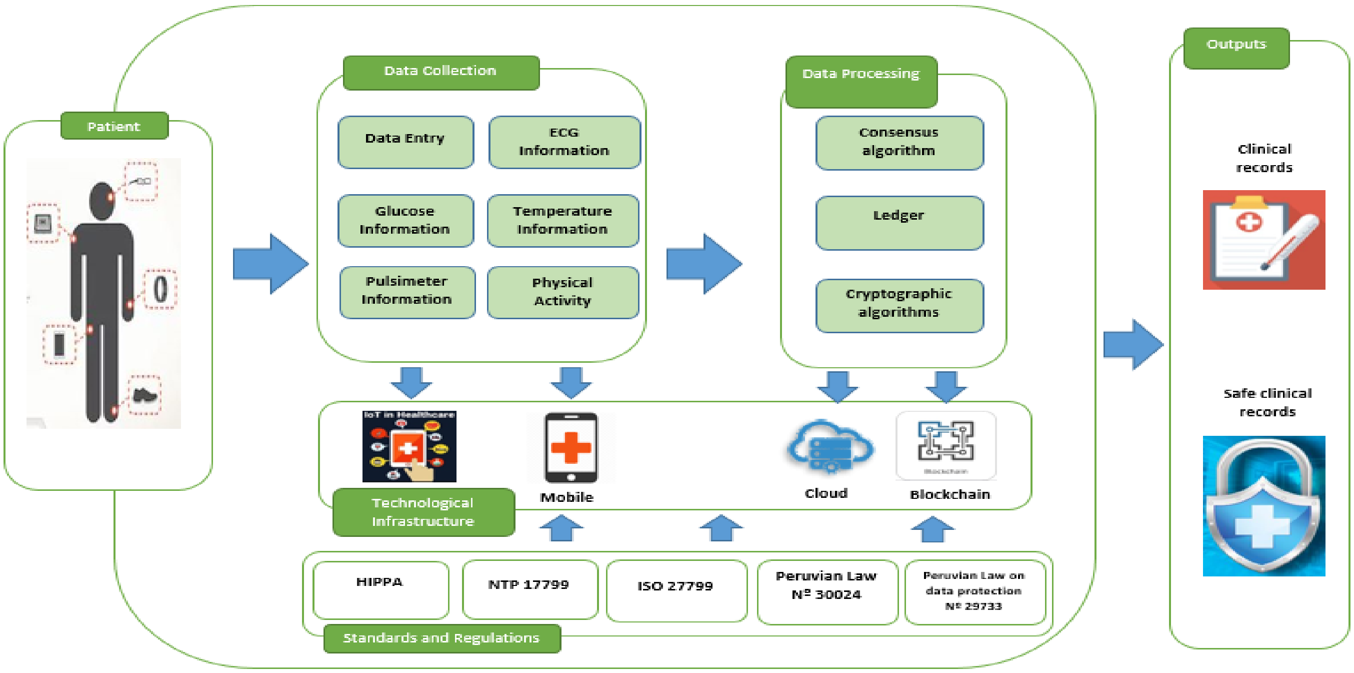

Fig. 4 Proposed security model based on Blockchain

B. *Stages of the model*

1) *Data collection*: Patient' data is collected through mHealth devices by the use of wearables, data entry in a mobile phone, PDA, etc. The patient shares his information giving access to the medical personnel and his/her relatives.

2) *Data processing*: Information flows through secure connections to the Blockchain network in the Cloud replicating the information among all the participant nodes having previously executed the consensus algorithm.

3) *System monitoring*: In this stage, system performance and generation of new blocks in the network are evaluated. This allows to evaluate system scalability.

The proposed model takes into consideration the main data security requirements on mHealth devices, such as availability, which means accessibility to information by an authorized user at any place and time; integrity, in order to guarantee that all stored data hasn't been modified by unauthorized third parties and to verify that the information has been sent by a reliable user; authenticity, to verify the identity of the participants in the network; and confidentiality, so that each participant can only have access to information according to his/her role in the organization and authorized access level [2]. In Peru, security levels established by HIPPA for mHealth systems have not been established nor regulated. This proposed model is supported on Peruvian regulations such as Law N° 30024, the law of protection of personal data; and the Peruvian Technical Regulations (Normativa Técnica Peruana) 17799, wich are mandatory in Peru.

