Blockchain-based Identity and Access Management in Industrial IoT Systems

Valentin VALLOIS
Universite de Paris
CNRS Borelli Research Center, INSERM, ENS
Beamap, Sopra Steria Group
Paris, France
vvallois@beamap.fr
valentin.vallois@etu.u-paris.fr

Ahmed MEHAOUA
Universite de Paris
CNRS Borelli Research Center, INSERM, ENS
Paris, France
ahmed.mehaoua@u-paris.fr

Mourad AMZIANI
phd, Beamap
Sopra Steria Group
Paris, France
mamziani@beamap.fr

***Abstract*—It's been ten years since blockchain technology was created. This amalgam of cryptography and peer to peer application brings many innovations and securities services beyond financial services to regular information systems and offers new use cases for distributed applications. Industrials Internet of Things systems have issues with delivering identities to devices, controlling access or managing a vast amount of data. In this paper, we will go through the benefits a blockchain infrastructure can bring to the industrial Internet of Things (IoT) systems and present a new approach for a distributed Identity and Access Management (IAM) using blockchain technology as the communication layer. The proposed work in progress architecture is suited for consortium of companies sharing a fleet of IoT devices. The blockchain ensures the integrity and the non repudiability of instruction at destination to the IAM controllers.**

***Index Terms*—Industrial IoT, IAM, Blockchain**

I. Introduction

There are 3 major innovations in the last decade, Artificial Intelligence (machine learning, deep learning...), big data (data clustering, data analytics...) and distributed systems (IoT, blockchain, micro-services...). Internet of Things (IoT) systems are at the convergence of at least two of them, big data and distributed systems while machine learning can also be a part of IoT, but its use cases are marginal or underexploited. IoT systems are complexes, they use a mix of legacy and new technology and keeping a coherent level of security is a real hassle, the majority of IoT devices are considered not secure [1]. Managing such systems is a feat on its own and are the result of years and years of careful upgrades transforming them into frankenstein monster of information systems. Especially critical industrial systems such as power grids, water delivery or dangerous environment factories have specific needs [2]. These infrastructures need to be resilients, the communication between components without interruptions and the monitoring of all the devices and components. Those are the major challenges for industrial IoT systems.
In this paper we will focus on one aspects of managing the IoT system, the Identity and Access Management (IAM). The growth of Internet of Things is inevitable, estimated around 5,8 billion devices in 2020 [3], IoT devices will reach the same problem as IP addresses as we need to identify each device individually. Distributed and complex infrastructure make it difficult for IAM to be effective but [4] state that centralised IAM systems are too expensive for large networks. As industrial ecosystem opened up with the emergence of platform enterprises. Initiative like the protocol ActivityPub for social networks prove that implementation of distributed IAM systems is a reachable goal and is suitable for individual [5]. A solution for managing devices identity in multiple contexts or information system is a challenge IoT had to overcome. For example, in a production chain with multiple enterprises, like Airbus with its planes, the information systems of each companies is different and there is no homogenisation of information between them. Blockchain technology solves this problem by associating an identity with a machine to track production and ensuring that its identity exists in each IAM system where all parties can verify the data.
The organization of the remaining paper is as follows. In section 2 we will present an overview of IAM and Blockchain technologies. In section 3 we will explore different approaches from the academics for blockchain based distributed systems. Then in section 4, we propose a work in progress blockchain implementation for a distributed IAM system.

II. IAM and Blockchain

A. Identity and Access Management

Identity and Access Management is the association of identity management and access control, accomplishing two main goals. The attribution and orchestration of digital identity to users (admin, operator, developper...), device (sensor, RFID chips, heavy machinery...), service (web service, application, database...) or resource (data, computing power...) and authentication and authorization of these identities. One of the leading challenges for Industrial Internet of Things (IIoT) is the management of the ever growing number of IoT devices. IAM needs to function "at scale" and in an open ecosystem.

