Open access • Proceedings Article • DOI:10.1109/NTMS.2019.8763849

An IoT-Blockchain Architecture Based on Hyperledger Framework for Healthcare Monitoring Application — Source link

Oumaima Attia, Ines Khoufi, Anis Laouiti, Cedric Adjih

Institutions: Manouba University, Université Paris-Saclay, French Institute for Research in Computer Science and Automation

Published on: 24 Jun 2019 - New Technologies, Mobility and Security

Topics: Enterprise information security architecture

An IoT-BlockChain Architecture Based on Hyperledger Framework For Health Care Monitoring Application

Oumaima Attia
National School of Computer Science
University of Manouba
Manouba, Tunisia
oumaima.attia@ensi-uma.tn

Ines Khoufi, Anis Laouiti
SAMOVAR, Télécom SudParis
CNRS, Université Paris-Saclay
9 rue Charles Fourier 91011 Evry, France
ines.khoufi@telecom-sudparis.eu
anis.laouiti@telecom-sudparis.eu

Cedric Adjih
Inria Saclay
Infine Team
F91120 Palaiseau, France
cedric.adjih@inria.fr

***Abstract*—BlockChain a form of distributed ledger is gaining enormous attention in area beyond its cryptocurrency like the Internet of Things (IoT). Health care monitoring is one of IoT applications where many devices are connected. These connected things carried data that needs to be stored in a secure way. In this context we focus on IoT-BlockChain architecture for health care monitoring application. We start our study by exploring both IoT and BlockChain technologies. Fabric Hyperledger is a BlockChain framework that fits our need. In this paper, we propose a security architecture based on the Fabric Hyperledger framework. We validate our approach first at a design level by running examples, then by showing some implemented functionalities.**

***Index Terms*—IoT, Blockchain, Fabric Hyperledger, NDN.**

I. Context and Motivation

The evolution of Internet of Things (IoT) started a decade ago as part of the first phase of the digital transformation and it is evolving as a powerful and an attractive next generation service infrastructure. Various applications and services exploiting sensors and producing data have been increasingly emerging into markets in broad and different areas such as health care, transportation, industrial automation, security, food safety, distant object control and emergency response to tragic and serious incidents particularly natural disasters and so on. These applications therefore will impact people's everyday life and on the other side they will revolutionize the industry organization which will increase the world's economic growth.

For example, smart-homes will enable their residents to automatically open their garage when reaching home, prepare their coffee and adjust climate control systems. The same idea can be applied in hospitals and health care services where medical devices such as heart monitors, blood pressure monitors, blood sugar sensors, and many other devices will be connected to the Internet and thus will be enabled to deliver more valuable data. This intensive use will lessen the need for direct patient-physician interaction.

Nevertheless, it is necessary to mention that opening connectivity to the external world creates new challenges and raises worries and questions about data and IT infrastructure security that need to be considered seriously in order to realize its potential benefits especially in the medical domain where there is no place to errors.

In our study we focus on health care application where medical connected objects collect relevant information about a person's health status to assist with medical follow-up and adherence. The data recorded in real time by connected sensors provides an indicator of the state of health of the user.

The main problem appears when we take in consideration hundreds of millions of IoT devices that are designed to carry out measurements, process and communicate collected data. The threat rises if these devices themselves are becoming more and more vulnerable to physical attacks that may lead them to non-cooperative behavior or misbehavior with the rest of the nodes in the network and even become malicious nodes which aim at damaging other nodes by causing network outage and by corrupting the basic functionalities of the related system.

It will be scary then to imagine how devastating it would be in medical domain, if these devices were spying on us or if the data in transit was intercepted by an unknown adversary or even if the network itself was exposed to a potential harm.

This is why security systems must offer adapted mechanisms to cope with these challenges and provide the availability, integrity and confidentiality of the systems.

Popularized recently (notably through one of their original application, the Bitcoin), BlockChains are a mean to exchange data, perform actions, and transactions in a distributed way, while maintaining a distributed ledger. As such, the BlockChains are ideally suited for the Internet of Things, which are associated to physical objects (even human users) and interacting with the physical world (smart watches, robots, mobile phones, automatons, cars, sensors& actuators) in an identical distributed way. In addition to its distributed characteristic, the BlockChain technology is based on public-key cryptography and primitives such as digital signatures and hash functions, which can give security. Also, through public key infrastructure (PKI), the BlockChain enables the confidentiality. In this context, a line of work has explored the use of BlockChains for IoT security.

