Blockchain and IoT for Security and Privacy: A Platform for Diabetes Self-management

Kebira AZBEG*, Ouail OUCHETTO, Said JAI ANDALOUSSI, Leila FETJAH, Abderrahim SEKKAKI
LR2I Lab, Dept. of Mathematics and Computer Science, Faculty of science Ain-chok, Hassan II University of Casablanca
Casablanca, Morocco
azbegkebira@gmail.com, {ouail.ouchetto, said.jaiandaloussi, leila.fetjah, abderrahim.sekkaki}@etude.univcasa.ma

***Abstract*—Diabetes is one of the most common disease over the world which requires a daily self-care in order to be controlled. Nowadays, diabetes self-management can benefit from the recent advanced technologies such as Internet of things (wearables and medical sensors) to take measurements and track health data. In this paper, we present a platform architecture based on the IoT and Blockchain to facilitate the follow-up of diabetes and to help patients to self-manage it properly. Our architecture combines the IoT with the Blockchain technology in order to collect patients' data, share it with their healthcare teams in a near real-time and in a secure manner while preserving patient's privacy.**

***Index Terms*—Blockchain, IoT, Diabetes Self-management, Healthcare, Security, Privacy**

I. Introduction

Diabetes is a serious disease that requires a particular self-care and a better follow-up in order to be controlled. According to the global report on diabetes, done by the World Health Organization, 422 million people in the world had diabetes in 2014 with a prevalence of 8.5% in the adult population, compared to 4.7% in 1980. In 2012, 1.5 million deaths are caused by diabetes and 2.2 million deaths by high blood glucose. 43% of these deaths occur before the age of 70 years [1]. Over time, uncontrolled diabetes can lead to several and serious health complications such as heart disease, kidney failure, vision problem, amputation, nerves and blood vessels damage. Patients must take diabetes seriously by following a good care plan and adopting an adequate lifestyle. This in order to stay healthy and prevent the short and long-term diabetes complications. In addition, to take medicines and follow a diabetes meal plan, patients should check regularly their weight, blood pressure and blood sugar. These measurements should be recorded and shared with medical teams in order to ensure a collaborative care.

The use of the Internet of Things, especially medical devices, wearables and sensors, will improve diabetes care by collecting health records automatically, such as blood pressure and glucose levels regularly. It will also help patients to share data and interact with their physicians in near real-time and then allows them to track diabetes information.

Multiple healthcare applications and platforms have been proposed for patient monitoring, healthcare management and health systems diabetes by using IoT [1] [2] [3]. However, in these approaches, we still have some issues in security and privacy.

One of the main goals of the Health Insurance Portability and Accountability Act (HIPAA) [2] is to ensure the privacy and security of health information when it is transfered, received, handled, or shared. Then, the security of medical records is an imperative aspect which must be guaranteed. Nowadays, several researches are trying to enhance this aspect by using the Blockchain technology. In [4], the authors proposed an architecture to manage permissions and medical data access using smart contracts. Their approach allows patients to manage access to their own medical data by deploying specific smart contracts in the Ethereum Blockchain [5]. Another research proposed a mobile application for collecting health data and sharing it with healthcare providers and insurance companies [6]. They used a permissioned Blockchain based on Hyperledger Fabric to ensure privacy, integrity protection and to store access control policies. In [7], "Ancile" is a framework based on a permissioned Blockchain to manage access control and increase interoperability in the case of electronic health records (EHR). The framework uses Ethereum Blockchain to store access permission and references to data, whereas patient's data still stored in the providers' databases. Six types of smart contracts are used in this framework to define permissions and execute other operations. Another work aims to manage access to eHealth data by using a gateway to handle data generated by sensors. An off-chain database, based on IPFS, is used to store data and an Ethereum Blockchain is used to deploy smart contracts in order to manage access to this data [8]. However, these approaches didn't take in consideration the security at the local level when data is transmitted from sensors to the gateway.

In this paper, we focus on that level. We aim to develop a decentralized application for handling information and registering devices in order to prevent addition of malicious devices. We propose a data management architecture based on the combination of IoT and the Blockchain technology. This architecture will allow diabetic patients to collect their medical data and share it automatically with their physicians in a secure manner. Patients will also be able to control access to their data, improve the integrity and protect their privacy.

