An Architecture Proposal for E-health Data Collection and Storage Based on Internet of Things and Blockchain

Alan Nascimento Gomes, Emanuel Ferreira Coutinho

An Architecture Proposal for E-health Data Collection and Storage Based on Internet of Things and Blockchain

Alan Nascimento Gomes[1] and Emanuel Ferreira Coutinho[1]

Federal University of Ceara (UFC), Quixadá, Ceará, Brazil
alanng@alu.ufc.br,emanuel.coutinho@ufc.br

Abstract

Currently, several technologies are being used together to improve the quality of services for people. Specifically for the health area, the application possibilities involving both software and hardware are quite diverse. Internet of Things (IoT) and blockchain are two technologies that are currently integrating more and more to provide better services, taking advantage of their characteristics. This work proposes an architecture for the collection and storage of e-health data, based on IoT and blockchain. For its validation, a prototype was designed and the flow of operations was analyzed. Preliminary results indicated the proposed architecture has the potential to integrate IoT and blockchain to support e-health applications, enabling research and application development, but a broader study with IoT devices is needed for a better assessment.

1 Introduction

With the integration of technologies such as Internet of Things (IoT) and blockchain, a new computational layer has emerged capable of offering secure data sharing and analysis, in addition to enabling privacy guarantees, where it is possible to authenticate, authorize, control and audit the data obtained from sensors [1]. In this context, the integration of these technologies has enabled the development of applications in different sectors: finance, health, education, etc.

IoT is a paradigm in which heterogeneous physical objects are interconnected through wired or wireless technologies. The basic idea is to integrate "things" on the Internet by providing users with various services [2][3]. Nowadays, many IoT projects have milions of IoT devices acting as sensor or actuator, collecting sensitive data from people or processing this data for the most varied purposes [4].

According to the *Healthcare Information and Management Systems Society* (HIMSS) [5], e-health is defined as the application of the Internet and other related technologies in the health sector to improve access, efficiency and the effectiveness of the quality of clinical processes and business processes used by healthcare organizations, professionals, patients and consumers, in an effort to improve the health status of patients.

In the literature, several works have invested in e-health applications [6][7]. Neto et al. [7] proposed an approach for monitoring people who are part of risk groups. For example, sedentary people, using IoT technologies. They monitored users' physiological data through wearable devices and sends this data to a computational cloud. These data are processed, stored and presented to the healthcare professional, who will monitor and establish new activities for the user. They built a mobile and web applications, and collected data from sensors and a dataset of health data. Neto et al. [6] presented an IoT approach to help sedentary people. This approach monitors users' physiological data through wearable devices and sends them to the cloud for processing. In the cloud, the data is processed and presented to the health professional, that will monitor and establish new activities for users. The data generated in

situations such as those described in these works brings the problem of how to access the data safely and how to avoid falsification.

Blockchain is a data structure that makes it possible to create a transaction-proof digital ledger and share it [8]. This technology uses public key cryptography to sign transactions between the parties. The transactions are then stored in a distributed ledger. The ledger consists of cryptographically linked transaction blocks, which form a blockchain [9].

The data obtained from the sensors when stored in centralized bases can cause several problems due to this centralized topology. Among the problems, we highlight those related to security, for example, when there is a server failure or when the server suffers hacker attacks. Blockchain shows itself as a potential technology to solve these problems by offering desired resources for large-scale IoT infrastructures, such as decentralization, reliability, traceability and immutability [10].

The objective of this work is to present an architecture that integrates IoT and blockchain technologies. A flow of operations from the collection of sensors data to the availability of this data in a web / mobile application will be described. An application prototype to validate the architecture will also be presented in the work.

This work is divided into the following sections: Section 2 shows some related work; in Section 3 the proposed architecture is presented; Section 4 shows the design of a proof of concept for the architecture, the developed prototype and some discussion; and finally, Section 5 presents the conclusions and future work.