Our study fits within this context. It consists in designing and implementing a secured IoT architecture based on the BlockChain technology for the Health care sector. Our choice is motivated by the fact that Health is an essential element of the international sustainable development. As a matter of fact, the aim of our architecture is to insure a secure remote monitoring system by the use of IoT. More precisely, we will monitor some patient connected devices and we will retrieve their collected data in the BlockChain network. This data will be fetched with its name instead of using the devices IP addresses. Thus, the Naming Data Networking (NDN) paradigm accommodate well for intermittent connectivity and mobility, multicast, and broadcast are natively supported. Then, the work will focus on configuring a BlockChain network using Fabric framework provided by Hyperledger [1] and designing a Graphical User Interface (GUI) that allows a user within the network to display its ledger in clear visualizations and dashboards.

The paper is organized as follows. In section II we propose a detailed state of the art about the IoT, BlockChain technology and NDN architecture. In Section III we present our proposed architecture. In Section IV, we present the chosen tool to implement our approach, we illustrate how our medical BlockChain is configured using the Hyperledger Fabric Framework and we validate it. Finally, Section V includes some conclusions and future developments.

II. State of the Art

In this section we investigate the concept of BlockChain technology in the Internet of Things [2] and the NDN paradigm. .

A. Internet of things IoT

The Internet of Things [3] enables physical objects to see, to hear, to interact, to communicate and to perform different tasks and jobs by having them ”talk” together in order to share information, to coordinate decisions and to collaborate toward a common goal. These connected things anytime soon will no longer be those traditional objects with limited capacities. Although, they will be transformed into smart objects with great computational and communication capabilities. Thanks to the fact of exploiting the Internet of Things' underlying technologies such as ubiquitous and pervasive computing, embedded devices and Internet protocols and applications. The use of the Internet to enable communication and collaboration between objects will offer new opportunities to the different systems but also will create new challenges that must be considered in order to realize its potential benefits. We distinguish 3 IoT Challenges : interoperability and standardization, identity management and security.

Most IoT smart devices will be connected through a common interface in order to communicate. Then, the task of standardization needs to be considered and redressed to provide interoperability among the various objects. Also, it is a mean to standardize the interaction and the communication among the network.

Identity management is also an important challenge in the Internet of Things that must be taken into account as millions of objects across the world are interconnected in various applications, thus the need for unique identification of each object arises. This calls for a naming and identity management scheme to be in place in order to dynamically assign unique names and identities to all the objects deployed worldwide and hence the importance of a data naming architecture for IoT systems such as Information Centric Networking Architecture (ICN) [4].

Traditional security mechanisms cannot be directly applied to IoT technologies due to the different standards and communication patterns involved. Moreover, the existence of such a large network of a high number of interconnected entities will definitely imply different scenarios of attacks. This will put all those devices at a high risk, thus harming the affiliated users. To cope with this challenge, cyber-security systems must offer adapted mechanisms to protect the collected data from the physical devices since it may store and manage sensitive user information. This means that at any moment IoT systems need to provide data confidentiality, integrity, and availability. This can be achieved by utilizing data encryption and data redundancy as well as authentication, access control and authorization mechanisms in order to prevent unauthorized users to access the system. However, in many situations, we have to protect ourselves as well as the whole system from the information providers since they can act deceitfully by providing false or misleading information and here traditional security mechanisms are unable to protect users against this type of threat. We need then to be sure that we are talking to the right thing, that it is operating correctly, that we can trust the information it provides and that no-one else can interfere along the way. Hence the importance of a secure distributed solution for IoT systems.

B. BlockChain technology

A BlockChain [5] [6] is a database that maintains the history of all the exchanges made between its users since its creation without the need for a central authority. This database or global ledger is secure and distributed: it is shared by its different users, without intermediaries, which maintains records of all the exchanges made between the nodes on a BlockChain network. This exchange is called transaction. The BlockChain shared characteristic allows everyone to check the validity of the chain. Each digital record or transaction in the thread is called a block and each block is linked to a specific participant and timestamped. Once a block is created, it has a unique hash, which presents its identity and all of its contents and it is always unique. Changing something inside a block would result in a total change of not only the local hash, but it influences all the following blocks.