978-3-903176-32-4

IAM is a necessity for securing machine to machine communication. IIoT devices need to be uniquely identifiable to establish trust and prevent spoofing and data corruption. One of the components of IAM is the permissions configuration, each actor must have a set of actions depending on their identities. There are several methods to define an access control, it can be RBAC (Role Based Access Control) or ABAC (Attribute Based Access Control) [6], [7]. A role is a set of actions based on tasks, a network administrator gains access to network resources but can't access developpement resources. The roles are predefined and each identity is assigned to them. In Attribute based access control, the permissions are defined by attribute of an identity which can be the location, features, credentials... For example, a sensor in factory A will have different permissions than the same type of sensor in factory B.

As IoT devices have a short lifespan the IAM lifecycle need to be executed more frequently (Provisioning, Authentication, Authorization, Permissions, Self service, De-provisioning) The provisioning is particularly important in IIoT scenario, assigning a unique identity to each devices require them to have unique feature to differentiate them. Yijian Li [7] presents initiatives to standardize a naming convention for IoT devices.

B. Blockchain

Blockchains are, in simple terms, a distributed database. The data is stored inside a block, each block refers to a previously published block through cryptographic hash of its content. Thus creating an oriented graph also called a chain. A block is composed of multiple transactions which are a data structure containing at least a time stamping and a cryptographic signature from the uploader. Information is replicated in all the nodes of the blockchain using peer to peer protocol. Blockchain offers many security services [8]. In the following section we will present the major benefits and constraints of a blockchain system and their impact on an industrial IoT system.

First and foremost, blockchain was created to solve the double spending problem in a distributed environment. Information, data or a digital resource can't be duplicated or replicated. For example in an exploitation system, mutual exclusion (mutex) synchronisation mechanism that prevents double utilisation of a ressource. In the Bitcoin blockchain the resource is the currency, each amount of currency is holded by an entity and nobody can claim the ownership of someone else's bitcoins and when someone transfers some of their bitcoin they lose the ownership of that amount of bitcoin.

Data integrity is the second major benefit of a blockchain system. An effective timestamping mechanism is by design to ensure a proper sequencing of the block. The robustness of the data integrity is secured by the consensus algorithm chosen by the implementers of the blockchain. The strength of the consensus is based on an opposed competition in which the actors put investment at stake, whether it is proof of work or proof of stake in a public. In a private blockchain the trust is based on contractual agreement.

By being distributed without a trusted third-party, the blockchain guarantees the availability of its content and offers censorship-proof capabilities. Interacting with the blockchain only needs a network connection to one of its nodes, this node can be hosted inside a private network or accessed through the internet. In a public blockchain environnement, to completely censor an actor the majority of the participants need to block its participation to the blockchain by not relaying its transactions or blocks making him incapable of interacting with the blockchain. Attacks have been theorised and some implemented [9]–[11], but countermeasures are quickly deployed into the blockchain softwares. In most cases, the attacked participant can reroute it's transaction to a node that will accept its data. Blockchains are particularly suited for adversary environments where actors don't trust each other. This untrust environment actually guarantees the data integrity, if one of the nodes modify the blockchain every other node will instantly notice it and reject the modification if they aren't compliant with the consensus rules.

Blockchain has major drawbacks that hinder its adoption by businesses and industrials, such as data processing latency, security depending on the number of nodes, and the "append only" approach to data storage. Blockchain use cases have to consider these drawbacks and look forward to future evolution. As research progresses in this field, some of these issues will be resolved, notably concerning latency in private blockchains [12], [13].

Blockchains process data slowly, even the fastest one are slower than traditional centralised systems [14] because the speed of data processing is correlated to security. A public blockchain needs to be slow, the information needs to propagate through the distributed network to synchronize between the nodes. Proof of work consensus strongly secures the chain of blocks. Due to the security constraint, storing data on chain can't be used for real time use cases. The data is considered to be saved and validated on the blockchain as soon as a sufficient number of blocks are created after their insertion. In the possibility of 2 concurrent blocks (fork) being created at the same time, the information stored in them is in a state of non confirmation as the system needs to elect the correct branch. This phenomenon is called a reorganization, although it is a natural event part of the public blockchain, it nevertheless changes the state of the blockchain. A transaction that is only present in the losing branch must be reintegrated in a future block. In the bitcoin blockchain, a transaction is considered confirmed if there are 6 blocks created after the transaction is inserted in the blockchain, with an average creation time of 10 minutes per block, this means that a data is considered to be safely added in the bitcoin blockchain after 60 minutes [15].

