IOT-BDMS: SECURING IOT DEVICES WITH HYPERLEDGER FABRIC BLOCKCHAIN

Nathalie BANOUN, Nafissatou DIARRA

Department of Research and Innovation, Capgemini, France

ABSTRACT

IoT is a rapidly evolving field with an increasing number of connected devices. This naturally leads to a need to ensure good scalability but also to guarantee the identity of devices, for better security. Most of existing solutions for identifying IoT devices are centralized (CA server), which results in lower fault tolerance and in less scalability. To address these issues, we introduce in this paper a new IoT Device Management System based on the Blockchain technology (IoT-BDMS). Our system offers two services through two Smart Contracts deployed on a multi-channel Hyperledger Fabric network: an Identification Smart Contract (ISC) to manage the devices identities stored over multiple channels, and an Authentication Smart Contract (ASC) to validate authentication requests from devices. An identity is generated by involving the actors of the device's ecosystem and evolves according to the device's lifecycle.

KEYWORDS

Blockchain, IoT Security, Hyperledger Fabric, Smart Contracts, Authentication.

1. INTRODUCTION

The Internet of Things (IoT) can be defined as a network of objects able to interact with each other and with their environment, via the Internet. These objects - which are more and more intelligent - collect data via sensors and processes are performed on this data to create value for their users or owners (decision making, recommendations, etc.).

IoT remains a rapidly evolving field, with predictions of several billion connected objects in the coming years (41 billion connected objects by 2027, and 125 billion by 2030) [21]. This rapid evolution enables new applications and usages to be imagined and explored, in areas such as manufacturing (Supply Chain), Industry 4.0, e-health, etc.

At the same time, the growth of IoT (both in terms of number of connected objects and of amount of data generated) is giving rise to new needs, mainly linked to the efficient management of objects and their security. And as already seen in the last years, security issues of IoT can cause disastrous consequences for humans (Mirai DDoS-attack in 2016 [22]). Along with security challenges, other issues such as scalability or interoperability need to be also tackled. An *Identity Management System* (IdMS) refers to the management of an *identity*, whereas an *identity* is a set of information to uniquely identify a given entity (a human, a device, …). *Authentication* refers to the verification of the identity of a given entity and comes along with Identification. Generally, authentication methods are based on something that you know (like a password), or you own (like a smart card), or you are (like a fingerprint). As with identification [28], there are several authentication methods [27] for IoT devices: symmetric-key based authentication schemes, public-key authentication schemes (PKIs, X509 certificates), token-based authentication schemes (*OAuth2.0*), RFID-based schemes, etc.

David C. Wyld et al. (Eds): CONEDU, NBIoT, MLCL, ISPR - 2021
pp. 41-51, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.110604

Existing IdMS for IoT generally ignore, during the identity generation process, the device lifecycle and the ecosystem in which this device evolves. From the authentication side, the use (for instance) of symmetric cryptography is not adapted to all types of devices (large keys size), and the mobility capacity of devices is often left aside. Finally, whether for identification or authentication, the traditional approaches used in IoT are most often centralized, which leads to a larger attack surface and therefore a lower fault tolerance, but also a low response to scalability needs.

Because of its decentralized, immutable and secure design, Blockchain technology could address some issues of identification and authentication in an IoT context. In fact, several authors [1, 3, 5, 6, 12, 16, 17, 18, 19] have explored the potential of using Blockchain technology to secure IoT devices. This Blockchain-based security generally includes a method for identifying devices, but also a use of the Blockchain to verify the identities of devices, and thus authenticate them.

Our work fits in with this Blockchain-based security for IoT, while addressing some of the issues mentioned above (consideration of the device's lifecycle and ecosystem, scalability). In this paper, we propose a Blockchain-based identification and authentication system for IoT devices, based on a single private Blockchain (Hyperledger Fabric). Our system is comprised of multiple Fabric channels, giving a prior response to IoT scalability needs for Enterprise Use Cases. We designed two Smart Contracts models (an Identification Smart Contract – **ISC** - and an Authentication Smart Contract - **ASC**) and deployed them on a multi-channel Hyperledger Fabric Blockchain. Each Smart Contract pair (ISC, ASC) is responsible of managing and validating devices identities related to its channel. Identities are generated so that they evolve according to devices lifecycle and are stored on specific ledger channels of the global Blockchain network. Devices do not communicate with the Blockchain network, but either send their authentication request through dedicated IoT gateways configured as light nodes.

