Implementing a Blockchain-Based Security System Applied to IoT

Martí Miquel Martínez(✉), Eva Marín-Tordera, Xavi Masip-Bruin, Sergio Sánchez-López, and Jordi García

Advanced Network Architectures Lab (CRAAX), Technical University of Catalunya (UPC), Barcelona, Spain
marti.miquel@upc.edu, {eva,xmasip,sergio,jordig}@ac.upc.edu

Abstract. Several discussions regarding IoT devices and Blockchain came out recently. On one hand, IoT devices have been widely adopted by a notable set of Internet services driven by their capacity to cover several needs (for example, monitoring a manufacturing process, guiding an autonomous car, or tracking a train). On the other hand, Blockchain technology has been considered by several companies to support some critical functionalities, such as security provisioning or data protection. Nowadays, many challenges on both technologies remain yet unsolved, in spite of the unstoppable and ever-growing interest both technologies are attracting. Actually, a substantial push to them both comes from their agnosticism, i.e., many scenarios, particularly those considered as smart, are considered as proper candidates for their deployment, for example smart transportation, smart manufacturing or smart cities, just to name a few. This paper focuses on the latter, proposing a preliminary architecture using both technologies intended to provide security and robustness in Smart Cities. Several Blockchain strategies are analysed in the paper to identify unequivocally every device that belongs to the proposed architecture, also describing the operation of the chosen Blockchain to meet the security requirements. In summary, in this paper, an architecture able to resist certain attacks and proven to be useful to the previous mentioned examples is designed and implemented.

Keywords: IoT · Cybersecurity · Blockchain

1 Introduction

Nowadays ICT systems are able to supervise itself, process information and perform other smart and tedious operations throughout ubiquitous, affordable and small IoT devices. The acronym stands for Internet of Things, encompassing anything connected to the Internet. There are plenty of use cases where IoT becomes relevant, from a simple environment sensing to the deployment of real actions, such as sending messages, issuing warnings, deploying smart decision making process, etc., all to be applied to a large set of domains, including manufacturing processes in the Industry 4.0, autonomous vehicles control, control systems in smart cities, e-health services, etc.

H. Gao et al. (Eds.): BROADNETS 2020, LNICST 355, pp. 143–153, 2021.
https://doi.org/10.1007/978-3-030-68737-3_9

For instance, in an Industry 4.0 context, a factory might deploy several IoT devices responsible for monitoring PLCs (Programmable logic controller) or even for carrying out relevant actions, such as shutting down specific systems or powering them up. Moreover, workers from outside the factory might have the possibility to execute code remotely, thus easing a dynamic management of the whole infrastructure. In a Smart City scenario, data from sensors along the city should be able to be read, having the ability to send commands to actuators deployed in the city remotely and securely. In both scenarios, the information is forwarded throughout the existing telecom infrastructure, leading to security concerns, mainly motivated by the inherent IoT dynamics and heterogeneity.

Needless to say, many threats are expected to pop up in the data transmission process, mainly coming from external attackers but also from internal issues (media transmission issues, errors, etc.), both of them potentially affecting any part of the entire system. Therefore, it is mandatory to secure the whole supply chain.

In these hostile scenarios, a certain level of protection is required in order not to leak or tweak the data from and to unknown actors. In consequence, manufacturers, companies and city managers need, in essence, tools and solutions aimed to prevent these hazardous actions to happen, thus providing security in every step within the pipeline. However, many challenges arise when facing nearly complete security provisioning to every transaction involving whoever and whatever is accessing IoT devices.

Indeed, a long supply chain presents vulnerabilities driven by weak points where attackers might want to sneak in. Identifying such weak points along with the impact the potential vulnerabilities may have on the whole ICT system, is a highly appealing research field, demanding for novel AI-assisted estimation techniques intended to proactively eliminate or mitigate the potential attacks effects.