2 Related Work

Some works in the literature have developed research related to IoT and blockchain [10][11][12]. Wang et al. [10] proposed a hierarchical blockchain storage structure, where the majority of blockchain is stored in the cloud, while the most recent blocks are stored in an overlay network. Research opportunities with the use of blockchain technology in applications that manipulate DNA sequence data were presented in Neto et al. [12]. For this, an architecture for general e-health applications with blockchain was proposed. They also implemented a proof of concept to analyze the use of blockchain technology in e-health applications using DNA sequence data and they also listed a set of research opportunities. A study of the use of blockchain technology in an e-health approach was described in Neto et al. [11], using the distributed database BigchainDB, where a performance analysis of transaction validation times was conducted.

Chendeb et al. [13] proposed a multi-layer IoT/blockchain based architecture customized and designed to be used in the medical field. Many parties interact With this information, including doctors, health service providers, insurance companies and pharmacies. A distributed blockchain cloud architecture model was designed to meet the design principles required to efficiently manage the raw data streams produced by numerous IoT devices, promoting the possibility of using blockchain technology with IoT and vertical applications. The proposed architecture was designed to support high availability, real-time data delivery, high scalability, security, resiliency, and low latency. As future work, the authors intent to implement this architecture in a real system, and evaluate performance.

Batista et al. [4] proposed Heimdall, a distributed smart contract-based framework that provides access control for sensitive or personal data collected by IoT devices that follow the prerogatives of General Data Protection Regulation (GDPR) and General Data Protection Law (Lei Geral de Proteção de Dados - LGPD). The users must be able to: authorize or revoke the data access without depends on a trusted third party; to define what subset of your sensitive or personal data may be accessed or not based on access rules; to audit whom accessed his sensitive

or personal data and be able to see when this occurred. For this, it is necessary develop a smart contract that rules the access control, create the protocol that defines the possible operations on the access control framework and the involved actions, define the syntax and semantics of access rules, design a distributed mechanism to verify the access rules and create a multidimensional index of sensitive and personal data to facilitate queries on stored data. This work is still in development.

3 Architecture Proposal

This section describes the main elements of the proposed architecture. These elements can be composed of sub-elements of hardware or software systems.

Figure 1 represents the proposed architecture and operations flow of an environment that uses IoT and blockchain technologies. The proposed scenario illustrated by the architecture is an e-health application, with the purpose of verifying the health status of a patient.

At a high level, the first element is the set of devices responsible for performing measurements and data capture. For an e-health environment, for example, these devices are sensors responsible for analyzing the patient's physiological events, such as temperature sensors, blood pressure, glucose, etc. The second element is the communication system used to transmit data from the input devices to a storage environment. The third element is the data management system, which is related to the machines responsible for processing, storing and retrieving the data. And finally, the applications responsible for making interactions of the system with users capable of verifying the health status compose the fourth element.

In item (1) it is possible to view an IoT prototype responsible for collecting the data, in addition to elements responsible for handling the data coming from the sensors and preparing them for sending to the server intended to carry out the storage on the blockchain. Item (2) presents the architecture element responsible for communicating the IoT Prototype with the server's itens. In item (3), server P will receive the data read from the patient's health status and perform the insertion of the data on the blockchain. In item (4), the server C responsible for reading the blockchain data is shown. Sub-items (5.1) and (5.2) show the applications that access blockchain data through the server C, which make up the set of applications in item (5). And sub-items (6.1) and (6.2) are the individuals who have access to the applications.

4 Proof of Concept, Application and Discussion

This section presents a proof of concept of the proposed architecture and an application to illustrate a possible e-health application scenario. At the end, some discussions about architecture and technology are presented.

4.1 Proof of Concept

In this section, the implementation of the architecture presented in the previous section will be discussed. For this, an IoT prototype was designed and built in a similar way to that presented in item 1 of Section 3, where the sensors used for the implementation were simulated in order to generate data regarding the measurement of body temperature, blood oxygen level and heart rate.