Our contributions are structured as follows:

1) In **Section 2**, we give an overview of existing works related to Blockchain-based Identification and Authentication for IoT, and highlight some of their limitations.
2) Our contributions are presented in **Section 3**. We list prerequisites of our system and give an overall description of it. We define the components of the system and design its architecture, based on Hyperledger Fabric's channels. Then we describe our identification and authentication schemes. The Section ends with a short analysis of our IoT-BDMS proposal w.r.t to some of the existing methods.
3) We finish in **Section 4** by giving an overview of our implementation on Hyperledger Fabric (with simulated IoT end-devices and gateways) and a Use Case example.

2. RELATED WORK

Traditional digital Identification and Authentication systems can be transposed to the IoT field. But this means addressing at the same time IoT issues, including the need for decentralization for more security, performance and scalability, as well as mobility and interoperability management. And as we mentioned above, the Blockchain, by design, has the potential to remove some of these limitations; indeed, several studies have been carried out to explore the use of the Blockchain to secure the IoT [12], but also to address its scalability requirements.

Regarding scalability, even before discussing that of architectures based on the Blockchain and supporting IdMS and Authentication protocols for IoT, we can already mention the IOTA platform, which defines itself as the (public) Blockchain for the IoT (note that IOTA is actually a DLT - *Distributed Ledger Technology* – based on a structure of DAG - *Directed Acyclic Graph*-

called *Tangle*). IOTA has been specially designed and optimized for the IoT. Hence, it proposes feeless transactions, low-latency micro-payments and claims to guarantee the scalability required in the IoT context (due to the *Tangle* structure used to store transactions). But IOTA actually suffer from many limitations, among which: a kind of "recentralization" via the existence of a *coordinator* in charge of validating transactions (even if work – the *Coordicide* - towards eliminating this *coordinator* seems to be progressing), use of Smart Contract and numerous criticisms around the use of its own cryptographic algorithms. And until now, the scalability highlighted by IOTA seems to remain theoretical.

Unlike IOTA (which is a Blockchain platform designed for the IoT), several works [13] to propose Blockchain-based IdMs and Authentication mechanisms have been carried out; for some of these works, a response (often partial or theoretical) to the IoT issues (such as scalability) is given [2,6,18].

Li et al. [2] designed Blockchain-based identity authentication and data protection mechanisms for IoT devices. In their system, each device is assigned a unique ID which is stored on the Blockchain and allows to authenticate mutually to any other device. However, each device is considered as a node of the Blockchain network, which may not be suitable for devices with low capacities.

In *HIBEChain* [16], authors propose an alternative to traditional IoT identification schemes, using Blockchain technology and based on a decentralized and hierarchical identity-based signature scheme (HIBS - *Hierachical Identity-based Signature Scheme)*. The system uses a collection of private Blockchains to form a hierarchical architecture: each private Blockchain forms a node of the global tree structure and will manage a set of devices. Thus, their hierarchical layered architecture seems to be a real opportunity for scalability issues, by decentralizing and distributing the management of devices identities between several nodes (the management would no longer be done by a single authority). But the solution remains rather theoretical and with a heavy implementation to consider; indeed, the authors do not mention what type of Blockchain could be suitable, what would be the validator nodes, etc. And the solution does not consider the ecosystem in which the device is supposed to evolve.

Authors of [18] propose an identification scheme relying “on three interconnected Blockchains: a (local) private Blockchain for each use case, a shared Blockchain (private) and an overly Blockchain (public). Their solution seems to resolve the identification issue, but it has multiple limitations, like the number of network communications (at least 8) generated by each operation, and the centralization of the local blockchains.

