Integrating Blockchain with IoT for a Secure Healthcare Digital System

Nada Chendeb, Nour Khaled, Nazim Agoulmine

Integrating Blockchain with IoT for a Secure Healthcare Digital System

Nada Chendeb[1], Nour Khaled[1], and Nazim Agoulmine[2]

[1] Lebanese University, Faculty of Engineering
nchendeb@ul.edu.lb, nouna.nour97@gmail.com
[2] University of Evry Val d'Essonne - Paris Saclay University
nazim.agoulmine@ibisc.univ-evry.fr

Abstract

In the past few years, the number of wireless connected devices has increased to a number that could reach billions in the next few years. While cloud computing is being seen as the solution to process this data, security challenges could not be addressed solely with this technology. Blockchain is the technology that underpins Bitcoin, it introduces manners to provide a fully autonomous secure system, by using smart contracts. Multi-layer BC is a very powerful solution to overcome many IoT challenges. This paper illustrates how Blockchain works, what are the IoT challenges, and how it can be integrated with Blockchain. We proposed in this work a multi-layer IoT/blockchain based architecture customized and designed to be used in the medical field. With this information interact many parties including the doctors, health service providers, insurance companies and pharmacies. The ultimate goal being to solve the problem of scalability and performance.

1 Introduction

Data generated from IoT devices is increasing dramatically. One of the most interesting applications of IoT is e-health or intelligent medical care. Medical data generated by IoT devices is critical and sensitive to any unauthorized access. This data should be protected carefully because it is directly related to patient's life. Security concerns are more accentuated in the medical field and need a special attention especially when this field embraces IoT.
In parallel to the advancement in the e-health domain, a new technology that was conceived first to secure financial transactions of the famous cryptocurrency bitcoin, was and still developing to find its applications in many domains including the medical field. Blockchain technology is a peer-to-peer technology that provides a global consensus and assures that no one can alter or change previously validated transactions. Blockchain is a very good solution for security but it still suffer from some problems especially when used by IoT devices. In this case, arise multiple problems such as scalability, complexity and architectural based problems. In this work, we aim to build an intelligent medical system in which all partners interact in an IoT/Cloud environment with protocols for communication, management and sharing of private data using blockchain technology. We aim mainly to solve the problems related to the integration between IoT and blockchain.
The remaining of this paper is organized as follow: section 2 contains some preliminaries to understand the topic and section 3 contains a discussion of the related work. In section 4 we present our design and solution for a new architecture integrating blockchain and IoT and in section 5 we discuss this architecture and explain how it works in different medical data exchange scenarios. Finally, section 6 concludes the paper and gives some perspectives.

2 Preliminaries and Definitions

2.1 What is Blockchain?

Blockchain is an information technology that allows transactions to be verified by a group of unreliable actors. It provides a distributed, immutable, transparent, secure and auditable ledger [1. This is mainly a distributed database of all transactions or digital events that have been executed and shared among participating parties. Once entered in the blockchain, information can never be modified or erased. The blockchain contains a certain and verifiable record of every single transaction ever made [2]. In a blockchain network, whenever a new transaction (record) is created, a new block is automatically generated stating the date and the time (known as a "timestamp") when the record was entered in the block. Each new block is automatically linked to its previous block, all the way to the originating block, using the previous block's "Hash". Every time a new block is created, it is broadcasted in real-time to all connected computers that participate in the blockchain network. These computers are known as "nodes". While creating a new block, the node uses its own Private Encryption (Crypto) Key and the Public Crypto Key of the receiving node that is also a node in the network. Without its Private Key, no node can create a new block [3]. When we talk about information security, blockchain can be majorly divided into two parts: hashing and digital signatures [4].

2.2 Smart Contracts

A smart contract is a computer program that directly controls the transfer of digital information or assets between parties under certain conditions[5]. Blockchain is ideal for storing smart contracts because of the technology's security and immutability. Smart contract data is encrypted on a shared ledger, making it impossible to lose the information stored in the blocks.