1) Principles & Properties: The success and evolution of the BlockChain technology rise from 5 main characteristics [7], which are:

- Distributed Ledger: Distributed because there is no central certificate authority for transactions and the data is geographically replicated across multiple participants.
- Decentralized network: Decentralized because the network runs on a peer-to-peer basis.
- Immutable: Immutable because no one can change the data once it has been written to a BlockChain.
- Highly Secure: Highly Secure because if someone wants to alter previous records, there is a very high cost to succeed, as the ledger is shared among all nodes.
- Public: Public because everyone participating can access the contents of the registry without a request for permission. This does not mean everyone can see the actual content of the data sent since it is protected by the sender's private key.

2) Basic concepts: Before using the BlockChain, we need to understand the basic concepts of this technology.

- Node: Computer connected to the network and using a program relaying transactions.
- Ledger: Registry in which transactions of a system are recorded
- Hash function: A hash function is a particular function which, from a data provided in input, calculates an imprint used to quickly identify, although incompletely, the initial data. The functions of hash are used in computer science and cryptography.
- Hash: Result produced by a hash function
- Smart contracts [8]: They are programs, accessible and auditable by all authorized parties, whose execution is thus controlled and verifiable; designed to execute the terms of a contract automatically when certain conditions are met [9]. The rules governing the program may cover, for example, any verifiable event in a computerized manner. The digital and automated nature of the contract therefore theoretically allows two partners to establish a constraint without having to trust each other beforehand, without any central authority or intervention. It is indeed the system itself, and not its agents, that guarantees the honesty of the transaction.
- Mining [10]: The use of computing power to process transactions, secure the network and allow all users of the system stay synchronized.
- Consensus mechanisms: They are used to ensure that all nodes in the network (pairs) have the same information and that only valid transactions are recorded in the distributed registers. In other words, this is the way to validate BlockChain blocks. The most known BlockChain concensus are [11]: Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Hashcash, Zero Knowledge Proof.

3) BlockChain types: There are 3 types of BlockChains : public, private and consortium BlockChain.

- The public BlockChain is completely open where anyone can join and participate to the network. Each transaction is verified and synced with every node affiliated with the BlockChain. In order to achieve consensus, each node must solve a proof of work so as to ensure that all nodes are in sync. As example of public BlockChains we can cite [12]: Bitcoin, Ethereum, Litecoin.
- In the private BlockChain, an access control layer is built. The network owner has control over who can join the network, and who can participate in the consensus process of the BlockChain. The Bankchain [13] is an example of a private BlockChain.
- The consortium BlockChain is partly private but operates under the leadership of a group instead of a single entity. A consortium between a set of known entities is made to decide who has access to the BlockChain ledger, which transactions can remain public, and which must be restricted to a smaller group of members. Some example of Consortium BlockChain: Hyperledger [14], MultiChain [15], Openchain [16].

4) BlockChain tools: Because of its great use in the world, several BlockChain tools have been created, to name a few:

- IOTA [17] is a new public distributed ledger that utilizes a novel invention called ”Tangle”. Tangle is a Directed Acyclic Graph (DAG). Unlike the traditional BlockChain, it has no blocks, no chain and no minors. IOTA supports nano-payments without transaction fees.
- MultiChain [18] is a private permissioned BlockChain that provides direct interface with many parameters. It uses a publish API to add a data stream. Then, each node can subscribe to those streams that is interested in. Mutichain may be a preferred choice for the private BlockChains especially because it has the advantage of an easy-to-interact-with API.
- Hyperledger is an open source IBM BlockChain product hosted by the Linux foundation. It is the most complete private BlockChain on the market, but it is also one of the most complex [1] to deploy. The set of components that must be implemented for a single node to be operational requires a lot of engineering and configuration. Fabric, Sawtooth and Ihora are the frameworks proposed by Hyperledger

C. IoT-BlockChain

Many studies focused on the use and adaptation of the BlockChain in the IoT context [19]. Among them, those that illustrate the use of this technology in the field of health care, whether for public health management, medical research based on the personal data of patients or for quality assurance in the production of drugs. Other researchers [20] presented an adaptation of the BlockChain for the smart home case. By clustering devices and adding local BlockChains, which show that it is possible to reduce the load on the network while ensuring the security of users' data and the protection of their private lives. Finally, smart contracts [21] can be interesting for IoT because they allow the automation of long processes while ensuring their verifiability.