The rest of this paper is organized as follows: Section II

[1] http://apps.who.int/iris/handle/10665/204871

[2] http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx

presents the importance of using IoT to self-manage diabetes. Section III discusses some use cases of using Blockchain technology to secure IoT. Section IV presents our approach and describes our architecture. In Section V, we present the system implementation and, in Section VI, we conclude the paper and introduce some future works.

II. Diabetes self-management

Diabetes management is very important to live healthy and have a near normal life. It is about keeping blood sugar close to normal in order to prevent diabetes complications. Diabetes management is mostly self-management and it requires a serious self-care concerning food planning, exercises, regular checkups of blood glucose and so on. Nowadays, self-management can benefit from technology advancements by using IoT devices like glucometer sensor to determine the approximate concentration of glucose in the blood. The use of IoT can help patients to keep track of their medication, take measurements and share them with their medical team. Over the past few years, there have been suggested several eHealth applications based on the IoT for diabetes management, but they still face some issues and challenges regarding security and privacy [3].

III. Blockchain and IoT

The number of connected devices is growing exponentially. The Gartner's predictions show that by 2020 we will have 20 billion devices connected to the Internet [3]. Every year, thousands of devices join the Internet and store their data on centralized servers. This architecture raises several questions regarding security and privacy [4], especially when devices manage sensitive and personal data. The implementation of security should take in consideration the adoption of the security model based on three essential parts: confidentiality, integrity and availability. These parts can be supported by using some tools and common security measures such as access control, encryption, firewall, intrusion detection system, redundancy methods and so on [9], or by using the Blockchain technology which can be a good solution to achieve the security model.

In terms of data security, the level of challenge is high, especially in the case of sensitive and critical data which are managed through smart health solutions. The Blockchain, which already secures Bitcoin transactions [10], could add a security layer in the IoT area.

In recent years, several researches and companies use the Blockchain technology in order to secure the IoT, manage access control and verify integrity. In [11], the authors provide a way to manage IoT devices by using the Ethereum Blockchain. Smart contracts were used to track the use of electricity by a meter and to configure policies in order to control the use of energy. In the other side, A. Dorri et al. propose to use both private and public Blockchain to secure IoT devices [12]. The local communication and policies storage are assured by a private Blockchain which is managed centrally by a smart home miner. A public Blockchain is used to handle transactions outside the smart home. In [13], Authors propose FairAccess, which is a Blockchain-based framework to manage access control for IoT by using smart contracts to define policies and distribute authorization tokens. Another work in progress tries to connect IoT end-devices with low power and storage capabilities to a Blockchain infrastructure [14]. They used Ethereum Blockchain and LoRa gateway for routing data and verifying integrity.

[3]https://www.gartner.com/newsroom/id/3165317

[4]https://www.bbvaopenmind.com/en/iot-and-blockchain-challenges-and-risks/

IV. Our approach

In this work, we present a detailed architecture of our proposed approach. We aim to create a platform to smart self-care and follow-up of diabetes by combining IoT devices and Blockchain. The advantage of using IoT is to facilitate data collection and make its sharing automatic. On the other hand, the platform benefits from Blockchain's security and smart contracts to achieve authentication, integrity, privacy and traceability. This will allow patients to have a total control over their data. They will be able to define access policies, permissions and to know who accessed? to what? and when?

The challenge with this combination is that medical devices used for diabetes self-care have low storage and computing power capacities. This makes their integration in a Blockchain infrastructure a complicated task. Mostly they don't support an installation of a light client to become a node in the Blockchain network. Some works proposed to use gateway as a Blockchain node in order to forward data from sensors to Blockchain [12]. However, we still have issues on how to secure the connection between patient's devices and gateway. For example, a third party can add malicious devices to transmit wrong data or to damage the gateway. Our work is focused on how to strengthen security at this level. The solution is to register each new device in the Blockchain by its owner, thus unknown device can not access to the platform unless the owner registers it and gives it permission.

To explain our proposed architecture, Fig. 1, we can divide it into four parts: connected devices, Blockchain network, smart contracts and medical team.