Two main strategies may be applied when dealing with ICT systems security: i) encrypting data, so nobody different than the recipient and the sender can understand the data, making sure it is not manipulated, and; ii) verifying the peer's identities. In fact, every node should be supervised so system administrators are aware of their status and whether they are being attacked or not. The aftermath of an attack may have highly negative effects, turning into serious monetary (blackmail, downtime, etc.) and even physical damages, when considering an industrial scenario.

The solution proposed in this paper deals with the two strategies highlighted above. Regarding the data encryption, we plan to use the classic TLS (Transport Layer Security) protocol to encrypt and decrypt data. However, to deal with the identity management, although it could also guarantee a vague identification, supported by the SSL Certificate, it only proves that the server is who is supposed to be, but no information about the client identity is provided. Hence, in order to fill this gap, we propose to use Blockchain for identity management, distributing every node's information and making it accessible for every participant.

This paper is structured as follows: Sect. 2 reviews the state of the art related to securing IoT, Sect. 3 presents the proposed architecture, Sect. 4 validate it and Sect. 5 concludes the paper.

2 State of the Art

In this section, we review previous work addressing new approaches for securing IoT. A survey with problems, challenges and proposed solutions for securing IoT can be found in [1]. Aligned to what we stated in the introduction, [1] highlights the fact that existing security technologies are not enough for securing the vast amount of heterogeneous and decentralized devices included in IoT, especially when these traditional approaches are based on centralized architectures. The problems arising in these centralized architectures are usually related to scalability, but also due to the dynamicity and volatility of IoT devices.

In this scenario, different authors have proposed the use of a Blockchain network. In [1] there is a revision of the benefits of using Blockchain in IoT; the main challenges found in the reviewed approaches are, on one hand the need for distributing the security architecture, and specifically the identity management and access control, and on the other hand, take into account the constrained capacity of IoT devices for implementing security features, what turns into the fact that IoT devices cannot store large ledgers. One of the existing approaches is presented in [2], where authors propose a Blockchain network for access control, which is composed by nodes actively working in the transaction process (validating it by mining). However, due to the IoT constraints (CPU and memory), the IoT devices do not belong to this network and then do not store the ledger, but they are clients of the Blockchain nodes. When an IoT device creates a transaction, the transaction is forwarded to the Blockchain network for processing and storing. Although, as in our case, the access control for IoT devices is proposed to be done by means of Blockchain, the article is only a guidance about using Blockchain to make a more secure IoT, and there is neither a deeply description of the architecture nor an implementation.

The work presented in [3] also proposes a decentralized access control architecture for IoT, where the access control information is stored and distributed using Blockchain. Similarly to [1], authors in [3] propose not to store the Blockchain (ledger) in IoT devices, but define a new type of Blockchain node, so-called Management Hub Node, that acts on behalf of IoT devices and that can be connected to several IoT devices, requesting the access to the network for these IoT devices. Additionally, in this paper authors propose the use of a single smart contract. In this smart contract, they are defined all the operations allowed in the access control system; and only a new proposed entity called manager is allowed to access and update the smart contract, for example for defining new access policies.

In a similar approach in order to overcome the difficulty to store and process the Blockchain by IoT devices, in [4] authors propose to cluster devices. A node from each cluster is selected as the cluster head, so-called Overlay Block Managers (OBMs), and will serve as manager of the Blockchain; to ensure scalability, transactions and blocks are broadcast only to the OBMs. In addition, authors also incorporate a number of optimizations specially tuned for IoT devices, such as a distributed time-based consensus algorithm, a distributed trust method, a distributed throughput management strategy and the separation of the transaction traffic from the data flow. Similar to this approach, in this paper we also propose a clear separation of IoT data and transaction data.

The main difference between our proposal and the reviewed proposals [2, 3] and [4] resides on where the Blockchain is physically implemented. Indeed, unlike these reviewed proposals where OBMs or management hubs nodes (responsible for processing and storing the Blockchain) are non-specialized devices executing also other processes or tasks, in our proposal the Blockchain nodes (peers) are implemented at fog devices only executing Blockchain related tasks. This approach is due to the high CPU and storage consumption of Blockchain tasks, including consensus algorithms.