The integration of the BlockChain into the IoT will lead to significant transformations in several sectors, leading to new models and requiring us to reconsider how existing systems and processes are implemented. The BlockChain can also offer a way of ensuring the security of user data as well as the protection of privacy, thus allowing for a greater adoption of IoT.

The adoption of BlockChain in IoT is not simple and leads to the following defects:

- Power and processing time: IoT networks are formed by devices that have different computing capabilities and not all of them able to run the same encryption algorithm at the desired speed. Indeed, the mining requires a computing capacity and the majority of the equipments will not be able to manage it. In addition, it takes a lot of time and IoT applications may require short response time.
- Storage: The BlockChain register must be stored on the nodes themselves. The needed storage space will increase in size as time goes on. This is beyond the capabilities of a wide range of intelligent devices such as sensors, which have a very low storage capacity.
- Traffic Overhead: The underlying BlockChain protocols create significant network traffic that may be undesirable for IoT devices with limited bandwidth.
- Scalability: BlockChain fails badly as the number of nodes in the network increases. Whereas, IoT networks can contain a large number of nodes. Thus, BlockChain is a promising technology for IoT but not straightforward and have to be adapted. We will present in the next paragraph the architecture proposed for IoT-BlockChain called smart home architecture.

Authors in [20] [22] proposed a smart home architecture that combines IoT and BlockChain technologies. This solution is a new instantiation of BlockChain that eliminates the concept of PoW and the need for rewards. The framework relies on the hierarchical structure and distributed trust to maintain the security and confidentiality of BlockChain while making it more specific to IoT requirements. However, the IoT-BlockChain architecture has not yet been implemented and it does not propose the most suitable BlockChain tool to its realization. Also, the existing architecture does not promote mobility. Hence the need for a paradigm to manage all the data in a secure way which can be supported by IoT devices. Thus the need for the NDN architecture.

D. The NDN architecture

The Information Centric Networking Architecture (ICN) [4] [23] has been recently proposed as an alternative to the TCP/IP communication model for a future Internet. ICN focuses on the data and no longer on the location of the hosts and the contents can be stored in memory of each node of the path.

In ICN, a node broadcasts its interest in content / information by using the name of that content. Each node of the network can respond to this interest if it has the requested content, which makes the content independent of a specific address in the network. Thus, the ICN separates the identifier and locator roles, which highlights the fact that each data object will be identified using a unique name called Named Data Object (NDO) without being mapped to a specific location. This will lead to one of the main features of the ICN which is content independent caching, where network elements such as routers can cache recent contents and send them back to the request of other users, called seekers.

The Named Data Networking (NDN) [24] is an ICN architecture that is an evolution of Content-Centric-Networking (CCN) [25] and can be used in IoT. In NDN, names are hierarchical and can be read by a human. The NDN's data-centric enables developers to work with things and their data directly, and for IoT networks to be deployed and configured easily to promote mobility.

In this architecture, there are two types of packets [26]: Interest packets and Data packets. The browser of a user who is looking for a piece of music on the Net will generate an Interest packet. This packet will be broadcast according to a protocol that we can, as a first approach, describe as very similar to peer-to-peer protocols that we know.

The name of the requested thing (Content Name) has a hierarchical structure that resembles to domain names, such as : $/[group-name]/[hospital]/[division]/[domain]/[personal-id]/[data]$. This is why NDN offers easy, robust and scalable data retrieval. In fact, a data packet "satisfies" an Interest packet if the Content Name of the Interest packet is a prefix of that Data packet.

Moreover, an Interest packet can be received for a document that does not exist yet, but that the server can create it on the fly.