2.3 Multi-layer Blockchain

Multi-layer blockchain can combine the benefits of blockchain and IoT and gives a solution for all the problems that cannot be solved by using one technology alone. By combining these two technologies, multi-layer blockchain gives a next-generation platform for IoT devices that are based on the blockchain technology. This is a multi-layered architecture, the main advantage of this architecture is to solve the problems faced by current blockchains mainly the lack of scalability. The IoT devices could be the nodes in the private blockchains, some of them are also part of the next layer public blockchain. We will base our proposed architecture on this main idea.

2.4 Mining

Mining is the concept of validating a block, it varies between different types of blockchain. What's important to know is the fact that a lot of computational power is needed for becoming a "Miner". Miners are usually rewarded, and mining might affect the whole system's performance.

3 Review of Literature

We start our discussion by the work done in [1] where we find three types of integration:
IoT- IoT: This approach could be the fastest one in terms of latency, and security since it can work offline. This approach is also applicable in scenarios involving only IoT devices.

IoT- Blockchain: In this approach, all the interactions go through blockchain, enabling an immutable record of interactions. Nevertheless, recording all the interactions in blockchain would involve an increase in bandwidth, which is one of the challenges.
Hybrid approach: Where only part of the interactions and data take place in the blockchain and the rest are directly shared between the IoT devices. In this approach fog/cloud computing [7] could come into play to complement the limitations of blockchain and IoT.
The last approach, may be a good candidate for our solution, the challenge posed by this approach is to optimize the split between the interactions that occur in real-time and the ones that go through the blockchain.

If we want to move to the architectures and models, authors in [8] speak about the Cloud Storage, Overlay network, etc. So, instead of saving the IoT data over blockchain, we use cloud storage servers to save the patient data. The cloud storage groups user's data in identical blocks associated with a unique block number. These clouds are connected to overlay networks, once the data stored in a block, the cloud server sends the hash of the data blocks to the overlay network. According to [9] and [10], the design consists of three core tiers that are smart home, cloud storage, and overlay network. Smart devices are located inside the smart home tier and are centrally managed by a miner. Smart homes constitute an overlay network along with Service Providers (SP), cloud storage, and users' smartphones. All transaction to or from the smart home are stored in a local private BC. Smart home miner is a device that centrally processes incoming and outgoing transactions to and from the smart home.

Furthermore, the architecture is more clarified in [11], where there is also three layers: device, fog, and cloud. At the edge of the network, the device layer is used to monitor the various public infrastructure environments and sends the filtered data that is consumed locally to the fog layer and uses the request services.
Most importantly, the authors of [12] make a full architecture that consists of three tiers: Tier 1 contains the constrained and unconstrained nodes (devices - sensors) and patient (gateway - aggregator), Tier 2 groups N Authorities (hospitals – labs – medical Insurance organization – medical research institute ...) and Tier 3 for the EHRs cloud providers (cloud storage servers for EHRs records).
Based on this study, and in order to meet the objective of our research, we will adopt the hybrid approach for IoT – blockchain integration with cloud storage of patients' data. A multi-layer blockchain is also a good candidate to alleviate the scalability problem. We think that not all IoT generated data in real time should be stored in the public blockchain, so a private blockchain for home related sensory data of the patient is a good solution, periodical report generated from the gateway could be stored in the public blockchain of a higher layer. A three-tier architecture is a good architecture for the system we will propose in the next section. This system will be mainly based on the solution proposed in [13] within the same research project.

4 The Proposed Three-Tier Blockchain Architecture

4.1 Baseline Solution/Design

Recently, members of the research project we are working on already proposed a basic architecture to secure medical data using blockchain [13], [14]. They proposed a communication protocol between nodes based on publish/subscribe model which is a model used specifically by IoT devices. They also propose an access control and management scheme based on the use of smart contracts, they define multiple smart contracts for publishers of IoT data, subscribers to