A blockchain isn't a traditional CRUD (Create, Read, Update, and Delete) database. Information is only appended and deletion isn't possible as it will go against the consensus mechanism. The size of the blockchain increases continuously as it is used. IoT devices collect a significant amount of data, and only adding these to the blockchain will saturate the storage of the nodes. There is a more efficient way to use the

blockchain by using off-chain functionality, such as a database where data is time stamped using a merkle tree or any other data structure then stored in the blockchain, saving storage space. For example, backing up only the root of the merkle tree will ensure the integrity of all associated data.
In conclusion, blockchains are suitable for virtually exchanging ressource, for timestamping information and for distributed databases. Their security differs between blockchain implementation, private blockchain are easier to set up , manage and run but the same level of integrity than a standard database and the same level of availability than a standard distributed database. They are more centralised than public databases but have shorter latency. Meanwhile a public blockchains have their own constraints, they have an operational expense as any transaction uploaded in the blockchain needs to pay a small fee in the associated cryptocurrency but they are more decentralised as more actors/nodes are keeping the blockchain and watching its integrity. Private blockchains have better throughput and better latency but are more centralised. Public blockchains are more secure and more decentralised but are slower and expensive.
Designing use cases for IoT systems using blockchain needs to take into consideration these benefits and constraints. Blockchain isn't the solution to every problem and most of the time it's less effective than standard centralised software.

III. Related Works

We see a growing interest in the application of blockchain technology in convergence with IoT systems, especially at the dawn of the Industrial Revolution 4.0. [16], [17]. In this section, we review related publications on the application of blockchain for replacing distributed functions focusing on IAM solutions [18]. Wang et al [19] present an IAM implementation on the Ethereum blockchain where the functions are done through a smart contract. The smart contract manages the identity and the access control directly on chain without intermediary. The access control mechanism used in this contribution is Attribute Based Access Control (ABAC). Iot devices or gateways host a light peer that manages the communication between the system and the blockchain. An implementation of a distributed Software Define Network (SDN) for IoT is presented by Yazdinejad et al [20]. The authors combine public and private blockchain (Ethereum) in a cluster architecture to configure the routing between multiple IoT sub networks. The public blockchain contains the registry of all the SDN domains and is stored in each cluster head. The role of a cluster head or SDN controller is to be responsible for the activation of the IoT devices. The private blockchain is placed between the IoT device and the SDN controller of a sub network and is used as an authentication and access control. Blockchains securely deliver messages to the SDN controller and users. Zhang et al [21] propose an implementation of multiple smart contracts providing an on chain access control to any other smart contract. First, the contract judge evaluates the behaviour of the entity that connects to the system and applies a sanction if the behaviour is malicious. The second, the Register Contract records information on access control and accessible smart contracts. This implementation makes it possible to secure the monitoring of access management directly on the blockchain.

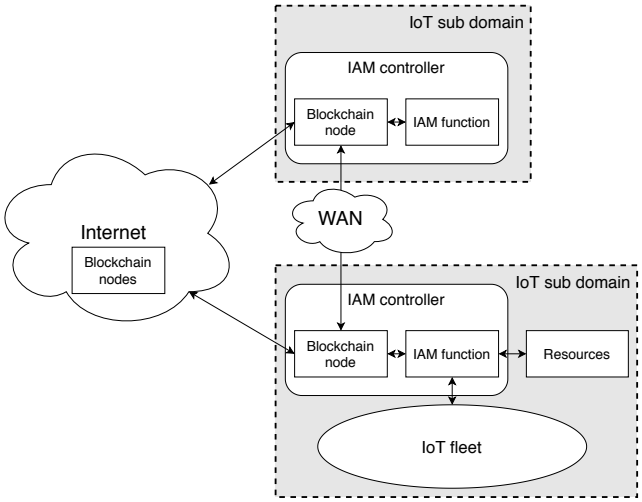

Fig. 1. High level design of the component

IV. Distributed Identity and Access Management

Modern Industrial Internet of Things infrastructures are deployed on multiple locations inside different networks. The IoT devices need to reach databases or services securely. In the era of the industry 4.0, a smart factory will be in interaction with diverse actors creating a complex ecosystem where interoperability is a key factor. A distributed IAM framework will solve the problems of consistency between multiple information systems. The blockchain solves the problem of interoperability between system and components [18] and keeps a log of all the operations.