III. Proposed Approach : Health Care Monitoring Architecture

In our model we focus on a scenario of a remote health care monitoring of patients out of hospitals, that are followed remotely by a medical staff. For this end, we assume that each patient is equipped with some wearable sensors, able to measure continuously a predefined set of parameters of a health status of a person (like blood pressure and oxygen saturation, heart rate, body temperature, etc ...). Other sensors can also be installed at the patient's home to monitor its immediate environments and allow the detection of the activity of a person and events like falls for instance. The data issued by these wearable devices and the other sensors located at home is permanently uploaded to a remote database system. At this stage a live monitoring system takes over to analyze this data in order to detect anomalies and raises alarms if needed to clinicians who may take some actions remotely. This data is also stored to keep a track of all the raised events, and may serve as well to doctors that follows the health status evolution of the patients. All the transactions between the different parts of our scenario are made on very sensitive personal data. It is obvious that these medical reports should be confidential and have limited access in a global system that insure the non repudiation. To satisfy all these requirements we designed an architecture based on the

BlockChain technology to monitor the patient state remotely. Our architecture illustrated in Figure1 is mainly composed of two BlockChains, a monitoring system and medical devices.

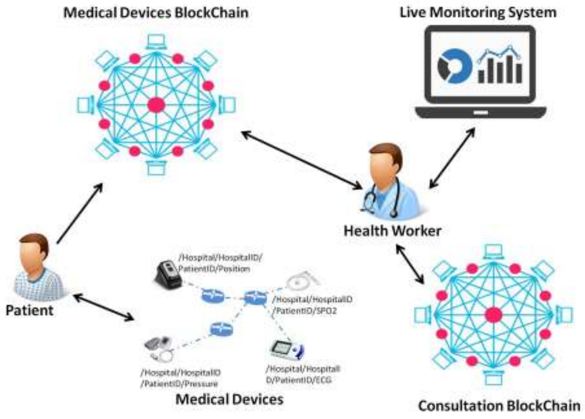

Fig. 1. Health Care Monitoring Architecture.

- Medical Devices BlockChain: In our architecture, each patient is monitored by a set of medical devices. This medical devices are in charge of collecting data that will be stored in the medical devices BlockChain. Hence, for each patient one medical devices blockChain is configured. The Smart Contract presents a part of the Medical Devices BlockChain. The use of the Smart Contract is explained in the next section.
- Consultation BlockChain: Unlike Medical Devices BlockChain, The Consultation BlockChain shown in our architecture is unique and it contains all the history of the patients records. This BlockChain is distributed between hospitals and include the patients records. Thus, it becomes easier and more secure to exchange the medical reports between hospitals and health workers. In our case, we choose to separate those two BlockChains because each one has its own purpose. The data received from the sensors needs to be maintained in the period of treatment. After, it will be not important to store it. However, patient records must be always available throughout the patient's life.
- Live Monitoring System: It is the entity that manipulates data continuously and analyzes the various information. It is basically used to make an alert (if necessary) to the doctor in case of emergency.
- Medical Devices: The data stored in the Medical Devices BlockChain is retrieved from the patient sensors with the NDN paradigm. That is to say that we define an hierarchy to enable communication between medical devices. In our case, the NDN naming convention is $Hospital/HospitalID/PatientID/DataName$.
- Health Worker: He can be a doctor, a nurse, an anesthetist ..etc. He represents a node (e.g. computer) in both Medical Devices BlockChain and Consultation BlockChain. He can visualize data through the Live Monitoring System based on the data stored in the Medical Devices BlockChain and He can either visualize or add data to the Consultation BlockChain.
- Patient: He is also a node (e.g. computer) of the Medical Devices BlockChain. He receives data from the Medical Devices and send them to the Medical Devices BlockChain to be stored in the ledger. The implementation of our architecture will be explained in details in the the next section.

IV. Approach implementation and Validation

In order to implement our architecture we choose Hyperledger Fabric since it respects the criteria of our requirements. In fact, neither IOTA nor MultiChain satisfies our needs. On the one hand, IOTA is a public, permissionless BlockChain that uses cryptocurrency, however, in our case we manipulate simple data messages. On the other hand, the MultiChain does not support the implementation of smart contracts. Although MultiChain follows the approach in which data is embedded immutably in a BlockChain, the Hyperledger Fabric frameworks is more suitable to our requirements since it adds a level of security and data privacy and offers a modular architecture.