The work presented in [5], despite not being the main objective proposes to secure IoT communication between IoT network and big databases by means of blockchain. The main difference with our proposal is, on one hand the use of the blockchain to store IoT data, and on the other hand the use of two levels of blockchain, one to pre-process and create the block (sidechain) and the blockchain network.

Finally, other approaches may be found in the literature aimed at securing IoT not based on Blockchain. One of these proposals, coming from the H2020 ANASTACIA project [6], presented in [7], focusses on the ability of software-based network mechanisms to protect IoT systems against security threats, providing automated and self-configurable SDN/NFV-based security mechanisms. The proposed security framework not only addresses the security of IoT devices, but also includes other functionalities, such as reconfiguring the system to disallow access to a certain sensor when detecting an attack.

3 Secure Fog to Cloud Architecture Based on Blockchain (SF2C-BC)

3.1 Scenario

Two different scenarios are envisaged, despite having similarities, Industry 4.0 & Smart-cities. In the first one, there exists a hierarchy responsible for segregating tasks and assigning them to each pyramid level. For example, simple actuators (machines) which work directly with the goods, are the lowest pyramid level (Fig. 1) whereas software designed to supervise hundreds of factories remotely represents the highest level. Devices which are part of level 0 only perform their work as ordered by higher levels, hence they are not capable of making decisions based on outside or external events. In the upper layers we find control systems which manage the equipment in lower layers. In this scenario, it could be a good idea to deploy IoT distributed devices in those factories to take measurements (level 0), act according to the control systems in level 1, and finally affect other devices situated at level 0. As mentioned in the Introduction, if these IoT devices are to be controlled remotely, security measures are needed to forward information from IoT devices to the higher layers and vice-versa.

In the second scenario, Smart cities could take different measurements, such as environment, traffic, status of buildings (lift, garbage etc.), and then forward the collected data to control systems managing the city. For instance, afterwards, traffic would be limited in certain time schedules to prevent pollution from rising, also narrowing down city congestion. In the same way, bus stops could show information regarding the on-going bus routes, possible delays, bus occupation and more. Security concerns emerge

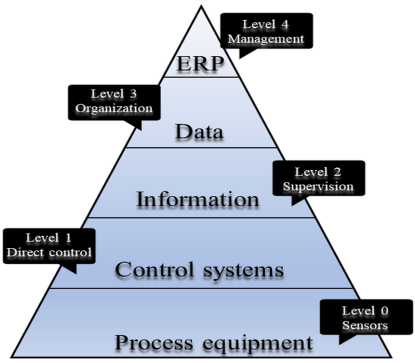

Fig. 1. Automation pyramid

due to the massive information being sent through communication networks, that would represent a Smart city, some of which could be sensitive.

3.2 Secure Fog to Cloud Blockchain (SF2C-BC) Solution

In both scenarios and with current management systems, IoT devices are present but not always reachable from everywhere (at least using traditional Internet connections point-to-point). For example, in previous Fig. 1, management systems at level 4 couldn't direct access to IoT devices at level 0. Therefore, reachability, security & identification are keywords that will be addressed later on in this paper in order to assert system's proper functionality.

Nowadays there exist numerous architecture paradigms that offer connectivity, reliability and more features such as Cloud or Fog-to-cloud (F2C) [8]. Referring to the earlier mentioned architectures, there are two main necessities: nearly immediate response (action-reaction) and persistent data (stored indefinitely). In case an action happens, such as a machine just broke or is malfunctioning, an action must be performed to repair it or even turn it off; it is time critical. What is more, perhaps for the company, knowing the conditions in which the machine was operating could result in useful information not to letting it happen again.