C. *Proposed Architecture*

On Fig. 5, we propose an architecture to support the data security model and the use of Blockchain technology in an mHealth system. This architecture shows collection and processing of patients' data. It considers 3 user's profiles: patient, doctor and relative. Each participant needs an associated personal card that allows access to the network and to make transactions. These cards have the combination of identity, connection profile and metadata, which are all required to connect to the Blockchain network.

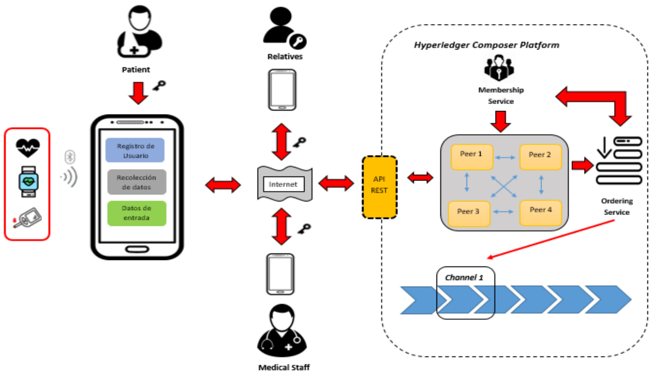

Fig. 5 Health technology architecture in Blockchain

On Fig. 5, we show the use of the Hyperledger Composer platform. This set of tools and development framework allows the creation of apps based on Blockchain technology. This platform is compatible with the Hyperledger Fabric infrastructure, which supports consensus protocols to ensure that transactions are validated in relation to network policy. Also, this architecture shows the integration and compatibility of mHealth mobile devices with Blockchain technology with the purpose of securing medical data.

IV. CASE STUDY

This case study shows the validations performed with the purpose of verifying security of medical information using Blockchain technology. For this, we validated through the developed mobile app the access control to the Blockchain network from an mHealth device, and the access to a patient's medical information for authorized users. The integrity of each transaction made in the network was also validated and, finally, the JMeter tool was used to measure system performance by simulating the interaction of several simultaneous users with the purpose of evaluating the scalability of the proposed system.

A. *Validation environment*

The validation made for the proposed model was developed under a controlled environment. The information used for this validation was provided by a specialist in cardiology from a Peruvian hospital. It should be noted that this information did not contain identifiable personal data (names, surnames, phone numbers, emails, etc.) and it was used only for the investigation. We worked with a sample of 75 records. The study was conducted between September and November of 2018.

B. *Implementation*

For this validation, a Blockchain network using Hyperledger Composer on Linux was implemented, and a mobile app was implemented simulating part of the system of a health entity, including records and queries of medical data. The tests were focused mainly on verification of compliance of the security attributes.

1) *Authentication (Access Control*): Two authentication factors were established in order to access the network: something the users knows and something the user has. For this, each new user (patient, doctor and relative) was enrolled by the network administrator. During this process, credentials were created (user and password) and a single identifier (a digital certificate) was automatically generated for each record. This identifier was shared with each user for interaction with the system; upon access, the app requests the identifier stored in the mobile device (mobile phone, tablet or laptop).

2) *Confidentiality:* In this case, data provided by the cardiologist was registered manually. Three inputs were received: heart rate, blood pressure and blood glucose levels. Patients had the authority of managing access permissions to their information, both for doctors and relatives, by granting and denying permissions to the data according to their needs.

3) *Data Integrity:* For this validation, we used Hyperledger Explorer, a web interface that allows visualizing transactions, blocks, nodes and interactions developed within a Blockchain network. As a user was registered, medical records were entered, and permissions were granted or denied, this interface showed a new transaction posted to the network. We integrated Hyperledger Explorer with the app, to verify that each transaction posted in the network contained a single hash provided automatically by the Blockchain technology.