The used development board was Esp8266 Nodemcu wifi module, responsible for receiving health status data and connecting to the Fiware framework. This framework is used to allow the

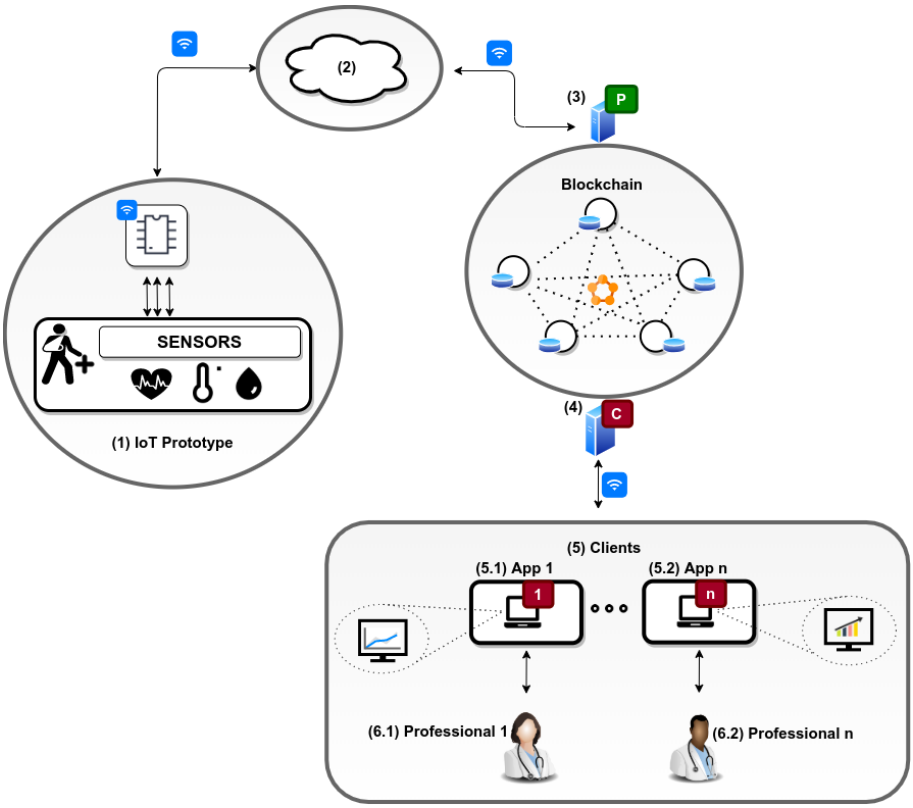

Figure 1: Architecture proposal

system to become scalable and to be able to deal with heterogeneity when the system becomes more robust [14]. Fiware is an open source project that provides a set of components whose objective is to facilitate the development of intelligent applications. It emerged in Europe from the Future Internet Public Private Partnership (FI-PPP), defining APIs for the development of solutions in several sectors, such as: smart cities, agriculture, e-health, transport and energy [15][16]. A simplified view of the components to perform the communication is shown in Figure 2.

In Figure 2, the implementation of items 1, 2 and 3 of Figure 1 is presented and the blocks will be described below. The main component of Fiware middlwware is presented in the block referring to Orion Context Broker, responsible for managing context information, such as: updates, queries, records and subscriptions [17]. The context information in the scenario presented refers to the patient's health status. For this architecture, Orion Broker will receive notifications from Agent IoT informing context updates.

The IoT Agent component presented in the block diagram has the function of communicating the physical devices with the Orion Broker, because in an IoT system it is common to have a diversity of technologies and communication protocols, requiring an entity responsible for carrying out the interpretation of data from the sensors for the Orion Context Broker. This component also addresses security issues and provides services for programmers AGENT. In this architecture, Agent IoT will listen to the MQTT Broker so that the measurements can be sent to Orion.