1) Hyperledger Fabric: Fabric is an Hyperledger framework based on a modular architecture that offers high levels of privacy, resilience, flexibility and scalability. It is designed to support plug-in implementations of different components and adapt to the complexity and subtleties that exist in the economic ecosystem.

Among the fundamental concepts of Fabric technology, we can expose:

- Chaincodes: is a self-executing program (the equivalent of a Smart-contract) currently written in Go language.
- Channels: is a private "subnet" of communication between two or more specific members of the network, with the aim of carrying out private and confidential transactions.
- Ordering service: ensures the consistency and scheduling of transactions.
- Endorsement policies: are rules used to allow a node to decide whether a transaction is approved or not.
- Application SDK: is a software development kit that allows the interaction of the peers in the network.
- Endorsing peers: endorse a transaction before being committed according to endorsement policies specified in the chaincodes.
- Committing peers: receive blocks from the ordering service to validate them and update the state of data into State DB and the ledger.

2) Medical Devices BlockChain Configuration with Hyperledger Fabric Framework: Figure 2 shows how we configure the Medical Devices BlockChain illustrated in our approach using the Hyperledger Fabric Framework.

The Patient entity in our architecture corresponds to the Application SDK of the Fabric framework. It provides APIs to facilitate the interaction with the Medical Devices BlockChain.

A peer is a node which acts, in our case, as both an endorsing peer and a committing peer. It is a part of one or

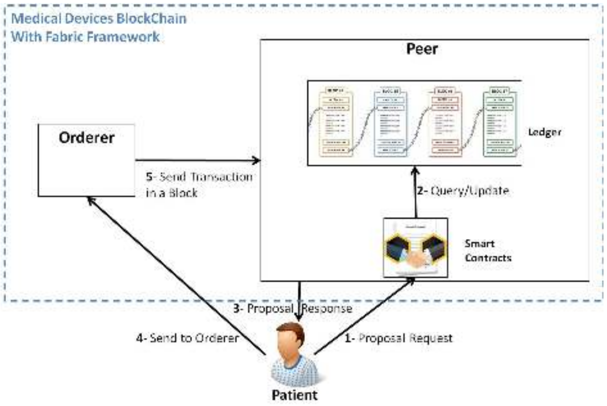

Fig. 2. Medical Devices BlockChain With Hyperledger Fabric Framework.

many channels. It contains one or many smart contracts (i.e. Chaincodes in the Fabric Framework) and a specific ledger for each channel.

The transaction proposal, which corresponds to the data received from the Medical Devices, is sent to endorsing peers to approve the proposal. It executes the Chaincode, to access to the ledger. Then, according to the endorsement policies, the endorsing peer decides whether a transaction is valid or not. If it is valid, the endorsing peer signs the proposal and sends a response to the Application SDK. Once the Application SDK receives enough approval for the same transaction using Practical Byzantine Fault Tolerance algorithm, this transaction will be sent to the Ordering service.

The Ordering service takes the validated transactions from the Application SDK, creates the blocks and send them to the committing peers. This committing peer takes the block and updates the ledger.

A. Running examples

We validate our approach at a design level by running two examples. The first example illustrates how to visualize the last data of each sensor and the second one present two use cases that illustrate the data processing.

1) Sequence Diagrams:

a) Visualize Last Data Sequence Diagram: The sequence diagram in Figure 3 provides a detailed scenario description of visualizing last data of each sensor. The user must request the newest available data located on the page ”index.html”. This component sends this request to the controller which calls the factory to retrieve data. We use nodeJs and expressJs in the server side because this approach is more scalable and secure. Thus, the router uses the backend controller to check the availability of the data by turning to the service that executes the Chaincode. If it exists, the data will be displayed to the dashboard page.

b) Data Processing Sequence Diagram: The sequence diagram shown in Figure 4 represents the two use cases which are the storage of patient data in the BlockChain network and the request of its history.