A. Design

The proposed architecture solves the problem of identity federation between several companies. Each organization retains control over its perimeter and is able to consult the authorizations of an IoT device. The blockchain serves as a means of communication between entities and guarantees the integrity of operations. Each company is identified by a public/private key pair used for the digital signatures required for the blockchain. A company registers an identity by sending a transaction on the blockchain containing a Unique Identifier and the permissions associated with it. The transaction is signed by the issuing company. If an update or revocation is required a new transaction must be issued referencing the previous transaction in the manner of public blockchains. The permissions and access rights depend on the computer systems of each company. The heterogeneity of these systems imposes a customization effort by companies to convert the content of a transaction to their internal information systems. For example, translating the transaction into an API request for the internal IAM software.

Thus all the actors share a device directory which allows devices to move and continue to be identified in each information system. Let's imagine a delivery drone arrives in a factory belonging to company A, its credentials indicate that the drone comes from company B. A and B each have a blockchain node in their information systems, and this allows A to verify the presence of the drone's identity in the blockchain. In our approach, we decided to choose the Hyperledger Fabric private blockchain because it offers more control, smart contract capabilities and better governance for the blockchain members, which are important criteria for industrial IoT scenarios. Hyperledger Fabric uses a voting system to validate a block 2/3 of the voting nodes need to approve the block. This consensus is particularly suited for a private blockchain built with multiple businesses.

In our system, the blockchain acts as the message bus (inspired from [19]) for the IAM infrasctruture and as a log for IAM instructions. The blockchain ensures the traceability of all the IAM functions and guarantees data synchronicity for each IAM controller as the final state of the identity ledger can be recreated by reading the blockchain. Hyperledger uses a traditional key-value database to store the state of the blockchain. This database access allows external applications to consult the data faster than by going through all the blocks. Each Business host an IAM controller (Blockchain node + IAM software), each one has a unique identity. A transaction is either addressed to every controller to set a global configuration or a specified number of controllers, allowing to restrict the actions of an device to specific sub domains.

In our proposition, there are 5 actions, based on [18]: Provisioning (Creation of an identity), Update (Modification of an identity), Revocation (Deletion of an identity), Lookup (Verification of the presence of an identity), Evaluate (Authentication of an identity). Action orders are issued through the blockchain and are executed by the IAM controller. Each of these actions are traceable on the blockchain, where the identity of the issuer is stored.

B. Scenarios

In this section, we will present how various scenarios unfold, underpinning the interaction between the components of the proposed blockchain based IAM framework.

1) Provisioning a new identity: Company A create a new identity for a tracking device by sending a new transaction on the blockchain. The device will input in the information system of other companies, in the transaction it will be specified as destination all the domains that the device must be authenticated, the domains of the company A and so on. The transaction will spread in the blockchain and all the actors will receive a copy of it, the recipient companies will register the identity in their information system.

2) Device request access to a resource: A device must access certain data within a database. Information systems will check within their IAM systems for both identity and authorization, if the identity does not exist in their IAM systems, the blockchain must be consulted. The company will browse the blockchain to obtain all transactions related to the identity of the device. Since the permission can be updated, only the latest transaction permissions will be used.