A. Connected devices

Connected devices are divided into two types. The first one encompasses medical devices, sensors and wearables that collect information about patient's health such as blood pressure, glucose level, heart rate, weight, and other necessary measures for diabetes monitoring. These devices take measurements and share them automatically with the healthcare team through smart-phone. The second type is a smart-phone, this device is used as an intermediary between medical devices and Blockchain network. It uses a mobile application for handling, encrypting information and routing it from devices to an off-chain database which can be accessible by authorized physicians and healthcare teams. The patient will be able to interact either with their devices and physicians by using this

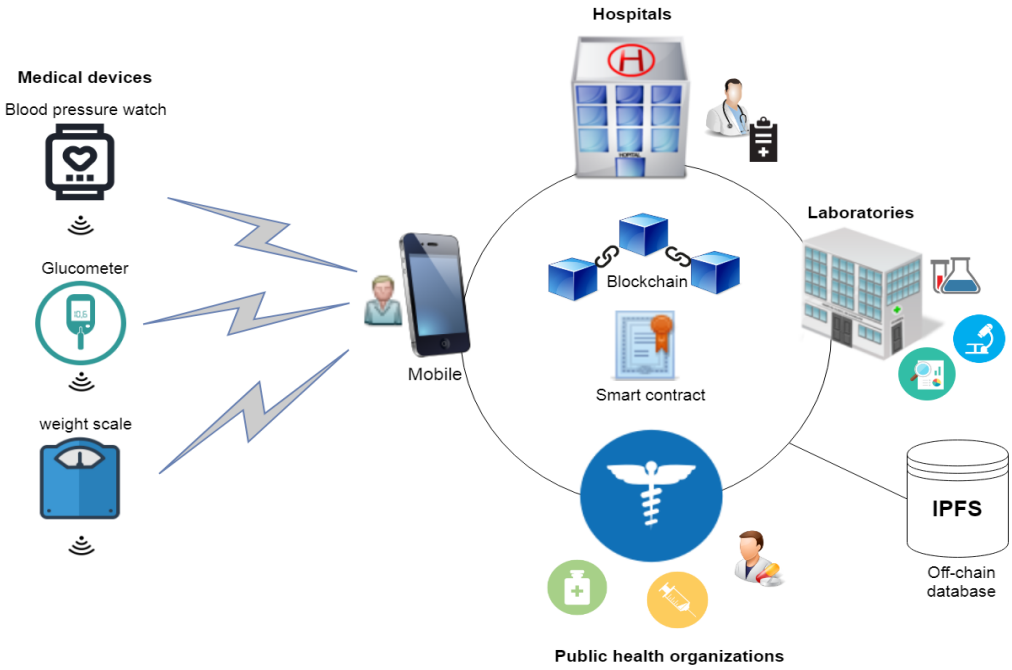

Fig. 1. Platform architecture.

application. He will be able to grant or revoke access and permissions, add or remove a device which will be translated by our application to an add/remove transaction forwarded and stored in the Blockchain network. The choice of smart-phone as a gateway is not arbitrary since the patient is always in move, he cannot be at home all the time. So we need a secure system able to follow him everywhere; at home, at work and even when he travels.

B. Blockchain network

The medical devices are linked to a permissioned Blockchain thanks to smart-phones. All patients will play the role of light nodes using their smart-phones, because of their limited storage capacity. Hospitals, laboratories and public health organizations will be full nodes. They will store a pointer to data, validate transactions, create blocks and append them to the Blockchain. This Blockchain will be used to store access control policies and enhance security as well as keeping traceability of each patient's data by recording every manipulation made on this data. The Blockchain will store just a pointer (a data hash) to data, while health data will be encrypted and stored in an off-chain database as a key-value. The off-chain storage is maintained by a peer-to-peer distributed file system (IPFS). Each patient will encrypt its data and store it in the IPFS which will generate the hash that will be stored in the Blockchain.

Patients have the choice to grant access to other parties or not. They have also the ability to choose what data to keep visible and for whom. All health entities can have access to the information while keeping patient privacy, because data are encrypted and each patient is identified just by an ID (his public key). This last represents him in the Blockchain and makes his identification impossible. In case of emergency, medical team must be able to view some data, thus each patient should select in advance this data, encrypt it and distribute the decryption key by using the secret sharing method. Then to decrypt this data, the medical team should cooperate with one or more members of patient's family to have the decryption key.