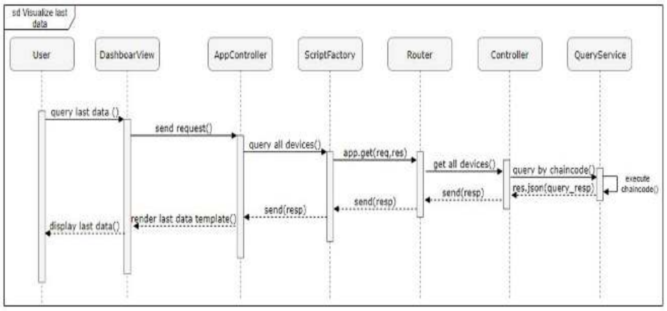

Fig. 3. Visualize Last Data Sequence Diagram.

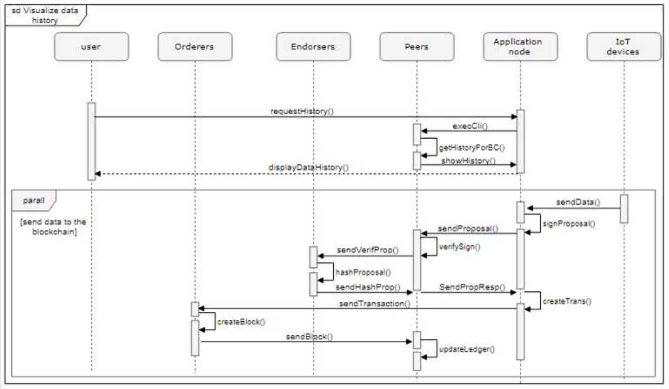

Fig. 4. Data Processing Sequence Diagram.

When a new data comes to the application node, it will be directed to the BlockChain and sent via Chaincodes. This process needs first the creation of the proposed transaction (called a proposal) and sending it to the peers. These latter verifies the transaction and sign it to invoke the endorser system which chooses to endorse or collect the proposed transaction according to the endorsement policy.

Peers give back to the application node the proposal response that is used for transaction verification, validation and achieving consensus. With this response, the client creates transaction after checking the endorsement policy and resend it to the peers. Thus, the peers transfer the transaction to the orderers where the consensus algorithm will be run and a block of one or many transactions will be created. After its creation, the block is delivered to other peers to update their ledgers.

B. Achievement: Dashboard interfaces

The main aspect of our application is to visualize data related to a particular patient. Not only the last one but also the history extracted from a log file. After successful authentication, the user has the privilege to query last data via the GUI. Furthermore, he may visualize the transactions history, get the patient position on the map or consult his profile. The Graphical User Interface (GUI) contains the following parts:

- Dashboard: which give real-time information on the current state of the BlockChain: the name of the data, its value, etc as shown in Figure 5

- Account: represents the available information related to the patient.
- A map: Allows the health worker to locate position of the patient to intervene in case of emergency.
- Charts: A graph that summarizes previous information about the provided data.

Clicking on the charts from the list on the left displays the history interface which contains charts displaying the data for the past hours as well to allow the health worker to establish a comparison between the outputs and the patient state. Each chart contains the information that corresponds to a precise data, namely its timestamp and its value as shown in Figure 6.

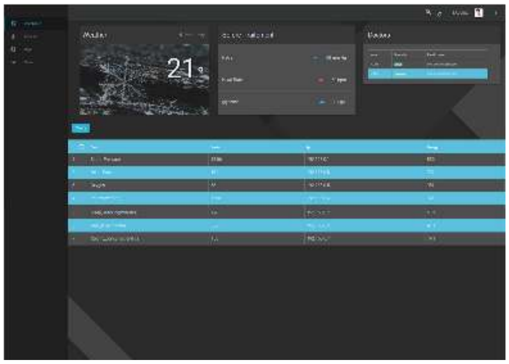

Fig. 5. Dashboard interfaces to visualize last data.

Fig. 6. Interface of the history of data stored.

V. Conclusion

In this paper, we focused on health care monitoring where the data collected by the deployed devices are critical. Our aim was to provide a distributed and secured access to these critical data using the emerging BlockChain technology. In this study, we designed an IoT-BlockChain architecture for a health care monitoring application. We explored the different BlockChain tools and we chosen Fabric Hyperledger to implement our architecture. We validate our approach by running examples and showing some implemented functionalities. As a future work, we aim to implement more functionality to get a complete IoT-BlockChain framework dedicated to health monitoring.

References

[1] Shikha Maheshwari. Blockchain basics: Hyperledger fabric. https://developer.ibm.com/articles/cl-blockchain-hyperledger-fabric-hyperledger-composer-compared/, 2018. [Online; accessed Feb-2019].