C. *Results*

According to obtained data, the importance of proper information management is determined through the use of technologies that contribute to data security for the benefit of patients and hospitals. The two implemented authentication factors shows that 100% of the users registered in the network had to introduce their credentials correctly and had to have the single identifier hosted in the device to access the network. In addition, due to the Access Control Logic (ACL), implemented by the Blockchain technology, robust permission management was guaranteed.

The integration of Hyperledger Explorer tool with the app demonstrated the integrity of the hosted data in the network because each posted transaction contained a cryptographic hash generated by the SHA256 algorithm used by the Blockchain technology.

Another important factor was the evaluation of system performance, related to scalability and efficiency in data processing. On Fig. 6, results of validation with a high load of requests to the system by users are shown. We simulated a range from 10 to 10,000 requests. The system showed an average response time of 4.27 seconds with 10,000 simultaneous requests.

On equation (1), we show the calculation of the average time response of the system, where ***t*** is the response time for each request, and ***n*** is the total number of requests.

$$\bar{X} = \frac{\Sigma t}{n} \qquad (1)$$

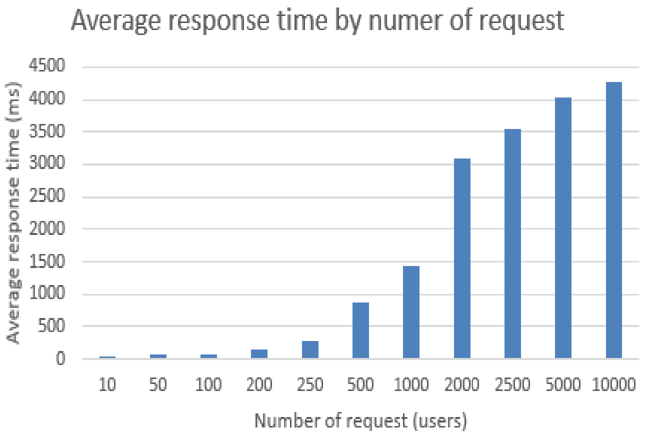

Fig. 6 Average response time of the Blockchain network

Finally, and in relation to the previous point, performance of the main functions of the system was evaluated: User authentication, data registration, and permission grant/deny. On Fig. 7, average response time for each functionality of the system are indicated, we observe that permission grant/denial presents a high performance based on the user's response time. Average response time for permission grant/denial for 10,000 simultaneous users is 4.13 seconds (grant) and 2.35 seconds (denial). In this way, we show that users can efficiently manage access to their data.

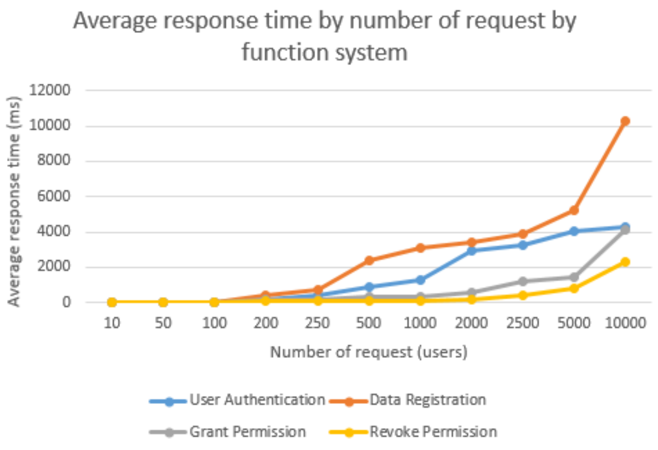

Fig. 7 Average response time of the Blockchain network based on system functions

V. CONCLUSIONS

In this paper, we proposed a security model using Blockchain technology, in order to secure data in a hospital. The model was tested in an controlled environment, using research data provided by a cardiology specialist from a Peruvian hospital. We conclude that the implementation of the proposed model guaranteed authentication, confidentiality, integrity and availability of the data, generating enhanced security in the hospital's systems.