C. Smart contracts

Smart contracts are programs built, compiled into byte code and then deployed in the Blockchain network. Each smart contract is identified by a unique address and can be triggered by transmitting a transaction to this address. Once the predefined conditions are realized, the smart contract will be executed automatically without third party intervention. In this work, smart contracts will be used to create a log for traceability by registering every manipulation made on data. It will also be used to register or delete devices, grant or revoke access, define policies and authentication verification.

D. Medical team

It can be public health organizations, diabetes management center, researchers, pharmaceutical laboratories, clinics or healthcare professionals in general. These entities will be connected through a permissioned Blockchain to have access to data. This will allow physicians to follow their patients' health and public health organizations to extract information in order to use it in research or statistics for example.

V. System Implementation

In this section, we present different tools needed to implement our approach.

- A permissioned Blockchain: Since our Blockchain handles sensitive medical data that requires a high level of security and privacy control, we will use a permissioned Blockchain. This type of Blockchain can restrict the nodes who are eligible to participate in the consensus algorithm. The consensus is reached by using proof of authority (POA). This consensus algorithm allows only the predefined validators (full nodes in our case) to append blocks to the Blockchain and secure the network. Thanks to POA, we will get a faster Blockchain that requires less computing resources and thus lower energy consumption. In the tests, a private Ethereum Blockchain is used.
- A decentralized application (DApp) is needed to interact with the Blockchain. A DApp is a decentralized application that works on a peer to peer network without the need of a central server. It has a lot of characteristics, due to its decentralized nature, which make it very interesting. It has a client side (front-end) written in HTML, CSS and JavaScript. Instead of connecting this side to a backend web server, it is connected to a Blockchain then linked with smart contracts. In our case, the patient will use the application interface to make different transactions Fig. 2.

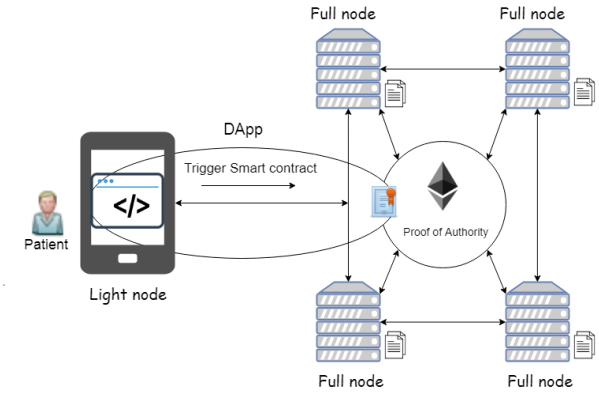

Fig. 2. Patient interaction with Blockchain through a decentralized application.

- Transactions: Each physician will add and register his patients in the Blockchain by generating for each of them a QR code. This QR code will contain the physician's Ethereum address and the Blockchain network information. Once the patient is registered in the Blockchain, he will be able to execute different transactions or actions; add/remove devices, grant/revoke permissions to other nodes, define policies, access to his data and show some summaries or dashboards. Our DApp will trigger smart contracts in order to launch these transactions and store it in the Blockchain for traceability. The patient will be added and registered in the Blockchain by his physician.
- Device registration: In this step, the patient will register each new device in the Blockchain by using an add_transaction. Each device will be identified by a unique set of values; its identifier (represented by its MAC address) and its owner's identifiers (Patient's public Ethereum address) Fig 3. Thus no one can add a device except the patient. In this way the patient can have a total control over his devices and can be protected against malicious devices.
- Data encryption: Data will be encrypted by the patient before being stored in the IPFS. If a party wants to access to data, it sends a transaction through the DApp and a smart contract will check its eligibility. If the party has access permission, then the patient will send the decryption key encrypted by the public key of the authorized party. Thus to access to data, the authorized party will decrypt the message with his private key to get the decryption key.