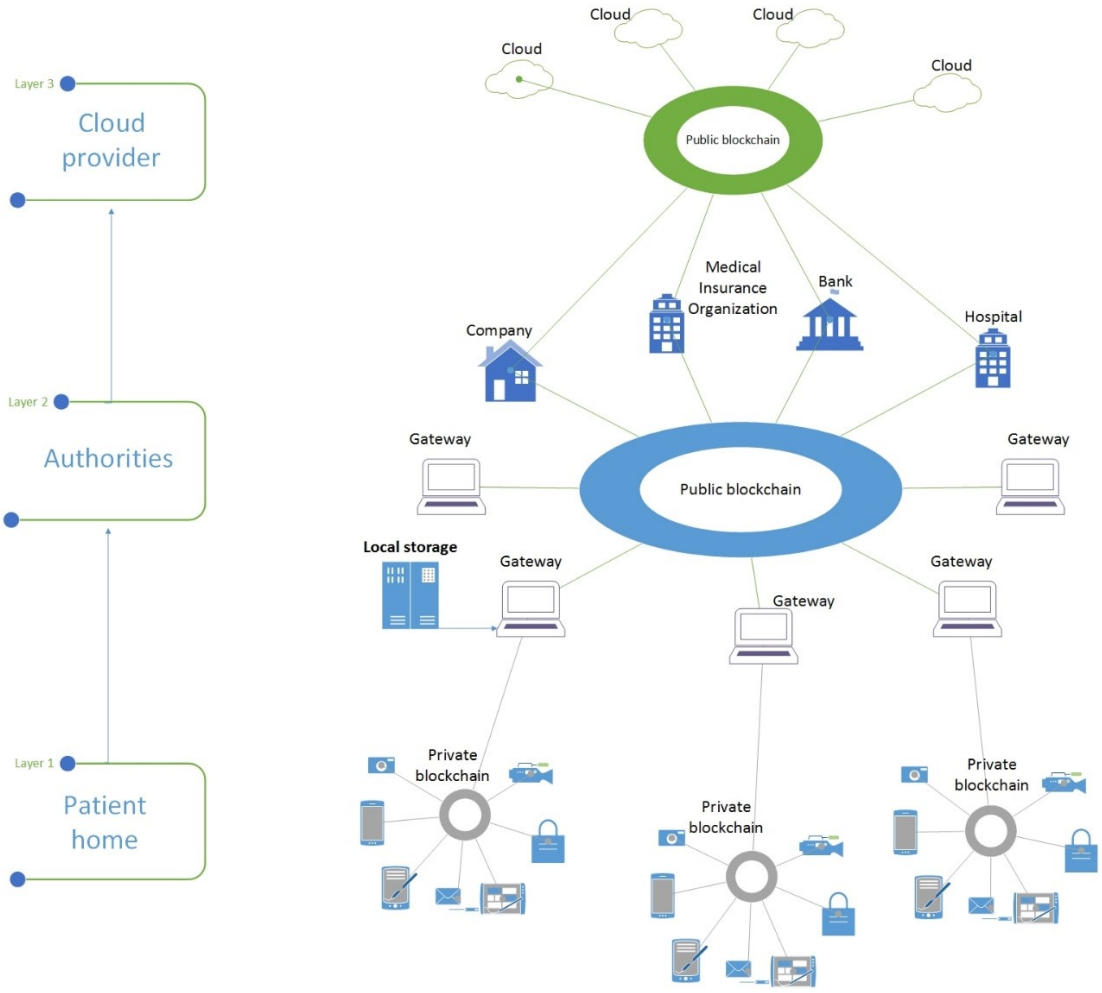

Figure 1: Integration of Blockchain with IoT, the three-layer architecture

that data and access permission done by the data owners. These smart contracts when executed define who can access to any generated data from any IoT device. Because IoT devices have capacity limitations, an off-chain storage was adopted to store the private data. Therefore, data is stored in distributed storage and hash of the data location is stored in the blockchain.
The proposed solution is a one-layer blockchain solution, which suffers from scalability limitations. In addition, IoT devices are data generators only and could not be considered as nodes in the blockchain making the integration of blockchain in the IoT very poor. We think that it is necessary to leverage this solution toward a better integration and better performance.