Finally, the system demonstrated to be scalable supporting a high load of requests by users. This allows performing transactions in the system in a very efficient way, to grant and deny permissions to the rest of the participants.

REFERENCES

[1] World Health Organization. mHealth: New horizons for health through mobile technologies-Volume 3. WHO Library Cataloguing-in-Publication Data, Switzerland, 2011.

[2] Zubaydi, F., Saleh, A., Aloul F., Sagahyroon A.: Security of Mobile Health (mHealth) Systems, pp. 1-5. UAE, 2015.

[3] Beltran, L. Cifuentes Y., Ramirez L.: Analysis of Security Vulnerabilities for Mobile Health Applications. International Scholarly and Scientific Research & Innovation, vol. 9, pp. 1067-1072, Bogotá, 2015.

[4] Yang, Y., Liu, X., Deng, R., Li, Y.: Lightwight Sharable and Traceable Secure Mobile Health System. IEEE Transactions on Dependable and Secure Computing, pp. 1-14, 2017.

[5] Azaria, A., Ekblaw A., Vieira T., Lippman, A.: Medrec: Using Blockchain for Medical Data Access and Permision Management. In: 2016 2nd International Conference on Open and Big Data, pp. 22-30, 2016.

[6] Alibasa, M., Santos, M., Glozier, N., Harvey, S., Calvo, R.: Designing a Secure Architecture for m-Health Applications. In: IEEE Life Sciences Conference (LSC), pp. 91-94, 2017.

[7] Zhang, H., Wang, Z., Scherb, C.: Sharing mHealth Data via Named Data Networking. In: Proceedings of the 3rd ACM Conference on Information-Centric Networking, pp.142-147, 2016.

[8] Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D.: Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. IEEE 28th Annual International Symposium on Personal Inndor and Mobile Radio Communications (PIMRC), 2017.

[9] Wiss, M., Botha, A., Herselman, M., Loots, G.: Blockchain as an Enabler for Public mHealth Solutions in South Africa. IST-Africa, pp.1-8, 2017.

[10] Teachracers, https://www.techracers.com/healthcare-mhealth-blockchain, last accessed 2018/09/23.

[11] OWASP Foundation, https://www.owasp.org/index.php/Main_Page, last accessed 2018/09/16.

[12] Vhaduri, S., Poellabauer, C.: Wearable Device User Authentication Using Physiological and Behavioral Metrics. In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, Canadá, 2017.

[13] Atat, R., Liu, L., Ashdown, J., Medley, M.: A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems. In: IEEE GLOBECOM 2016, pp. 1.15. IEEE, Washington, 2016.

[14] Hyperledger Fabric, https://www.hyperledger.org/projects/fabric, last accessed 2018/10/12.

[15] Ethereum, https://www.ethereum.org, last accessed 2018/10/12.

[16] Multichain, https://www.multichain.com, last accesed 2018/10/15.

[17] Ichikawa, D., Kashiyama, M., Ueno, T.: Tamper-Resistant Mobile Health Using Blockchain Technology. pp. 1-10. JMIR Mhealth and Uhealth, Japon, 2017.

[18] Dubovitskaya, A., Xu, Z., Ryu S., Schumacher, M., Wang, F.: Secure and Trustable Electronic Medical Records Sharing using Blockchain. pp. 650-659 AMIA Annual Symposium Proceedings Archive, 2017.

[19] Mannaro, K., Baralla, G., Pinna, A., Ibba, S.: A Blockchain Approach Applied to a Telefermatology Platform in the Sardinian Region (Italy). In: e-Health Pervasive Wireless Applications and Services (e-HPWAS'17), pp. 1-15, 2018.

[20] Dai, H., Young, P., Durant, T., Gong, G., Kang, M., Krumholz, H, Schulz, W., Jiang, L.: TrialChain: A Blockchain-Based Platform to Validate Data Integrity in Large, Biomedical Research Studies, pp. 1-7, ArXiv, 2018.