Considering the need of nearly immediate response, cloud is discarded. Therefore, the solution proposed is based on F2C, with devices at different layers including the entire cloud continuum, that is Edge, Fog and Cloud. However, the F2C architecture must be extended to guarantee a secure connectivity between all devices. In our proposal, Secure Fog to Cloud Blockchain (SF2C-BC), we deploy a VPN (Virtual Private Network) to assure the data encryption and propose Blockchain for identity and access control, see Fig. 2.

The tree layers are considered, Cloud (Data centres), Fog (Nodes), and Edge (Devices), so while large computation is carried out in the cloud, other simpler tasks stay between Fog and Edge. However, knowing that third party attackers may keep trying to sniff traffic for illegal purposes, VPN will be used to provide secure communication between the devices in different layers. One of the main reasons for choosing VPN is

to mitigate the inability of maintaining public IPs for every IoT device (needed so they become reachable from everywhere) – specially nowadays where IPv6 is not yet world-wide adopted [9]. Also, VPN provides ACL (Access Control List) in part as a result of PKI (Public Key Infrastructure) infrastructure, letting revoke certificates whenever desired therefore banning future connections.

At this point, we can prohibit clients from accessing; however, there is no any record for IoT devices information. Thus, using a decentralized immutable database like Blockchain will persist nodes known IP addresses, IDs, roles, characteristics etc. The immutability property is crucial for having the awareness that data is untouchable, every transaction will be persisted. Every device's modification or addition of a new one leads into a Blockchain transaction. Blockchain peers will be distributed among the city (or factories) in specialized devices at the Fog layer.

The proposed Blockchain is Hyperledger Fabric, due to its modularity. One advantage is that the main consensus algorithm proposed is byzantine-failure resilient (RBFT), which hugely helps rejecting malicious requests from legit nodes. Only every IoT device info will be saved into the blockchain, whereas data generated by IoT devices situated at the edge will be persistently stored in the cloud, with large storage capacity, thus being perfect for this task.

VPN Centre, a powerful server which could be replicated as shown in Fig. 2 will be placed, for instance in the smart city scenario, in a public facility with a public IP; all devices will be able to reach out to it from anywhere. Its main purpose is to interconnect Fog & Edge devices within themselves. Throughout the VPN, Fog and Edge devices are not only able to communicate between themselves but also with the Blockchain nodes.

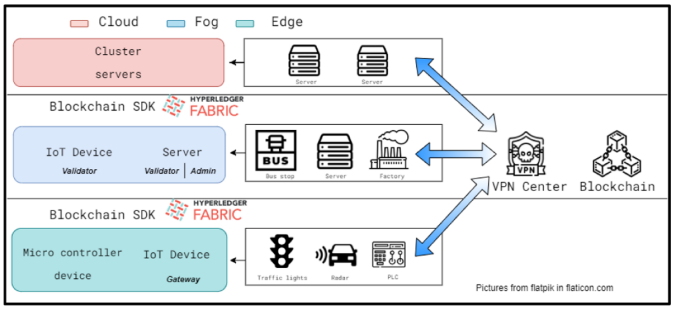

Fig. 2. SF2C-BC

Let's assume that we want to know the weather in a specific area within the city. To do so, IoT devices at the Edge layer which are situated in that area and have weather measurement capabilities will begin to take them. Then, they prepare a JSON-RPC payload with the gathered information, own unique identity and signed digest. At this point, they only prove that in fact they own a pair of public & private keys but anything else. There is a need to verify this payload against Blockchain records, and check whether that node is still able to send requests. Consequently, some devices situated at the Fog layer (validators) will proxy those requests, validate the signing chain and later on act

accordingly (sending data to the cloud & reaching to other EDGE devices if needed to), see Fig. 3.