In [14], authors propose to combine a *central* Blockchain (in this case a consortium Blockchain like Hyperledger Fabric) with several *sidechains* (IOTA *sub-Tangles*), in order to make the IoT data management more efficient and secure. Data generated by a device is encrypted before being transmitted to its sub-Tangle coordinator (sub-Tangles coordinators form the nodes of the consortium Blockchain). The system heavily relies on identity control to manage and protect access to IoT data, using Fabric Smart Contracts. A prototype has been set up with software simulations and experimental tests (with performance measures) have also been conducted to motivate the authors' proposal.

From the authentication side, the use of Blockchain has also been widely explored, like in [9, 10, 11, 16, 17, 19].

In [17], author propose *Bubbles-of-Trust*, an Ethereum-based mechanism to mutually authenticate IoT devices and gateways. *Bubbles-of-Trust* was implemented upon the public blockchain

Ethereum, and aims at the creation of secured virtual zones, where devices can communicate securely.

In *Homechain* [19], a Blockchain-based mutual authentication system is proposed for Smart Homes. To provide mutual authentication between users and the home gateway in a Smart Home context, the Blockchain is used together with *group signatures* and MACs (Message Authentication Code); thanks to group signatures, a user is authenticated without disclosing any specific information about him or it's associated gateway,. The system also allows for the efficient tracking of any user who misbehaves in the future. Authors carried out experimental implementations to demonstrate the technical feasibility of their solution (with a few dozen group users). However, these implementations do not consider either the ecosystem of devices or their hardware capabilities. Moreover, *HomeChain*, as its authors point out, has been designed for a specific use case, in this case that of Smart Homes.

To summarize, most of the existing proposals (both for identification and authentication) use architectures either based on public Blockchains [12] such as Ethereum or on hybrid public-private [17] networks, or use Blockchain's hierarchical [16] architectures. But public Blockchains generally come with transaction fees and do not meet all performance requirements for IoT. The use of hybrid architectures often add complexity, with a non-obvious integration and less performances; and the multiplication of communications inside the global Blockchain architecture [18] can also limit the system's performances. On the other hand, as for traditional IdMS, most of the proposals based on the Blockchain technology do not consider the fact that the device's lifecycle can evolve, and therefore its identity as well.

Thus, there is a need to propose a Blockchain-based IdMS and Authentication scheme providing a solution to these limitations.

3. A NEW BLOCKCHAIN-BASED SYSTEM FOR SECURING IOT DEVICES

3.1. Hyperledger Fabric

Hyperledger Fabric (HLF) [4, 6] is part of the Hyperledger suit [7] and is a platform for building consortium/private Blockchain networks. HLF proposes *Smart Contracts* to automate transactions, *channels* for privacy-preserving transactions and allows *membership management* (via Certificate Authorities). HLF ensures good performance metrics (in terms of numbers of transactions per Second for instance) and good scalability.

In our **IoT-DBMS** system, the use of a private/consortium Blockchain such as HLF allows the main actors of the device's ecosystem (manufacturer, administrator, customer or end user, etc.) to be involved in theZ transaction validation process, and therefore in the verification and validation of device identities. Also, HLF Smart Contracts can act as brokers for authentication between devices and their associated gateways.

3.2. Overall Description

Our starting point is a pool of IoT devices spread over several geographical zones. On each of these zones, there is an IoT gateway acting as a bridge between the devices and the IoT Cloud Server. We propose a system based on Blockchain technology to secure the IoT devices of the pool. We use Hyperledger Fabric [7] to build our blockchain network, comprising of multiple channels, each of then representing one of the geographical zones (**Fig. 1**). To take in account the limited capacity of the end devices – and sometimes of the gateways also -, neither the end

devices nor the gateways are considered as nodes of the Blockchain. Instead, gateways can communicate with the Blockchain via API calls, and IoT devices do not communicate in any way with the Blockchain network.

The global workflow comprises two parts: the *Identification Phase* (section **3.4**) and the *Authentication Phase* (section **3.5**).