4.2 System Architecture

The system architecture is composed of three layers as shown in figure 1

Layer 1: This is the layer related to the "patient"; it includes all the IoT nodes gathering

information from a specific patient; medical information or any other type of information describing his environment. A main node in this blockchain is a powerful computer that will act as a gateway to higher layer blockchain. Note that each patient will have its proper blockchain.
Layer 2: This is the core layer or the "authorities" layer; it contains representative nodes for all interacting parties in the medical field who have interest in the data related to patients such as hospitals, medical centers, labs, etc. The gateways in the first layer are also members of this blockchain.
Layer 3: This is the higher layer or the "cloud provider" layer. In fact, IoT devices are in general completed by processing and storage capacities in the cloud. A blockchain at the cloud level is necessary to control the interaction between cloud providers in order to grant access for patient's data to each others wherever it is located.

To understand how the system will work, we recall that we are using the publisher/subscriber's model described in [13], smart contracts for access management and off-chain database for storage. In the core blockchain (layer 2), and based on the description of the access management in [13] we consider that:
○**Gateways:** are the publishers that generate all the data related to a certain patient (medical data). Publishers specify who can access and who has the permission to read/write/modify its data in the cloud (using smart contracts).
○**Authorities:** are the subscribers that are able to access the data of the publishers in the cloud. They also have the right to write and modify data according to the access rules specified by the publishers.
In the lowest layer, we propose to use private blockchain. In this platform, there is only one miner, which is the gateway in our case. Moreover, all IoT devices are generating data so the gateway pre-processes this data and generates records to higher layers. Hence, the gateway replaces all the IoT devices and acts like a publisher of the data generated from these devices.

4.3 Workflow in Different Scenarios

4.3.1 Scenario 1: The gateway collects IoT data and generates a new record

In this scenario, the entire network will be active. In the private BC (BlockChain), the sensors and their gateway are the nodes, so the miner is the gateway because it is the most powerful node in its private blockchain. Every device has to authenticate with the network before starting to send data by using public and private keys. These two keys are specific to each device. The gateway saves all the keys in its local storage to easily recognize any device that authenticates with it.
With every private blockchain, there might be a local storage. Note that only filtered, processed and abnormal data that reflects critical situations should be stored in the cloud. After completing the registration, the device starts creating a new block. This block, once validated by the gateway will be added to the patient's private BC (Figure 2). All the data collected is saved in the off-chain database (at the gateway local storage). The gateway processes the data and creates periodically medical records. However, the gateway has to be registered in the remaining two layers' blockchains: layer 2 to communicate with different types of authorities, and layer 3 to save some periodic records and the emergency data. All information in the next steps only concern the periodic/emergency records.

In the layer 2 blockchain, we have mainly the interactions between the patients and different types of authorities; we may also have interactions between the authorities themselves. Here we have the Proof of Work (POW) [15], and the Proof of Stake (PoS) to validate any transaction