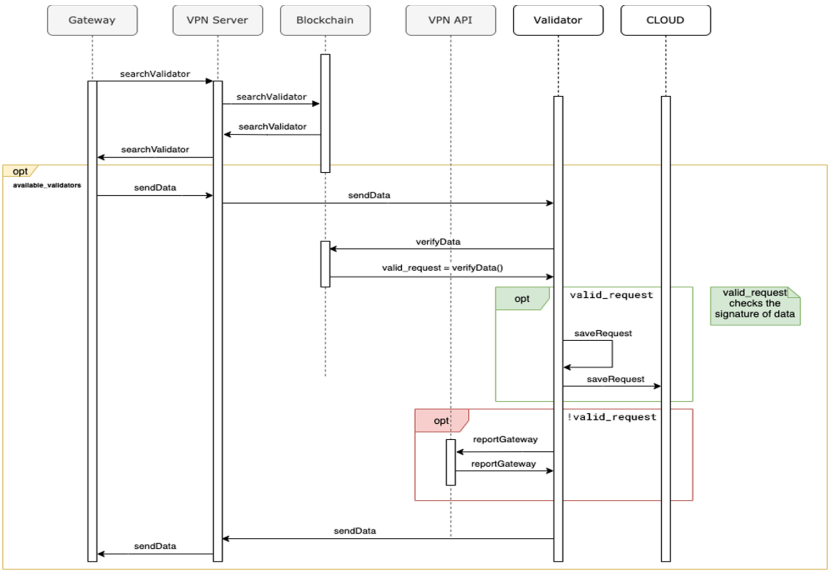

Fig. 3. Message passing

If the checks fail, VPN Centre will have a record of that and obviously there won't be any further actions. The earlier mentioned message passing is depictured in Fig. 3.

Every device in Fog – Edge layer depicted in Fig. 2 through different colours will have either one of these roles:

i) Gateway: IoT device belonging to the Edge which only takes measurements or performs actions.
ii) Validator: Device belonging to Fog which validates gateways petitions by using asymmetric RSA signing.
iii) Administrator: Reserved for future use, able to perform any action to the system.

Cloud will be responsible for persisting data indefinitely for future processing, whereas devices situated at Fog layer will temporarily save them in RAM (Random Access Memory) for nearly immediate access. To summarize, we'll have data replicated because it will be in certain time lapses both in Cloud and Fog, with the advantage of being able to save data and carrying out tasks really quickly.

Nevertheless, every device at Fog and Edge layers will be identified by a unique UUID (Universal Unique Identifier), along with these attributes:

- Node_Type: Validator | Gateway | Administrator
- Virtual_IP: IP static address assigned by the VPN Centre

- Banned: Boolean regarding ban status
- Banned_timestamp: Timestamp from the moment in which the node is banned.
- RSA_Public_Key: Public RSA key in PEM format.

4 Validation

We can safely assume that in order to check the performance of the proposed solution, we'll have to run testing in different conditions for scalability purposes. To this end, we'll need these devices:

1. Sensor & microcontroller (Edge)
2. IoT device with "gateway" role (Edge)
3. IoT device with "validator" role (Validator)
4. VPN Centre in one Fog node
5. Blockchain distributed in two specialised Fog nodes
6. Server intended for Cloud

In the testbed, there'll be a real IoT device, sensor and validator whereas other components will be simulated using virtualization technologies such as Docker and Virtual Machines, see Fig. 4. The first test consists of proving that the architecture works for the simplest use case: report weather in a smart city coming from a sensor. As a proof of concept, one city will be tested along its scalability.

In essence Fig. 4 represents the scenario of two smart cities, with their own servers to interconnect Fog and Edge devices. Although only one of the scenarios is represented, the main idea can be extended for the Industry 4.0 scenario, where instead of two smart cities we can assume two factories; installed sensors in machinery monitor their operation. As a proof of concept, one city will be tested along with its scalability.

The blockchain is placed near the VPN Centre, distributed into two peers, allowing the interaction through Fabric SDK's smart-contracts. They intend to do it by running what they call chain-code (available in different programming languages); every device that has to either read or write new transactions to the blockchain, will have to invoke RPC (Remote Procedure Call) methods. Also, they'll sign the petitions with their private RSA key, leading to non-repudiation of origin.

Figure 5 depicts the internal structure of testbed's Fabric; end-users such as IoT devices belong to the red area, blue area are peer nodes and finally in grey the CA servers which issue credentials using PKI (Public Key Infrastructure).