Through the *Identification Phase*, each new device in the pool will be assigned an identity, stored on the ledger of the appropriate channel. The *Authentication Phase* comes in second, and refers to the validation of a device authentication request before sending data to the IoT server: it is required from the device to send an authentication request at its associated gateway (at least once -after the device first deployment-, and after expiration of the device session).

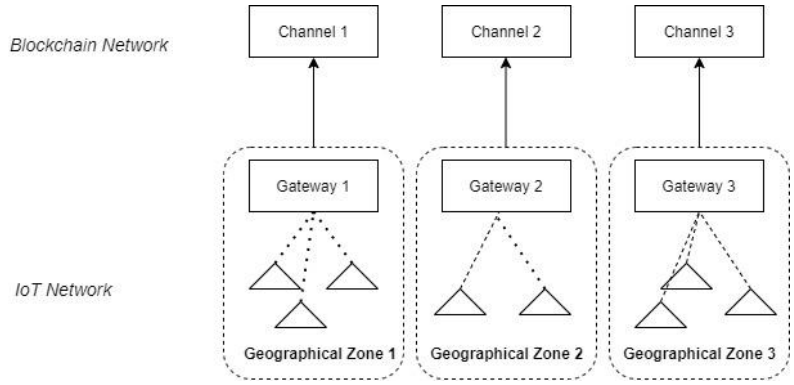

Figure 1. Overview of the System Components:

3.3. Prerequisites

Our system assumes that the following conditions are met:

- **Use of a secure information channel**: To avoid man-in-the-middle attacks (MITM) [23], we assume that devices and gateways exchange data through a secure channel, by communicating for instance over the MQTT (*Message Queuing Telemetry Transport*) protocol [23] secured with TLS(*Transport Layer Security*) [24].
- **Multiple channels on the Blockchain network**: The Fabric network is configured with multiple *channels*, each of them representing a geographical zone containing many IoT devices. And two Smart Contracts (more details in the next section) are deployed on each channel of the Fabric Blockchain.
- **IoT gateways as Blockchain light clients**: The IoT gateways are configured as Blockchain light clients (via a Fabric SDK/REST API), and hence they can communicate with the Blockchain network via the Smart Contracts. Each IoT gateway can only communicate with one channel of the Blockchain network (this can be configured/specified when configuring the gateway as a Blockchain client).
- **Devices keys**: We assume that the manufacturer generates for each device an ECDSA (Elliptic Curve Digital Signature Algorithm) [25] keypair. The private key is then injected into the device (in a kind-of "secured zone"); the corresponding public key is given to the device owner (or to the platform administrator).

3.4. The System Architecture

The system is divided into two parts: the Blockchain network and the IoT network. figure below gives an overview of the (principal) components of our system: the administrator, the Fabric Blockchain network deployed with two Smart Contracts, and the IoT gateways as light clients of the Fabric network.