V. Conclusion

In the current state of our work we didn't address the confidentiality inside a transaction, we plan to explore this subject in future works. For example, a message may be encrypted before being added to the blockchain and only a participant in the information system will decrypt it. Encryption isn't a trivial implementation and takes into consideration multiple parameters such as the keys exchange, symmetric or asymmetric encryption, key storage, etc. The IAM function could be done directly inside a smart contract but not all the blockchains have the capabilities to execute complex smart contracts, we choose to propose an agnostic solution. A blockchain like Bitcoin has strict rules for its native smart contract, only a limited set of functions are available while the Ethereum or Hyperledger blockchains offer Turing complete programming language. Using smart contracts can increase the security of the system, by ensuring the execution of the IAM function will be directly saved on the blockchain and reducing the number of components needed for an IAM framework. We presented an implementation of blockchain for a distributed IAM system and the benefits and drawbacks of such technology. A blockchain is a useful tool in scenarios with multiple shareholders that need to keep accountable to each other. It's a complex answer to specific needs. Our solution uses the blockchain as a message bus to transmit IAM instructions securely across multiple environments.

References

[1] M. Ahmad, T. Younis, M. A. Habib, R. Ashraf, and S. H. Ahmed, "A Review of Current Security Issues in Internet of Things," in Recent Trends and Advances in Wireless and IoT-enabled Networks, M. A. Jan, F. Khan, and M. Alam, Eds. Cham: Springer International Publishing, 2019, pp. 11–23.

[2] A. Ghasempour, "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges," Inventions, vol. 4, no. 1, p. 22, 2019.

[3] Gartner, "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020," Gartner, 29-Aug-2019. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io. [Accessed: 28-Oct-2019].

[4] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," Computer Networks, vol. 112, pp. 237–262, 2017.

[5] S. Göndör and A. Küpper, "The Current State of Interoperability in Decentralized Online Social Networking Services," in 2017 International Conference on Computational Science and Computational Intelligence (CSCI), 2017, pp. 852–857.

[6] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," Computer, vol. 48, no. 2, pp. 85–88, 2015.

[7] V. Franqueira and R. Wieringa, "Role-based access control in retrospect," Computer, vol. 45, no. 6, pp. 81–88, 2012.

[8] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," IEEE Communications Surveys Tutorials, pp. 1–1, 2018, doi: 10.1109/COMST.2018.2863956.

[9] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse Attacks on Bitcoin's Peer-to-peer Network," in Proceedings of the 24th USENIX Conference on Security Symposium, Berkeley, CA, USA, 2015, pp. 129–144.

[10] K. Wüst and A. Gervais, "Ethereum Eclipse Attacks," ETH Zurich, 2016.
[11] P. L. and J. S. Unit Dell SecureWorks Counter Threat, "BGP Hijacking for Cryptocurrency Profit." [Online]. Available: https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit. [Accessed: 25-Apr-2017].
[12] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability," in 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 536–540.
[13] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017, pp. 1–6.
[14] R. Yasaweerasinghelage, M. Staples, and I. Weber, "Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation," in Software Architecture (ICSA), 2017 IEEE International Conference on, 2017, pp. 253–256.
[15] A. M. Antonopoulos, Mastering Bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc., 2014.
[16] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, "Blockchain Applications for Industry 4.0 and Industrial IoT: A Review," IEEE Access, pp. 1–1, 2019, doi: 10.1109/ACCESS.2019.2956748.
[17] M. Kamran, H. U. Khan, W. Nisar, M. Farooq, and S.-U. Rehman, "Blockchain and Internet of Things: A bibliometric study," Computers & Electrical Engineering, vol. 81, p. 106525, Jan. 2020, doi: 10.1016/j.compeleceng.2019.106525.
[18] M. Nuss, A. Puchta, and M. Kunz, "Towards Blockchain-Based Identity and Access Management for Internet of Things in Enterprises," in Trust, Privacy and Security in Digital Business, vol. 11033, S. Furnell, H. Mouratidis, and G. Pernul, Eds. Cham: Springer International Publishing, 2018, pp. 167–181.
[19] P. Wang, Y. Yue, W. Sun, and J. Liu, "An Attribute-Based Distributed Access Control for Blockchain-enabled IoT," in 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2019, pp. 1–6, doi: 10.1109/WiMOB.2019.8923232.
[20] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An Energy-efficient SDN Controller Architecture for IoT Networks with Blockchain-based Security," IEEE Transactions on Services Computing, pp. 1–1, 2020, doi: 10.1109/TSC.2020.2966970.
[21] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," arXiv:1802.04410 [cs], Feb. 2018.