4.1 Tests

We carry out two tests: one to check the basic functionality of the system and the second for testing the scalability:

- Basic functionality including: 1 sensor, 1 gateway, 1 validator, 1 VPN Centre, 1 Cloud and 2 Blockchain peers:

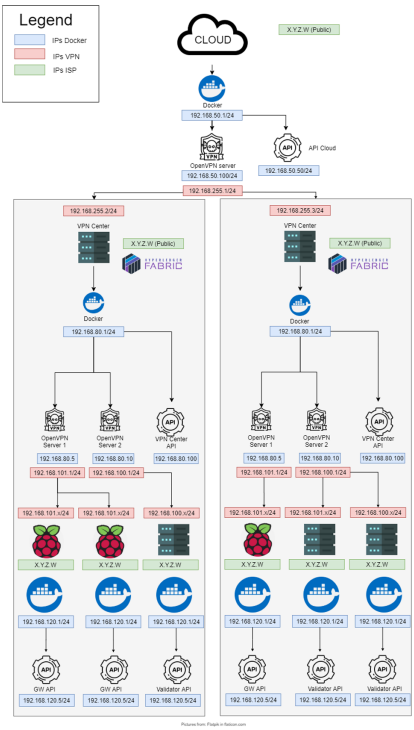

Fig. 4. Two smart-cities architecture

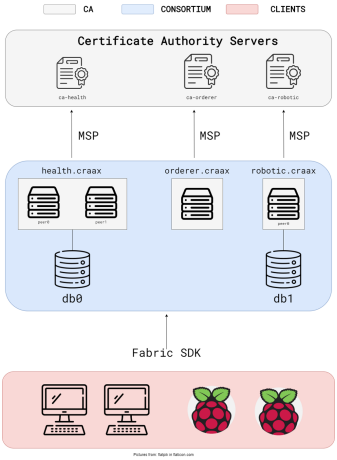

Fig. 5. Internal Blockchain architecture

- **Input**: Sensor sends a valid JSON RPC payload (weather measurements) with a valid signed digest.
- **Expected output**: Transaction success, cloud has a copy of this data stored.
- **Transaction success** means that the validator is able to verify the signature of the payload's digest correctly, and the requester is not banned in the Blockchain, some of the transactions are shown in Fig. 6.
- Scalability test including the following devices with the same input, expected output and transaction success, see Table 1.

Table 1. Amount of used devices

Device	Quantity	Device	Quantity
Real sensor	1	Simulated Gateway	19
Simulated sensor	19	Simulated Validator	20
Real Gateway	1	VPN Centre	1
Blockchain peer	2	Cloud	1

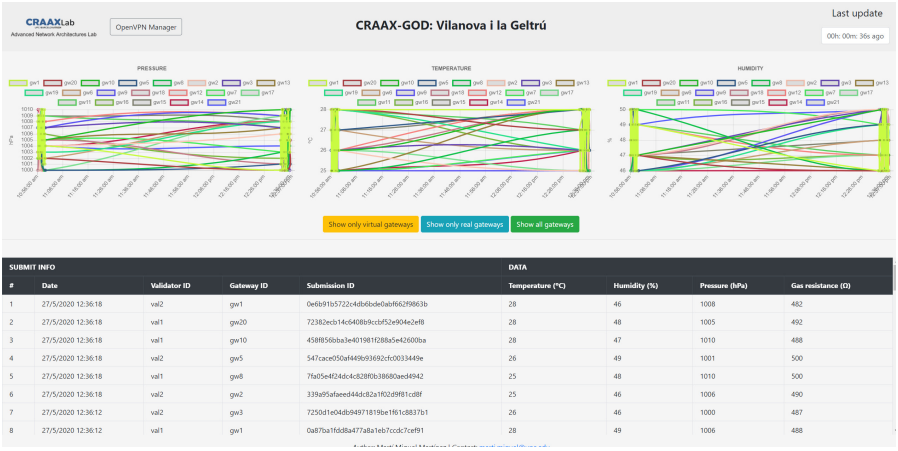

Fig. 6. Dashboard representing various successful requests

4.2 ACL Verifications

In this section, we will test that ACLs are correctly applied by two type of verifications:

- RSA verification

Firstly, the chosen validator extracts the signed digest from the JSON-RPC payload in every request, taking the unique ID given by the request and obtains the corresponding public RSA key from the Blockchain. Afterwards, it verifies that in fact that message was signed by whomever that had a private key from which the public key derived from. If the result is incorrect, notify VPN Centre and reply with a negative response to the gateway, considering the petition non-legit. Figure 7 shows the warnings due to non-legit petitions.

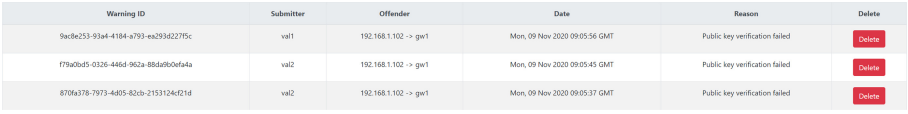

Fig. 7. Petitions from non-verified devices

- Blockchain banned device

Firstly, extract the signed digest from the JSON-RPC payload in every request. Take the unique ID given by the request and check with the Blockchain whether the device is banned. If it is, notify the VPN Centre and reply with a negative response to the gateway, considering the petition non-legit, see Fig. 8.

Fig. 8. Petitions from banned devices

5 Conclusions

In this paper, we have ensured that despite having security concerns in any of the two envisaged ICT scenarios (industry 4.0 and smart cities), an architecture capable of withholding impersonations (attacks) has been designed, nevertheless only the smart city scenario has been implemented and validated. What is more, we've tested numerous devices in the Fog & Edge layers to simulate a more real scenario, sending requests at a high rate in a random fashion, and validating the results in terms of ACL verifications and delay. It has been verified that Blockchain can help in these cases as long as information doesn't require to be updated frequently; obtaining information from each IoT device within the Blockchain is not a transaction, rather a read operation. Only modifications and additions are considered transactions leading to propagated updates.

Acknowledgements. This work was partially supported by the Spanish Ministry of Economy and Competitiveness, under contract RTI2018-094532-B-I00 (MINECO/FEDER) and the Spanish Thematic Network under contract RED2018-102585-T.

References

1. Hassija, V., Chamola, V., Saxena, V., et al.: A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access **7**, 82721–82743 (2019)
2. Singh, M., Singh, A., Kim, S.: Blockchain: a game changer for securing IoT data. In: IEEE World Forum Internet Things, WF-IoT 2018 - Proceedings 2018-January, pp. 51–55 (2018)
3. Novo, O.: Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. **5**, 1184–1195 (2018)
4. Dorri, A., Kanhere, S., Jurdak, R., Gauravaram, P.: LSB: a lightweight scalable blockchain for IoT security and anonymity. J. Parallel Distrib. Comput. **134**, 180–197 (2019)
5. Casado-Vara, R., Chamoso, P., De la Prieta, F., Prieto, J.: Non-linear adaptive closed loop control system for improved efficiency in IoT-blockchain management. Information Fusion **49**, 227–239 (2019)
6. ANASTACIA Project. https://www.anastacia-h2020.eu/
7. Molina Zarca, A., Bernal Bernabe, J., Farris, I., et al.: Enhancing IoT security through network softwarization and virtual security appliances. Int. J. Netw. Manag. **28**, 1–8 (2018)
8. Masip-Bruin, X., Marín-Tordera, E., Tashakor, G., Jukan, A., Ren, G.: Foggy clouds and cloudy fogs: a real need for coordinated management of fog-to-cloud computing systems. IEEE Wireless Commun. **2**, 9–20 (2012)
9. IPv6 – Google. https://www.google.com/intl/en/ipv6/statistics.html