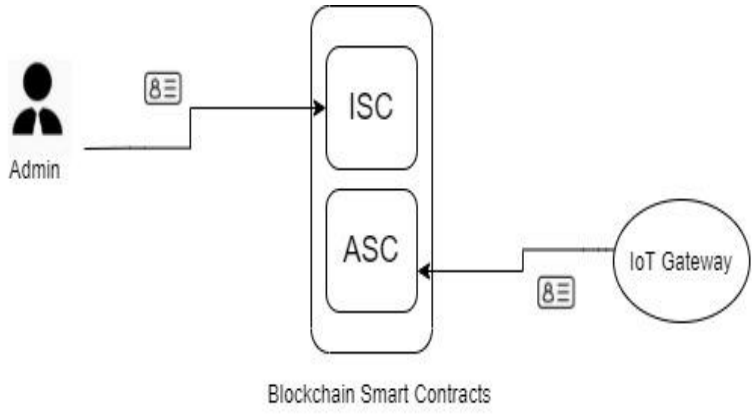

Figure 2. Actors interacting with the Blockchain

a) Two Smart Contracts are deployed on each channel of the Fabric network**:** the **Identification Smart Contract (ISC)** and the **Authentication Smart Contract (ASC).** As their name suggests, the **ISC** is responsible of all transactions related to devices identities (it contains all identity-related functions: registration, update, deletion), and the **ASC** contains functions to authenticate devices (e.g. check existence of devices identities on the Ledger, and verify/validate identities proofs).
b) The **administrator** is responsible of identifying devices. In our system, the identification step refers to assigning to each device an identity and to writing this identity on the appropriate ledger channel on the Fabric network. Administrator is given in advance credentials to access the Identification Smart Contract (ISC), which is in fact responsible of writing on and querying the Ledger.
c) **IoT Gateways** act like intermediaries between end devices and the IoT Server (or Cloud). In our solution, the gateways are also used to check and validate authentication requests coming from their associated devices…. Gateways are configured as light nodes of the Blockchain network (through API clients and calls with the required credentials), an only have access to the Authentication Smart Contract (ASC).

In our system, the Smart Contracts, the administrator and the IoT gateways are the main actors, interacting with the Blockchain network at various levels. But the end devices and the Fabric Blockchain “full” nodes are also part of the system.

```
boolean authenticate_device (device_id_number, challenge, signature) {
        boolean device_authentication_status;
        public_key = ledger[device_id_number].device_public_key;
        if (public_key = null) {
                device_authentication_status = false;
        }
        else {
                device_authentication_status = ECDSAverify (challenge, signature);
        }
        return device_authentication_status;
}
```

Figure 3. Overview of the *authenticate_device* function in the ASC

3.5. The Identification Phase

This phase involves the different actors of the device's ecosystem. Initially, the device is delivered with a kind of secret (an ECDSA private key) injected by the manufacturer. Then the IoT platform administrator will enter certain information related to the device (including data related to its lifecycle, its geographical zone and its deployment context) through a User Interface.

Finally, this information is hashed as follows to construct the device identity:

device_identity = keccak256(serial_number||gateway_id||deployment_date)

where:

* *keccak256* is the SHA3 [26] hash function with a 256 bits-output;
* *serial_number* is the serial number of the device, and *deployment_date* is the date of deployment of the device;
* *gateway_id* is the identifier of the unique gateway in the geographical zone where the device is (or will be) deployed.

The identity will thus vary according to the device's lifecycle (for instance, a change in the *gateway_id* - meaning the deployment of the device in another geographical zone – will result in a complete change of the device's identity). And following needs of the Use Case, other device data (for example the device status: *DEPLOYED*, *MANUFACTURED*, the firmware version, etc.) can be added before the hashing process, to obtain device identity.

After the generation of the identity, the following data structure is stored on the appropriate channel of the Blockchain network, using the Identification Smart Contract (**ISC**):

[device_id_number, device_identity, device_public_key], where:

- *device_id_number* is a unique number identifying the device (generally obtained from (or linked to) the IoT platform)

- *device_public_key* is the device's ECDSA public key. The corresponding private key was previously injected in the device by the manufacturer.

3.6. The Authentication Phase

The next part is to authenticate a device via its associated gateway, and thus to guarantee its authenticity at the IoT platform level. This assumes that the device already had an identity stored at the Blockchain ledger (on the appropriate channel). At this step, the process uses the Authentication Smart Contract (**ASC**).

To show how our Blockchain-based authentication process works, we assume for instance that we have a certain with temperature sensors on it. And the device must periodically send the measures to the IoT Server (Cloud).

Once identified on a channel of the Blockchain (*Identification Phase*), the device will have at first to be authenticated by the appropriate IoT Gateway. The workflow is described as follows:

1) The device generates a MQTT message including its **device_id_number** and sends it to its associated gateway.
2) The gateway generates a challenge and returns it to the device.
3) The device signs the challenge with its ECDSA private key and sends the signature to the gateway.
4) The gateway (as a Fabric light client) calls the ASC on a specific channel, to verify the correctness of the device signature, by giving he **device_id_number** and the device signature.
5) The ASC queries the channel ledger with the **device_id_number** to retrieve the device public key if the device already had an entry on the ledger (else, the authentication process is stopped). The *authenticate_device()* function is called on the ASC to verify the device signature, and the validity status (*true*, *false*) is sent back to the gateway.
6) Following the response received by the gateway, the device will then be considered as authenticated and will send sensors data to the IoT Server, again through the gateway.

- once authenticated, device can then send data to the Cloud, through the IoT gateway.

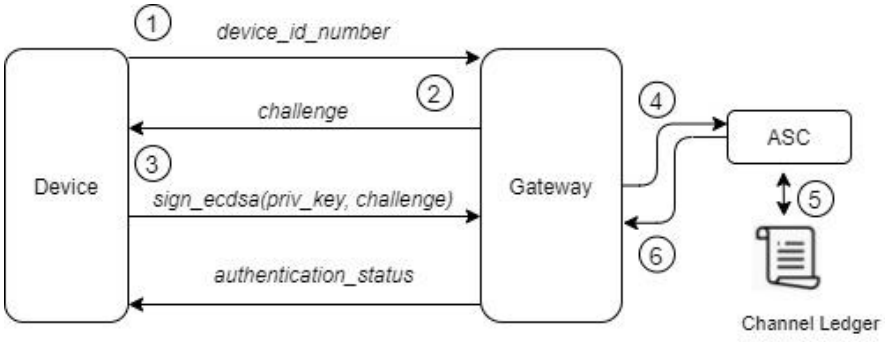

Figure 4. Authentication Workflow

3.7. Short Analysis

Compared to the methods we have analysed in section 3, our IoT-BDMS system has some advantages. First, we do not use a public Blockchain, and we manage to define a potentially scalable architecture using only concepts (in this case *channels*) specific to Hyperledger Fabric.

The fact that we only use HLF allows us to avoid issues related to the integration of several Blockchains (*hybrid* architecture) (like in [16, 18]). To identify and authenticate devices, we use specific Smart Contracts (ISC and ASC); these concepts are not new and have already been used in [1,12]; but unlike [12], and to consider the weak capacities of devices, our identification and authentication features defined in the Smart Contracts do not require the device to participate as a node in the Blockchain network. The identification of the device on the Blockchain is therefore delegated to an administrator for example, and its authentication is done through its gateway which will itself communicate with the ASCs. And this identification takes into account the life cycle of the device, by providing in this identity, from the beginning, information related to this life cycle (such as for instance the geographical area where the device is located at a certain time). To finish, we implemented a proof-of-concept for our system.

4. IMPLEMENTATION AND CASE STUDY

We implemented a prototype (*proof-of-concept)* of our proposal on HLF, with Smart Contracts written in Javascript. and MQTT/Java for the exchanges between the end device and the gateway. Our Fabric Blockchain consortium was made up of 3 channels, each maintained by 2 organisations. Each organisation contains 2 peers, and 1 ordering node. All the Fabric nodes were deployed as Docker containers on a single Linux (Ubuntu 18.04) server hosted on Azure.

On each of the 3 channels, we deployed the ISC and the ASC contracts (**Fig. 5**).

Beside this Blockchain architecture, we also simulated an IoT gateway and an end device, as well as their exchanges (via *WebSockets* and the Mosquitto [15] MQTT broker). On the gateway, we have configured a REST Client to communicate with the ASC (a REST API was developed to expose the services of our Smart contracts). We have tested the end-to-end scenario of the authentication protocol, from the registry of the device identity (done by an administrator through an Angular User Interface) on one channel of the Blockchain, to the authentication request of the device and its validation by the gateway via the Blockchain REST API.

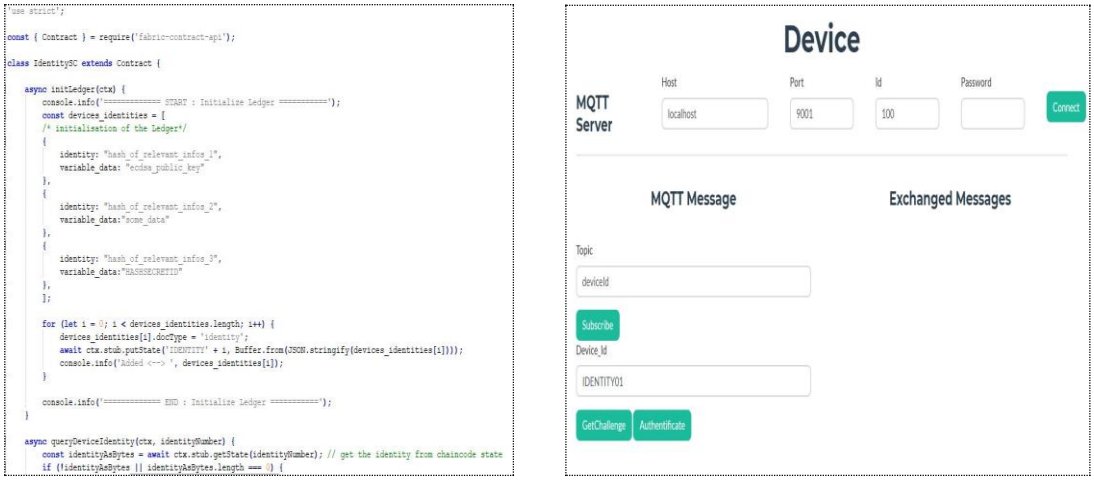

Figure 5. Overview of the ISC (*left*) and the simulated end-device (*right*)

Our system could be deployed for a multi-site manufacturing enterprise, with a dedicated Fabric channel for each site. On each site (e.g. geographical zone), there will be a gateway acting as a broker for the end devices to the authentication functionality on the ASC. This multi-channel architecture could help to handle Blockchain-based authentication for a large amount of IoT devices, at least from a theoretical point of view. In fact, the next step will be to carry out load

testing to identify the maximum number of channels and devices per channel that our architecture is able to support, while continuing to ensure a minimum of performance (*latency* among other indicators).

5. CONCLUSIONS

We proposed an IoT Device Identity Management System (IoT-DBMS) based on Blockchain technology. We distributed the devices identities over multiple Fabric channels hosted on the same Blockchain network and proposed a light Blockchain-based authentication protocol for those devices. We have also implemented our IoT-BDMS by simulating IoT devices and gateways, which provides a sustainable proof-of-concept. As perspectives, we plan to conduct performance tests in order to give some concreteness to the theoretical scalability of our architecture. Integration and deployment in a real IoT environment – thanks to the XIoT [20] platform – are also planned. We also plan to make enhancements so that our Blockchain-based identification and authentication protocols could address the mobility features of some devices, an aspect that has been very - if not completely - unexplored in most existing solutions.

REFERENCES

[1] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, ‘‘Smart contract-based access control for the Internet of Things,’’ IEEE Internet Things J., vol. 6, no. 2, pp. 1594–1605, Apr. 2019.

[2] D. Li, W. Peng, W. Deng and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT". In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018; pp. 1–6.

[3] H. Liu, D. Han and D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT", in IEEE Access, vol. 8, pp. 18207-18218, 2020, doi: 10.1109/ACCESS.2020.2968492.

[4] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, and Y. Manevich,‘‘Hyperledger Fabric: A distributed operating system for permissioned blockchains,’’ in Proc. 13th *EuroSys Conf.*, 2018, p. 30.

[5] M. Banerjee, J. Lee, Q. Chen and K. R. Choo, "Blockchain-Based Security Layer for Identification and Isolation of Malicious Things in IoT: A Conceptual Design", *27th International Conference on Computer Communication and Networks (ICCCN)*, Hangzhou, 2018, pp. 1-6, doi: 10.1109/ICCCN.2018.8487447.

[6] O. Novo, ‘‘Blockchain meets IoT: An architecture for scalable access management in IoT’’, *IEEE Internet of Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[7] “Hyperledger”, at https://www.hyperledger.org/. Last accessed on January 15, 2021.

[8] “ Comprehensive Guide to IoT Statistics You Need to Know in 2020”, at https://www.vxchnge.com/blog/iot-statistics. Last accessed on January 15 2021.

[9] Zhu Xiaoyang, and Youakim Badr. “Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions”, *Sensors (Basel, Switzerland)* vol. 18,12 4215. 1 Dec. 2018, doi:10.3390/s18124215.

[10] Inayat Ali and Sonia Sabir. “Internet of Things Security, Device Authentication and Access Control: A Review”, *(IJCSIS) International Journal of Computer Science and Information Security*, Vol 14, No 8, August 2016.

[11] Achraf Fayad, Badis Hammi and Rida Khatoun. “An adaptive authentication and authorization scheme for IoT's gateways: a blockchain based approach”, *Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, 2018, pp. 1-7, doi: 10.1109/SSIC.2018.8556668.

[12] R. Neisse, J. L. Hernández-Ramos, S. N. Matheu, G. Baldini and A. Skarmeta, "Toward a Blockchain-based Platform to Manage Cybersecurity Certification of IoT devices," *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, GRANADA, Spain, 2019, pp. 1-6, doi: 10.1109/CSCN.2019.8931384.

[13] Shu Yun Lim, Pascal Tankam Fotsing, Abdullah Almasri, Omar Musa, Miss Laiha Mat Kiah, Tan Fong Ang and Reza Ismail. “Blockchain Technology the Identity Management and Authentication

Service Disruptor: A Survey", *International Journal on Advanced Science Engineering Information Technology*, Vol 18, No. 4-2

[14] Yiming Jiang, Chenxu Wang, YaweiWang and Lang Gao. "A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management", *Sensors* 2019, 19, 2042; doi:10.3390/s19092042.

[15] "Mosquitto Broker", at https://mosquitto.org/documentation. Last accessed on January 15, 2021.

[16] Zhiguo Wan, Wei Liu and Hui Cui , "HIBEChain: A Hierarchical Identity-based Blockchain System for Large-Scale IoT", *IACR Preprint*, at https://eprint.iacr.org/2019/1425.pdf. Last accessed on January 1, 2021.

[17] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot and Ahmed Serhrouchni, "Bubbles of Trust: a decentralized Blockchain-based authentication system for IoT". *Computers & Security*. 78. 10.1016/j.cose.2018.06.004.

[18] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. "Blockchain for iot security and privacy: The case study of a smart home", In *Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017 IEEE International Conference on, pages 618–623.

[19] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar and K. R. Choo, "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes", *in IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 818-829, Feb. 2020, doi: 10.1109/JIOT.2019.2944400

[20] "Internet of Things – XIoT Platform". At https://www.capgemini.com/service/digital-services/digital-engineering-and-manufacturing-services/iot-and-connected-products/internet-of-things-xiot-platform/ . Last accessed on January 15, 2021.

[21] "Leaked Mirai Malware Boosts IoT Insecurity Threat Level". At https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/ (October 4, 2016). Last accessed on January 15, 2020.

[22] F. Callegati, W. Cerroni and M. Ramilli, "Man-in-the-Middle Attack to the HTTPS Protocol", in *IEEE Security & Privacy*, vol. 7, no. 1, pp. 78-81, Jan.-Feb. 2009, doi: 10.1109/MSP.2009.12.

[23] "MQTT - The Standard for IoT Messaging". At https://mqtt.org. Last accessed on January 16, 2021.

[24] Tim Dierks and Eric Rescorla. "RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2", *Internet Engineering Task Force (IETF)*, August 2008.

[25] National Institute of Standards and Technology. "Digital Signature Standard (DSS)", FIPS PUB A86-4. At https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf, July 2013.. Last accessed on January 15, 2021.

[26] National Institute of Standards and Technology. "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", FIPS PUB 202. At https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf, August 2015. Last accessed on January 18, 2021.

[27] El-hajj, Mohammed & Fadlallah, Ahmad & Maroun, Chamoun & Serhrouchni, Ahmed. (2019). "A Survey of Internet of Things (IoT) Authentication Schemes". *Sensors* 2019. 10.3390/s19051141.

[28] Cremonezi, Bruno, Borges Alex, Miranda Nacif and José Nogueira, Michele. "Survey on Identity and Access Management for Internet of Things". 2020. 10.21203/rs.3.rs-66793/v1.