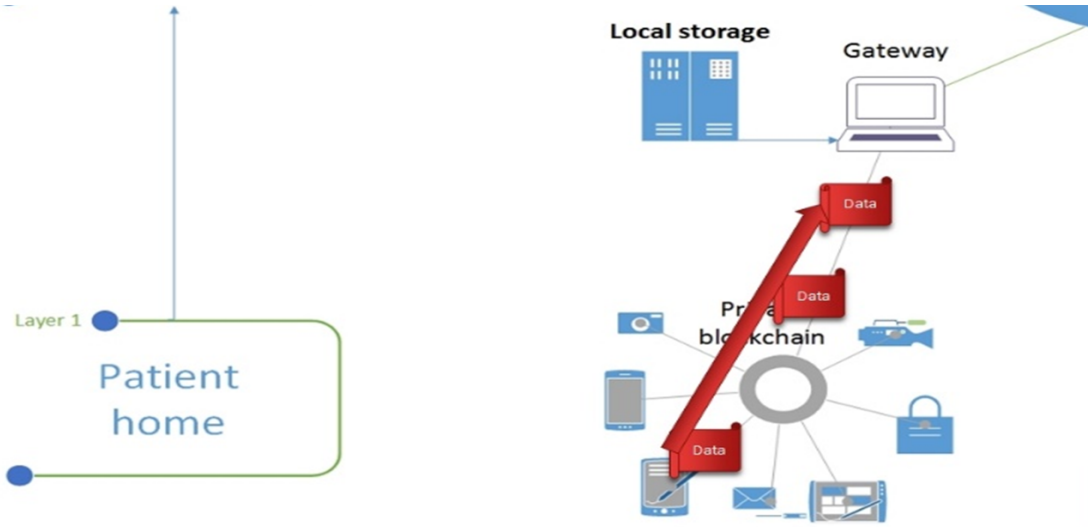

Figure 2: The gateway collects data from a device

based on the previous ones. This means that there should be many miners to mine the blocks and validate them. After the registration, the gateway creates a new block in the public BC (Ethereum is a good choice), to tell the concerned authorities (healthcare specialists who care of this patient) that there is newly created data (Figure 3). The gateway saves the record in the cloud layer, meanwhile the cloud produces (creates) a block to note that new data is created.

4.3.2 Scenario 2: Gateway/Authority Want to Access Patient's Medical Record

In this scenario, the records containing patient's data have already been stored in the patient's cloud provider. The gateway/authorities that have permission need to access a record that has already been stored. The main work is concentrated in layer 3 when all cloud providers are linked, using public blockchain. The control of access and permission is done by using the cloud contract. The patient has a direct access to the data in the cloud by using its account; it is simply the data owner. When it stores the record, the cloud gives back the ID of this record. Using this ID, the patient can access this record. The cloud creates then a transaction to note that the patient has accessed the record of that ID on this date. The authority sends its ID to the appropriate cloud and waits for the ACK. The ACK in this case is the result of finding that the authority's ID is one of the allowed IDs of the list in the cloud's contract.

4.3.3 Scenario 3: Patient Visits and Interact with an Authority

A new block is added to the layer 2 BC when a patient visits an authority. Consequently, the same block will be added to all authorities and a related block will be added to the cloud's provider blockchain. When the patient finishes its visit, the authority adds a new block to the public BC that includes the ID of the authority, the ID of the patient and some information about the data stored in the off-chain storage of this authority (this data might be medical or

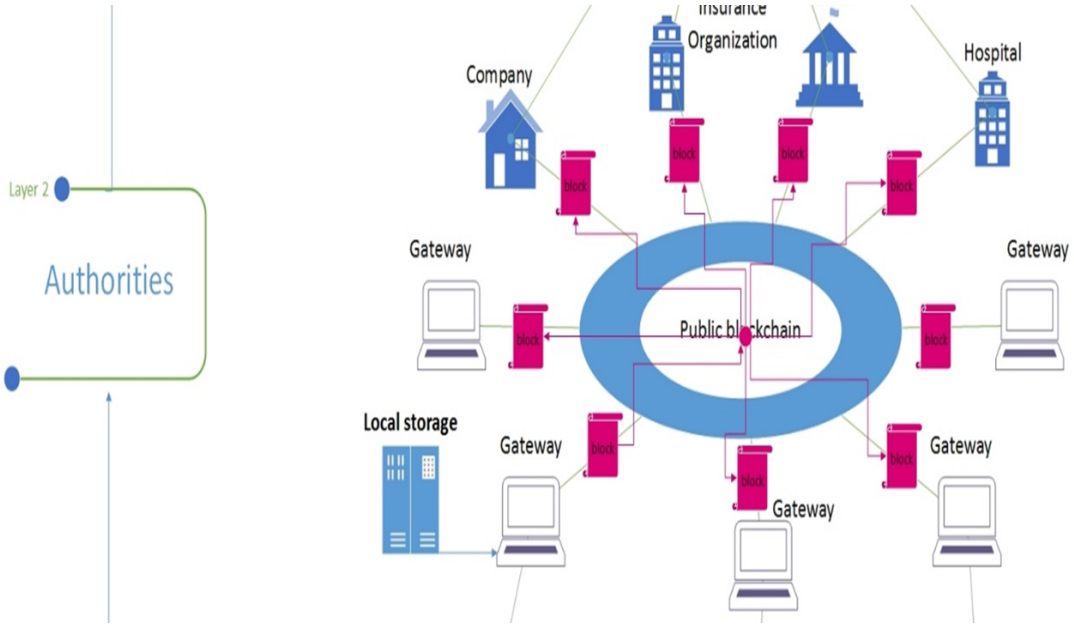

Figure 3: Gateway adds new block to the ledger of BC in layer 2

administrative). The visited authority creates in the cloud's blockchain a block to note that the patient of this ID has visited the appropriate authority. It even notes the place where the data had been stored.