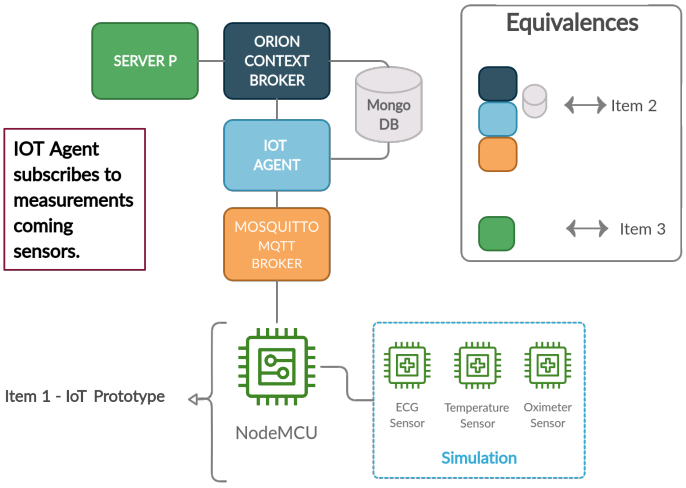

Figure 2: Simplified view of the components to perform the communication

In addition, Orion Context Broker uses the MongoDB database to store information related to the context state of devices across entities. These states are stored in the JSON format [18].

With Orion Broker, it is possible for asynchronous notifications to be sent to applications connected to the Broker. This is made possible when applications subscribe to receive update notices. This makes it possible for applications that communicate with the Orion Context Broker do not make requests unnecessarily, but only when the context of an entity is updated. The use of the signature mechanism will therefore reduce the volume of requests and the amount of data transmitted between the components of the system. This reduction in network traffic will improve overall responsiveness [19]. Therefore, whenever a change in the patient's health status occurs, a POST request is submitted to the server P, in order to update the patient's information.

Regarding the section of architecture dedicated to data storage, the types of available blockchains were initially analyzed. Blockchain networks are divided into two groups based on the type of permission, which are: without permission (permissionless) and with permission (permissioned). An example of a blockchain network without permission is Bitcoin, in which topology block insertion in the network is not restricted. However, this approach does not satisfy the requirements of the implemented scenario, as the data related to health are of a private nature. In blockchains with permission only individuals with authorization can interact with the network [20]. This type of network is interesting for the implemented scenario because the access to patient data is limited.

The solution for using a permissioned blockchain was to use Hyperledger [21]. The Linux Foundation launched this project in 2015, which built a corporate blockchain development platform [22]. Hyperledger Fabric is a technology from Hyperledger technologies. It uses a modular structure to provide scalable components, including encryption, authentication, consensus algorithm, smart contract, data storage and other services [23]. Chaincodes are the smart contracts responsible for allowing applications to interact with the network, depending on the business rule of the application. For this architecture, in the chaincodes functions were defined that insert the data in the blockchain, the reading of the network data, through the servers P and

C respectively, and the search of the data history.

With the data inserted in the Hyperledger network, it is already possible for applications to make requests in order to obtain the data from the sensors and present them in a more readable way. For the demonstration of this architecture, the servers P and C were implemented in Node JS and the application responsible for demonstrating the data in Vue JS.

4.2 Application

In this section, the prototype of the WEB application will be described. We highlight here that the idea is to have an application that is an e-health application scenario just to illustrate the architecture.

This application initially aims to display graphs of the patient's situation, based on three variables indicating: heart rate, body temperature and blood oxygen level. The values of these variables are obtained from the Hyperledger network and are changed by the simulated sensors, as previously discussed. In the proposed scenario, only one patient is being considered, whose identification is being named by the identification 111.111.111-11.

As the used network ledger is immutable and transparent, it is possible to take advantage of these characteristics to track transactions and thus obtain the current status and history of the patient's vital signs. Figure 3 shows the last data stored in the network regarding measurements that indicate heart rate (92 beats per minute), temperature (37 degrees) and blood oxygen saturation (98%). This chart can be used by professionals to facilitate visualization of the patient's current situation through the measured values. This would be just a possible feature of the application. E-health applications have many features and depend a lot on the type of application or area of expertise. As patient data is stored on the blockchain, its origin is transparent to the end user.

Figure 4 displays the data history. These data are: timestamp, name, docType, ekg, temperature and oxymeter. These data represent the timestamp in which the transaction was performed by the network nodes, the patient's name, an identifier of the type of transaction, the measured heart rate value, body temperature and blood oxygen rate, respectively. This is a code vision. The final user did not visualize this information in this format. This history is obtained by the server C from Figure 1, which makes a request to the Hyperledger network to obtain an array that is formed by the values of the vital data and time stamps, this array is built based on the patient's identifier. Data of ekg, temperature and oxymeter are displayed in the graphs of Figure 3.

Finally, in Figure 5, the line graphs show samples of the data history. These graphs were constructed with the values similar to those in Figure 4. Through them it is possible to investigate individually and together the three variables that are being measured by the sensors. Thus, it is easier for the application user to study the patient's situation, through the knowledge of the behavior of these data in the past, since it is possible to easily examine the trajectory of the variation of the information obtained from the sensors according to the evolution of the time that is in the horizontal axis. And by selecting one of the markers, users are provided with an immediate visualization of the absolute values measured at each instant, as shown in Figure 5.

The line graph consists of the presentation of three variables: the upper line (orange and dotted) shows the measured values referring to the percentage of oxygen in the blood, the intermediate line (blue and continuous) refers to the value obtained from the ECG sensor, and the bottom line (green and dotted) is body temperature. The variation of the horizontal axis indicates the displacement in time and variations in the vertical axis define the measured value

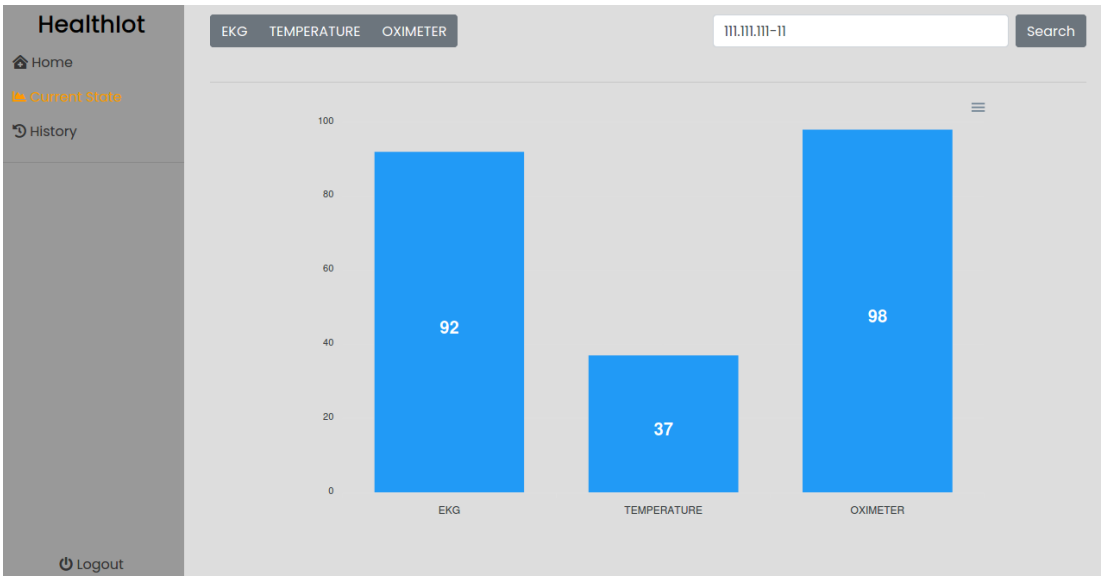

Figure 3: Measuring sample

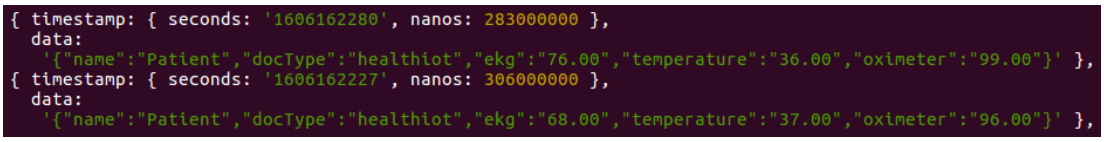

Figure 4: Hyperledger network data

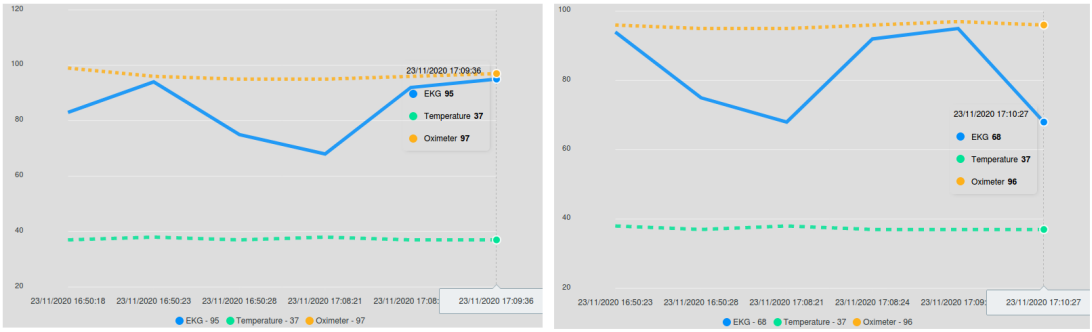

Figure 5: Samples of history captured from the sensors

for each variable.

The application presented in this section aims to validate the architecture discussed previously, indicating that with the implementation of the system through technologies for data collection, communication, storage, processing and presentation, it is possible to confirm that the components and the flow of operations established in the Figure 1 can be implemented and executed together.

4.3 Analysis and Discussions

As previously informed, there was no implementation of the architecture with all the items. In this case, the capture of sensor values was simulated, consisting of a work limitation. However, this does not invalidate the work as the flow of operations remains.

The application considered the use of a permissioned blockchain, that is, for e-health applications it would be better if the blockchain infrastructure was controlled with permissions for the involved institutions. In this case, Hyperledger was used for that purpose.

Several data are generated by the sensors, and the volume is often large. However, not all data makes sense to be stored on the blockchain. This is a research challenge, which involves data selection and merging, as the blockchain's storage capacity is limited. To get around this situation, relational databases can be used as a complement to the applications.

Regarding the financial cost, storing the data on a public blockchain would have an associated cost. This was yet another reason to use a permissioned and private blockchain. However, there is a cost to maintain the infrastructure between the involved institutions.

In order to fully serve a real e-health application, further study on the e-health sub-areas to be used is still needed. There are many sub-areas, so the number of features is also high. The integration between different systems and between different data formats also becomes a challenge, especially when considering issues of performance and quality of service. In this scenario, the use of IoT and blockchain must be carefully designed so as not to harm the entire e-health environment.

5 Conclusions and Future Work

This work presented an architecture for integrating IoT and blockchain. Thus, with its implementation, it will be possible to perform the flow of operations from the collection of data originating from sensors to its availability through a web or mobile application. A prototype of an e-health application was developed to validate parts of the architecture.

This work contributes to the spread of blockchain technology and its application. In addition, the proposed architecture can be applied to several domains using IoT and blockchain. This work is at an early stage, and it is possible to try several technologies related to IoT and blockchain. There is a need to have a deeper study on the integration of actuating and sensing devices to further characterize the relationship with IoT, and how data can be stored on the blockchain. It is also necessary to have a study more appropriate to e-health applications, so that prototypes can be developed that benefit well from the technologies involved. All of these tasks consist of future work.

Also as future work, we intend to fully implement the architecture in a more robust e-health application and consequent performance evaluation. For its evaluation, this will initially occur through the use by users specialized in e-health and also an analysis of application performance according to different workloads applied to the environment.

Acknowledgments: This work was supported by PIBIC 2020/2021 (01/2020) program, project **Integração de Aplicações E-health com Ambientes de Computação em Nuvem e Blockchain**, from Federal University of Ceará (UFC).

References

[1] Fabíola Greve, Leobino Sampaio, Jauberth Abijaude, Antonio Coutinho, Ítalo Valcy, and Sílvio Queiroz. *Blockchain e a Revolução do Consenso sob Demanda*, chapter 5, pages 1–52. Sociedade Brasileira de Computação (SBC), Maio 2018.

[2] Yongqing Zhu Quanqing Xu, Khin Mi Mi Aung and Khai Leong Yong. *A Blockchain-Based Storage System for Data Analytics in the Internet of Things*, pages 119–138. Springer International Publishing AG, 2018.

[3] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805, 2010.

[4] Bruno L. A. Batista, Jose Neuman de Souza, and Joaquim Celestino Junior. Heimdall: An authorization framework based on blockchain for sensitive data access. *8th Internacional Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE)*, Jan 2020.

[5] HIMSS. Himss - healthcare information and management systems society — himss. https://www.himss.org/, 2019. 2020-01-22.

[6] Mauricio Moreira Neto, Emanuel Ferreira Coutinho, Matheus Roberto Oliveira, Leonardo O. Moreira, and Jose Neuman de Souza. Asp: An iot approach to help sedentary people. *6th Internacional Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE)*, Jan 2018.

[7] M. M. Neto, E. F. Coutinho, L. O. Moreira, J. N. de Souza, and N. Agoulmine. A proposal for monitoring people of health risk group using iot technologies. In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–6, Sep. 2018.

[8] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[9] Nir Kshetri. Can blockchain strengthen the internet of things? pages 68–72, July/August 2017.

[10] G. Wang, Z. Shi, M. Nixon, and S. Han. Chainsplitter: Towards blockchain-based industrial iot architecture for supporting hierarchical storage. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 166–175, July 2019.

[11] Maurício Moreira Neto, Emanuel Ferreira Coutinho, Leonardo Oliveira Moreira, and José Neuman de Souza. Toward blockchain technology in iot applications: An analysis for e-health applications. In Augusto Casaca, Srinivas Katkoori, Sandip Ray, and Leon Strous, editors, *Internet of Things. A Confluence of Many Disciplines*, pages 36–50, Cham, 2020. Springer International Publishing.

[12] M. M. Neto, C. S. d. S.Marinho, E. F. Coutinho, L. O. Moreira, J. d. C. Machado, and J. N. d. Souza. Research opportunities for e-health applications with dna sequence data using blockchain technology. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, pages 95–102, March 2020.

[13] Nada Chendeb, Nour Khaled, and Nazim Agoulmine. Integrating blockchain with iot for a secure healthcare digital system. *8th Internacional Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE)*, Jan 2020.

[14] FIWARE FOUNDATION. Fiware catalogue, 2018. https://www.fiware.org/developers/catalogue/.

[15] FIWARE FOUNDATION. Developers, 2019. https://www.fiware.org/developers.

[16] EUROPEAN COMMISSION. The future internet platform fiware, 2018. https://ec.europa.eu/digital-single-market/en/future-internet-public-private-partnership.

[17] FIWARE FOUNDATION. Welcome to orion context broker, 2018. https://fiware-orion.readthedocs.io/en/latest/index.html.

[18] FIWARE FOUNDATION. Iot over mqtt, 2018. https://fiware-tutorials.readthedocs.io/en/1.0.0/iot-over-mqtt/index.html.

[19] FIWARE FOUNDATION. Subsctiption, 2018. https://fiware-tutorials.readthedocs.io/en/1.0.0/subscriptions/index.html.

[20] K. Wüst and A. Gervais. Do you need a blockchain? In *2018 Crypto Valley Conference on*

Blockchain Technology (CVCBT), pages 45–54, 2018.

[21] The Linux Foundation. Hyperledger, 2020. https://www.hyperledger.org/.

[22] V. Aleksieva, H. Valchanov, and A. Huliyan. Implementation of smart-contract, based on hyperledger fabric blockchain. In *2020 21st International Symposium on Electrical Apparatus Technologies (SIELA)*, pages 1–4, June 2020.

[23] Hyperledger Fabric. Hyperledger fabric model, 2020. https://hyperledger-fabric.readthedocs.io/en/release-2.2/fabric_model.html.