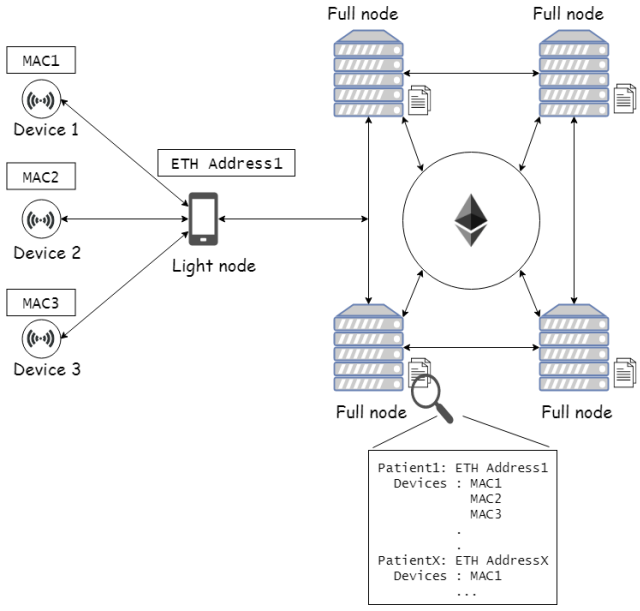

Fig. 3. Devices registration.

VI. Conclusion and Future Works

Controlling and managing diabetes is a very important thing that can be done by supervising health information such as blood glucose levels regularly. To make that process automatic, the use of IoT devices is necessary. In this way the patient can ensure the collect of his health information regularly and in some cases automatically. In other hand, this information should be shared with a medical team in a secure and faster way, thus the necessary of using a secure system. In this paper, we propose a platform based on the combination of IoT and Blockchain to collect health data and share it with health entities in order to have a daily smart care.

In our proposition, we focused on the patient privacy and the security between patient's devices in order to protect against

malicious devices. We chose proof of authority as a consensus algorithm for a faster system and cheaper in terms of energy and time. In this paper, we presented just a global overview of our approach. Currently, we are working on making a detailed conception for each component of our system. The next step is to implement our system by giving a proof of concept to demonstrate the feasibility of our approach and to verify its performance, then to suggest some ameliorations if needed. Another future work is the use of artificial intelligence in order to analyze node behaviors so that the system can identify abnormal node behaviors in real time.

ACKNOWLEDGMENT

This work is supported by the National Center for Scientific and Technological Research (CNRST).

REFERENCES

[1] M. A. Al-Taee, W. Al-Nuaimy, A. Al-Ataby, Z. J. Muhsin, and S. N. Abood, "Mobile health platform for diabetes management based on the internet-of-things," in *Applied Electrical Engineering and Computing Technologies (AEECT), 2015 IEEE Jordan Conference on*. IEEE, 2015, pp. 1–5.

[2] K. Darshan and K. Anandakumar, "A comprehensive review on usage of internet of things (iot) in healthcare system," in *Emerging Research in Electronics, Computer Science and Technology (ICERECT), 2015 International Conference on*. IEEE, 2015, pp. 132–136.

[3] S. Deshkar, R. Thanseeh, and V. G. Menon, "A review on iot based m-health systems for diabetes." *International Journal of Computer Science and Telecommunications*, vol. 8, no. 1, pp. 13–18, 2017.

[4] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Open and Big Data (OBD), International Conference on*. IEEE, 2016, pp. 25–30.

[5] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform, 2014," *URl: https://github.com/ethereum/wiki/wiki/White-Paper (visited on 10/09/2016)*, 2014.

[6] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on*. IEEE, 2017, pp. 1–5.

[7] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[8] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchain technology for ehealth data access management," in *Advances in Biomedical Engineering (ICABME), 2017 Fourth International Conference on*. IEEE, 2017, pp. 1–4.

[9] M. FRUSTACI, P. Pasquale, A. Gianluca, and G. FORTINO, "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE Internet of Things Journal*, 2017.

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[11] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *Advanced Communication Technology (ICACT), 2017 19th International Conference on*. IEEE, 2017, pp. 464–467.

[12] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*. ACM, 2017, pp. 173–178.

[13] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.

[14] K. R. Özyılmaz and A. Yurdakul, "Work-in-progress: integrating low-power iot devices to a blockchain-based infrastructure," in *Embedded Software (EMSOFT), 2017 International Conference on*. IEEE, 2017, pp. 1–2.