[2] Veena Pureswaran and Paul Brody. Device democracy : Saving the future of the internet of things. Technical report, IBM Institute for Business Value, The United States of America, 7 2015.

[3] Y. Zhang and J. Wen. An IoT electric business model based on the protocol of bitcoin. In *2015 18th International Conference on Intelligence in Next Generation Networks*, pages 184–191, Feb 2015.

[4] Cenk Gündogan, Peter Kietzmann, Thomas C. Schmidt, Martine Lenders, Hauke Petersen, Matthias Wählisch, Michael Frey, and Felix Shzu-Juraschek. Information-centric networking for the industrial iot. In *Proceedings of the 4th ACM Conference on Information-Centric Networking*, ICN '17, pages 214–215, New York, NY, USA, 2017. ACM.

[5] Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. BlockChain Technology Beyond Bitcoin. Technical report, Sutardja Center for Entrepreneurship and Technology, University of California, Berkeley, 10 2015.

[6] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In *International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, 6 2017. IEEE.

[7] Vitalik Buterin. A next-generation smart contract and decentralized application platform. Technical report, IBI, International Blockchain Inverstments, 2016.

[8] K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, 2016.

[9] Blockchain France. Les applications prometteuses des smart contracts. https://blockchainfrance.net/2016/01/28/applications-smart-contracts/, 2016. [Online; accessed 28-January-2016].

[10] Arshdeep Bahga and Vijay K. Madisetti. Blockchain Platform for Industrial Internet of Things. *Journal of Software Engineering and Applications*, 9(10):14, 2016.

[11] newgenapps. 8 Famous Blockchain Consensus Mechanisms and their Benefits. https://www.newgenapps.com/blog/8-blockchain-consensus-mechanisms-and-benefits, 2018. [Online; accessed 19-April-2018].

[12] BLOCKCHAIN Luxumbourg S.A. Blockchain. https://www.blockchain.com/, 2018. [Online; accessed 2018].

[13] Primechain Technologies. Bankchain Community. http://www.bankchaintech.com/, 2016. [Online; accessed 2016].

[14] The Linux Foundation. he Hyperledger Greenhouse. https://www.hyperledger.org/, 2018. [Online; accessed 2018].

[15] Coin Sciences Ltd. Open platform for building blockchains. https://www.multichain.com/, 2018. [Online; accessed 2018].

[16] Coinprism. Blockchain technology for the enterprise.

[17] Serguei Popov. The tangle. Technical report, IOTA, 10 2017.

[18] Gideon Greenspan. Introducing MultiChain Streams. https://www.multichain.com/blog/2016/09/introducing-multichain-streams/, 2016. [Online; accessed 15-September-2016].

[19] M. Conoscenti, A. Vetr, and J. C. De Martin. Blockchain for the Internet of Things: A systematic literature review. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pages 1–6, Nov 2016.

[20] Ali Dorri, Salil S. Kanhere, and Raja Jurdak. Blockchain in Internet of Things: Challenges and Solutions. *CoRR*, abs/1608.05187, 2016.

[21] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 839–858, May 2016.

[22] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, March 2017.

[23] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos. A survey of information-centric networking research. *IEEE Communications Surveys Tutorials*, 16(2):1024–1049, Second 2014.

[24] Divya Saxena, Vaskar Raychoudhury, and Nalluri SriMahathi. Smarthealth-ndnot: Named data network of things for healthcare services. In *Proceedings of the 2015 Workshop on Pervasive Wireless Healthcare*, MobileHealth '15, pages 45–50, New York, NY, USA, 2015. ACM.

[25] Bengt Ahlgren, Anders Lindgren, and Yanqiu Wu. Demo: Experimental feasibility study of ccn-lite on contiki motes for iot data streams. In *Proceedings of the 3rd ACM Conference on Information-Centric*

Networking, ACM-ICN '16, pages 221–222, New York, NY, USA, 2016. ACM.

[26] Cenk Gundogan, Thomas Schmidt, and Matthias Wahlisch. Publish-subscribe deployment option for ndn in the constrained internet of things. Technical report, HAW Hamburg and Freie Universitt, 3 2018.