5 Conclusion and Future Works

In this work, we proposed a new distributed blockchain cloud architecture model to meet the design principles required to efficiently manage the raw data streams produced by numerous IoT devices. We were able to verify the possibility of using blockchain technology with IoT and vertical applications, by proposing, implementing and testing a multi-layer structure. The proposed architecture was designed to support high availability, real-time data delivery, high scalability, security, resiliency, and low latency.
To complete this work, multiple performance tests regarding mining time, difficulty variation, and blockchain size should be achieved which will help further enhancements in this domain. Finally, what is important for the future of this technology, and this proposal, in particular, is to implement this architecture in a real system, and continue to evaluate the performances.

Acknowledgments

This research was supported by The Lebanese University and CNRS Lebanon.

References

[1] Ana Reyna, Cristian Martin, Jaime Chen, Enrique Soler and Manuel Díaz,"On blockchain and

its integration with IoT. Challenges and opportunities", *Future Generation Computer Systems*,vol. 88,pp. 173-190, 2018

[2] Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma and Vignesh Kalyanaraman, "BlockChain Technology", *Sutardja Center for Entrepreneurship and Technology*, 2017

[3] Gemalto, "Blockchain Security: 3 Ways to Secure Your Blockchain", 04 December 2018. [Online]. Available: https://blog.gemalto.com/security/2018/12/04/blockchain-security-3-ways-to-secure-your-blockchain/

[4] Preeti Seth, "Smart Contracts: The Blockchain Technology That Will Replace Lawyers", SYSTweak, 13 06 2018.[Online]. Available: https://blogs.systweak.com/an-insight-into-hashing-digital-signature-in-blockchain/

[5] Ameer Rosic, "Smart Contracts: The Blockchain Technology That Will Replace Lawyers", 2016 . [Online]. Available: https://blockgeeks.com/guides/smart-contracts/

[6] Ameer Rosic, "What is Ethereum? [The Most Comprehensive Guide Ever!]", Blockgeeks, 2016 . [Online]. Available: https://blockgeeks.com/guides/ethereum/

[7] Hany F. Atlam, Robert J. Walters and Gary B. Wills, "Fog Computing and the Internet of Things: A Review", *sensors*, 15 January 2019

[8] Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar and Rajani Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT", Big Data Cogn, vol. 10, 2018

[9] Ali Dorri, Raja Jurdak, Salil S. Kanhere and Praveen Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home", vol. 161, March 2017

[10] Ali Dorri, Salil S. Kanhere and Raja Jurdak, "Blockchain in Internet of Things: Challenges and Solutions"

[11] P. K. Sharma, M.-Y. Chen and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT",*Special Section on intelligent systems for the internet of things*, vol. 10.1109, 2017

[12] Shaimaa Badr, Ibrahim Gomaa and Emad Abd-Elrahman, "Multi-tier Blockchain Framework for IoT-EHRs Systems",*ScienceDirect*, vol. 141, p. 159–166, 2018

[13] Nabil Rifi, Nazim Agoulmine, Nada Chendeb Taher and Elie Rachkidi, "Towards using blockchain technology for IoT data access protection", *IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB)*, 2017

[14] Nabil Rifi, Nazim Agoulmine, Nada Chendeb Taher and Elie Rachkidi, "Blockchain Technology: Is It a Good Candidate for Securing IoT Sensitive Medical Data?", *Wireless Communications and Mobile Computing journal*, 2018

[15] Georgios Konstantopoulos, "Understanding Blockchain Fundamentals, Part 2: Proof of Work and Proof of Stake", loom, 8 Dec 2017. [Online]. Available: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb