future internet

MDPI

Article

A Lightweight Blockchain-Based IoT Identity Management Approach

Mohammed Amine Bouras [1,*], Qinghua Lu [2], Sahraoui Dhelim [1] and Huansheng Ning [1]

[1] The School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China; sahraoui.dhelim@hotmail.com (S.D); ninghuansheng@ustb.edu.cn (H.N.)
[2] Data61, The Commonwealth Scientific and Industrial Research Organisation (CSIRO), Canberra 2601, Australia; qinghua.Lu@data61.csiro.au
* Correspondence: bouras.ma@xs.ustb.edu.cn

Abstract: Identity management is a fundamental feature of Internet of Things (IoT) ecosystem, particularly for IoT data access control. However, most of the actual works adopt centralized approaches, which could lead to a single point of failure and privacy issues that are tied to the use of a trusted third parties. A consortium blockchain is an emerging technology that provides a neutral and trustable computation and storage platform that is suitable for building identity management solutions for IoT. This paper proposes a lightweight architecture and the associated protocols for consortium blockchain-based identity management to address privacy, security, and scalability issues in a centralized system for IoT. Besides, we implement a proof-of-concept prototype and evaluate our approach. We evaluate our work by measuring the latency and throughput of the transactions while using different query actions and payload sizes, and we compared it to other similar works. The results show that the approach is suitable for business adoption.

Keywords: identity management; blockchain; internet of things; distributed ledger technology; sensor; access control

Citation: Bouras, M.A.; Lu, Q.; Dhelim, S.; Ning, H. A Lightweight Blockchain-Based IoT Identity Management Approach. *Future Internet* **2021**, *13*, 24. https://doi.org/10.3390/fi13020024

Academic Editor: Kien Nguyen
Received: 8 December 2020
Accepted: 18 January 2021
Published: 22 January 2021

1. Introduction

The Internet of Things (IoT) is a network of devices (e.g., sensors), where they communicate and interact with the surrounding. With the fast growth of applications and services designed for IoT, communication and interaction are becoming a challenge due to the massive number of connected devices and the lack of a robust dynamic identity management solution [1,2]. Identity management of things is allocating identifiers to IoT physical and logical entities from motion, and temperature sensors to scrolling and screen behavior trackers in phones enabling them to exchange data with the other entities effectively and securely, while taking the relationship and the lifecycle of entities, addressability, and authentication methods into consideration [3–5].

The identity management of things is a fundamental feature of IoT, notably many academic investigations proposed solutions and standards to tackle the different challenges of the IdM [6,7]. The conventional solutions mostly adopt a centralized architecture, which may lead to a single point of failure. On the other hand, scalability is another issue regarding the maintenance and infrastructure of identity management solutions.

A consortium blockchain is a permissioned blockchain that is composed of a group of participants that collaborates to set policies and manage all of the interactions in the BC network. Consortium blockchains are faster, highly scalable, and provide transaction privacy, as the participants authenticate to the system before performing any interaction; less energy consumption as compared to public blockchains, as it is less computationally complex and has pre-selected nodes controlling the consensus mechanism. Additionally, IoT devices and sensors need solutions with lower energy consumption [8] .

Integrating blockchain technology with identity management will be the solution for some prevalent issues, such as centralized governing of identities, which also leads to some security and availability issues, such as a single point of access and single point failure. Moreover, blockchain will eliminate the need for trusted third parties to perform checks on identities as the blockchain ledger is distributed across the consortium participants. The clients will have control over their personal information, as the data in BC are immutable, encrypted, and cannot be deleted. Many industry leaders are keen to adopt blockchain in order to enhance the privacy and security of their identity management infrastructure and to change their traditional business model or to build the economy of sharing concept. Despite this, the blockchain is not adequate for all businesses, and any unstructured or inadequate ready to use solution may lead to failure due to shifting the business strategy for centralizing to the decentralized concept.

The paper contribution is to propose a lightweight blockchain-based IoT identity management approach. First, we present our work architecture describing blockchain-based identity management and the associated protocol of registration, verification, and revocation. Our protocol addresses privacy and security issues in traditional centralized systems, and spotlights the concept of distributing the authority of an identity system to a group of organizations. Furthermore, we implement the proof-of-concept prototype and evaluate the approach of splitting the main functionalities of an identity management system to separated immutable ledgers and discussed the results. Finally, we give a detailed related work comparison and present our future research directions.

The remainder of this paper is organized, as follows. Section 2 discusses the related work. Section 3 presents the proposed blockchain-based identity management approach.Section 4 introduces the implementation of a proof-of-concept prototype. Section 5 presents and discusses the evaluation of used approach and conducts a detailed comparison with related work. Finally, Section 6 concludes the paper and highlights the future work.

2. Related Work

With the fast growth of the Internet of Things area, the role of identity management is expanding to cover sensors, actuators, and smart devices. The role is more about to grant access to IoT services and applications and to monitor sensors. Many scholars have undertaken the identity management of things area and proposed several models and frameworks in order to support the fast-growing IoT network.

A. Fongen [9] proposed a framework for authentication and integrity protection while using simple cryptography operation. The work discussed the tamperproof authentication and the trust model, while taking the lightweight IoT units into consideration. Zhao et al. [10] presented a novel asymmetric mutual identity authentication scheme for IoT-based on hash algorithms and elliptic curve cryptography technique. The structure focuses on two primary roles, the platform and a terminal node, while a certificate authority center is responsible for issuing and verifying all of the exchanged certificates. Bernabe et al. [11] tailored a novel holistic and privacy-preserving solution for the Internet of Things. They coped the authentication and access control systems with the claims-based approach. They also used the Idemix credential system to hide sensitive identity attributes.

The works that are mentioned above lack implementation and real-world use cases; besides, all of the papers adopted the traditional IdM centralized approach that has already shown weak security and privacy performance. Moreover, combining cryptography primitives with the existing solutions without taking into consideration that the IoT decentralized network architecture and requirements, such as guaranteeing secure communication between different IoT entities, assuring data privacy and integrity, and providing high availability when authenticating and authorizing IoT entities, will lead to a standstill.

On the contrary to the centralized approach, Lo et al. [12] reviewed many works regarding identity management models while using blockchain technology. According to their review, few articles proposed particular identity models to manage things, while most of the studies used PKI (Public Key Infrastructure) mechanism for implementation.

They also claimed that all of the reviewed identity models that are based on blockchain are not mature enough to back the IoT network.

Dorri et al. [13] investigated a case of using blockchain in a smart home where they considered high resource devices as miners, responsible for handling all intelligent home communication and preserving the private blockchain. The work audited the security, integrity, and availability of the framework.

Moreover, Sonnino et al. [14] proposed a selective disclosure credentials scheme framework in order to ensure confidentiality, authenticity, and availability. Mainly, the work tries to fill the privacy research gap by enabling selective disclosure credentials while using the cryptography primitives that are offered by Ethereum blockchain and chainspace protocol. Bao et al. [15] presented IoTchain; a three-tier blockchain-based IoT security architecture comprises an authentication, blockchain, and application layers that are designed to leverage many features, such as identity authentication, access control, and privacy protection. Brogan et al. [16] discussed the benefits of adopting the distributed ledger technology to advance the electronic healthcare domain. In this work, they discussed the need for using DLT in order to ensure the authenticity, integrity of the data generated from health, and wearable, embedded devices using IOTA protocol as a core technology of their work.

To the best of our knowledge, all of the reviewed blockchain-based identity management solutions and decentralized identity frameworks did not discuss the identity management functions and lifecycle of an entity inside the network, the interoperability, or entities' interaction in the network. Additionally, the public blockchain platforms used for implementation, such as Ethereum and IOTA protocol, are having some significant issues regarding scalability and security [17]. On the other hand, some reviewed work used simulators and not IoT real cases, which makes the results lack solidity.

3. Blockchain-Based Identity Management Architecture and Protocols

In this section, we first present the architecture for blockchain-based identity management and then presents the detailed protocol of the system.

3.1. Architecture

The Internet of Things is changing the era of digital identity drastically from user-centric to entity-centric [18,19], where identity management should focus on all entities participating in the IoT network. As all entities in the IoT have the same interaction ecosystem, the IoT identity management must be able to manage human-to-device, device-to-device, and device-to-application interactions and data exchange while taking into consideration the relationships between the different IoT entities, as shown in the Figure 1. All of the communication endpoints in the IoT ecosystem, such as users, smart things, and applications, should register and authenticate to the blockchain-based IDM. The blockchain-based IDM network is the backbone for the IoT system that formed by a defined consortium sharing the same industrial needs or business interests that are responsible for building and defining the network policies and governing the shared ecosystem. The blockchain-based IDM solution includes a consortium membership service and identity management protocol. The membership service is responsible for issuing and revoking authority certificates for the network components, such as BC admins, nodes, consensus ordering, and communication channels. Unlike the other works, our design aims to split the identity protocol into three phases identity registration, identity verification, and identity revocation, and each phase is taking place by issuing, resolving, or revoking unique identifiers as well as certificates to each entity. The identity protocol employs smart contracts to interact with the blockchain network. On the blockchain ledger, each block contains a set of identity transactions that are issued by the identity protocol. In addition to the decentralization, privacy, and security offered by DLT, our design goals include simplicity to provide an efficient protocol to meet the needs of all IoT organizations. Interoperability, to permit sharing sensors within and across organizations by following the

decentralization standards. Extensibility, by employing only the main phases of an identity system on the top of the DLT structure, which can be tailored by all identity management of things models .

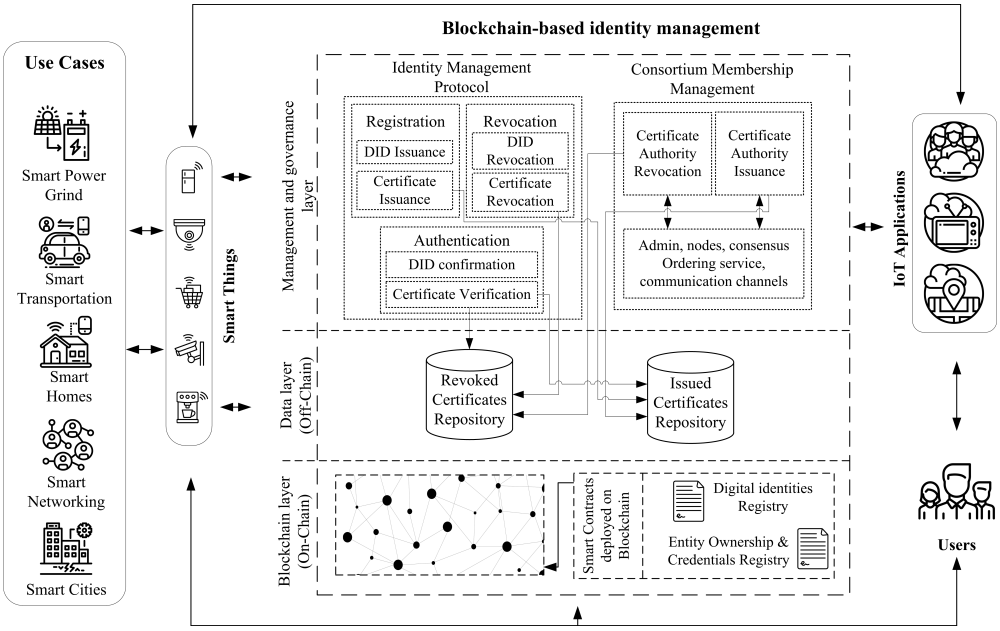

Figure 1. Consortium blockchain-based identity management architecture and interaction.

Adopting a modular consortium blockchain architecture will help to match any use case in all domains, and it gives a greater degree of flexibility and resiliency. The consortium blockchain should provide essential architecture components to meet the need of a blockchain-based IDM, such as:

- Identity protocol: several existing BC solutions use remote procedure call (RPC) as an identity service; all other solutions also make use of BC cryptography primitives to perform such services that lead to weak entities identity management. Designing an identity protocol on the top of the BC solution will help to manage the solution effectively and have more control regarding transaction types and transactions outcome.
- Membership service: is a crucial component in the consortium blockchain network. Membership service is responsible for listing the defined participants, mapping the resources of the participants, and, most importantly, setting the roles and access privileges of the network resources, such as admins, nodes, ledgers, and communication channels.
- Network policies: in order to form a solid structure of the consortium and to reach specific outcomes, all of the participants and the IoT entities should follow the endorsement policies that are defined by the network participants. Such arrangements provide robust governance over the network and assure transparency and enforce consortium decisions in order to reach the needed outcomes.
- Smart contract: generates an executable logic in order to interact with the immutable blockchain record. Developing a refined smart contract will help to keep the records guarded and it reduces security concerns. Identically, governing and verifying the parameters of the smart contract by enforcing network endorsement policy before interacting with the ledger will make it less vulnerable.
- Ordering service: consortium ordering service is a crucial component that is composed by the participants nodes, working collectively to form the setting that is responsible for performing the consensus process within the network, such as maintaining the list of organizations, admins, nodes that are allowed to be part of the consortium, while also validating and restricting smart contracts transactions.

3.2. Protocols

Each entity is registered to the blockchain network only one time, as the blockchain provides a unique identifier to each entity used globally, while authentication is to present one or more of entity credentials after registration for verification and the process is occurring each time that the entity interacting with the other entities. In the same manner, revocation is an infrequent function for all entities, and an entity holder can only revoke his identity one time, as shown in the Figure 2.

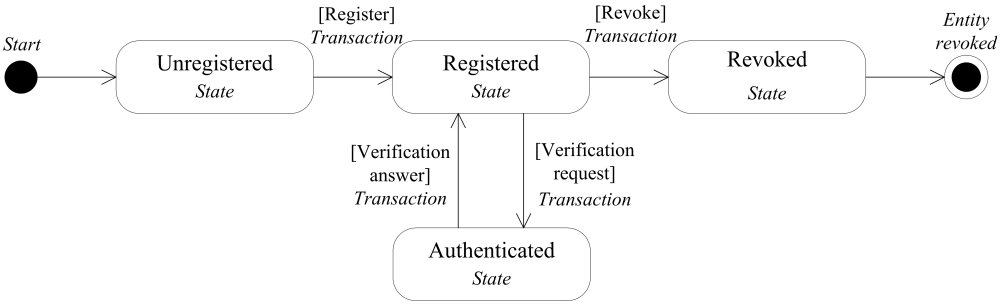

Figure 2. The lifecycle of an entity inside the consortium blockchain-based identity management system.

3.2.1. Identity Registration

The registration phase consists of providing participants a unique identifier ID and the tools that are needed to join the consortium network. The trusted admins manually register the different entities to answer the trust and credibility of the identity solution. An entity sends a request for registration; in a moment of receiving the query, the DLT platform runs the registration function that contains three main steps, checking the existence of the registered entity, assigning a unique ID, communicate the ID to the requester, as shown in Figure 3.

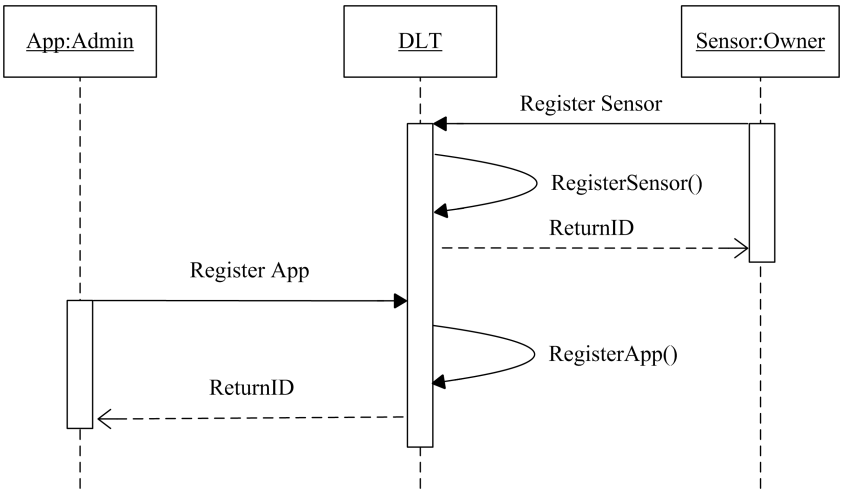

Figure 3. The registration Sequence Diagram.

After defining the needed data for registration by the consortium, each entity owner sends his essential identity credentials $identity_{info}$ which uniquely identifies a realistic $Entity_i$ usually in the form of text managed by the entity owner and encrypted by the private owner key in the *DLT*. The hash of $identity_{info}$ combined with *DLT* metadata form the unique identifier ID_i.

$$ID_i = Hash(identity_{info}, DLT_{metadata}) \quad (1)$$

Consequently, the $identity_i$ of an $Entity_i$ in the system is the combined ID_i and the ledger address where the identity information is stored $Address_i$.

$$identity_i = (ID_i, Address_i) \tag{2}$$

In practice, we assume that updates of identity information may not accrue as the solution collects the essential information; in the same manner, the DLT address may also change. In order to keep track of the different addresses, we combine the new address to $identity_i$ to form an updated identity as follow.

$$identity_i = (ID_i, Address_i, Address_i^{'}, Address_i^{''}) \tag{3}$$

3.2.2. Identity Verification

Identity verification or authentication is an essential feature in all identity systems, as it enables organizations to keep their networks secure by only permitting the authenticated entities to access the resources. As long as the entities registered to the network, authentication is the next step, where an entity is inspected by checking its credentials if matches in the distributed ledger. An entity sends an authentication request, and the platform checks the existence of the entity in the first place, then, if the entity exists in the ledger, the platform will record the request and send the authentication answer to the requester, as shown in Figure 4.

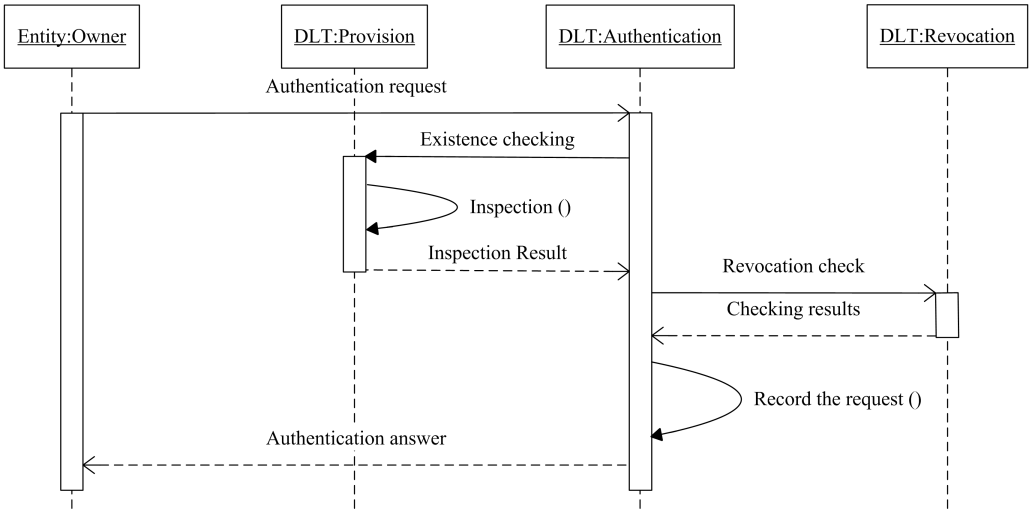

Figure 4. The authentication sequence diagram.

Adopting the mechanism of digital certificates, the inspection process that is based on public key infrastructure technology, where the private key of the entity owner sign the authentication request before sending it, and the public key of the same entity is used in order to check the validity of the received request. The recorded transaction after a successful authentication contains the information of the requester $identity_{info}$, the output of the transaction O, and the ledger state S.

$$T_{auth} = (identity_{info}, O_i, S_i) \tag{4}$$

3.2.3. Identity Revocation

The identity revocation is repealing entities from accessing to the network resources, as the consortium defines the revocation rules. The revocation is an infrequent function, our design uses a separate ledger that only contains the revoked identities, and, before any authentication operation, the network inspects the entity request by parsing the revocation ledger, as shown in Figure 4. Henceforth, the reason behind splitting the

identity registration and identity revocation functions is to preserve the decentralized, simple, and extensible design architecture.

4. Implementation

In this section, we implement our architecture while using Hyperledger Fabric for the smart home scenario, where many services are designed in order to make use of the home sensors to improve the quality and efficiency of the assisted living environment. Our proposed model aims to support interoperability and cross-domain data exchange while using IoT devices and sensors, an identity model that is based on Hyperledger Fabric, which is a pluggable transactional network that delivers a high degree of flexibility, resiliency, and confidentiality. In the beginning, all of the smart home sensors should register to the blockchain identity solution by providing the necessary information, while, in the same manner, all of the services should roll onto the distributed identity network.

4.1. Fabric Consortium Network

Taking advantage of Hyperledger Fabric, a distributed operating system for permissioned blockchain, the proposed network infrastructure consists of four organizations, R1, R2, R3, and R4, which form the consortium and each organization participates with one peer node (P1, P2, P3, and P4) and one orderer node (O1, O2, O3, and O4) respectively, three channels of communication C1, C2, and C3, and three ledgers matching registration, authentication, and revocation, L1, L2, and L3, as shown in Figure 5. In the same manner, three smart contracts (chaincodes S1, S2, and S3) are responsible for executing the identity management functions in the network and two applications A1 and A2, which represent two services interact with the blockchain network.

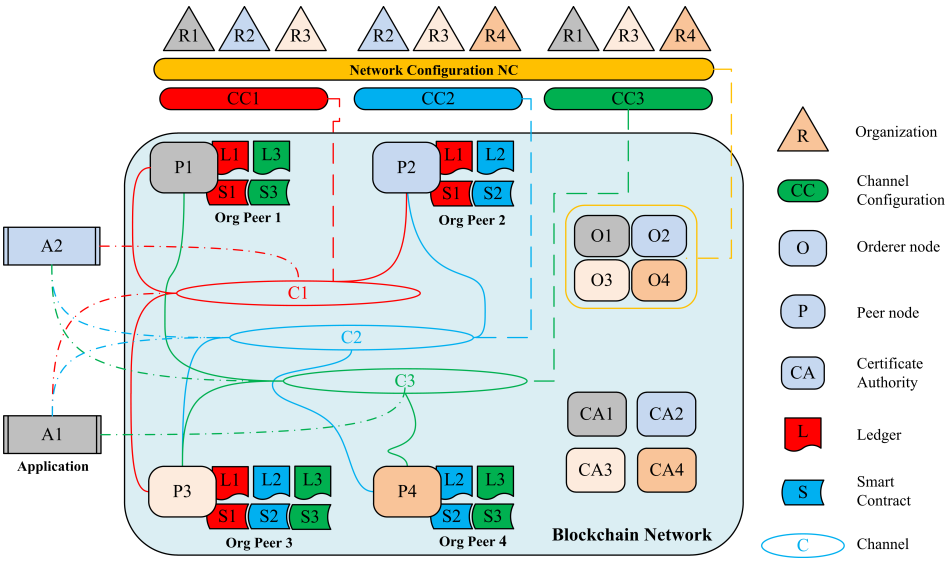

Figure 5. The blockchain-based identity management network architecture.

4.2. Organization

The permissioned blockchain solutions maintain an access control layer in order to allow only identifiable participants or organizations to perform actions in the network. An organization itself manages a group of members and participants (nodes) in the network with the help of the membership service provider (MSP). Each organization has an MSP connected to the certificate authority (CA1, CA2, CA3, and CA4) responsible for issuing nodes credential and maintaining all of the participating nodes in the system, authenticating all of the interactions occurring in the network, and verifying the integrity of transactions typically by digital signatures. After recognizing the participating organization, a network initiator or a network configuration (NC) that formed by the organizations to define and control the network nodes, channels, and interactions.

4.3. Peers

Peers are primary elements of the blockchain network, as they host the ledgers and chaincodes. In the projected infrastructure, we have peer nodes (P1, P2, P3, and P4) that are responsible for connecting the application to the ledger and executing chaincodes following the endorsement policy that was defined by the consortium. Peers interact privately with each other and applications while using channels mechanism. Moreover, ordering service composed by orderer nodes (O1, O2, O3, and O4), called consensus mechanism, to manage and retain peer's ledger consistency. Hyperledger fabric separate consensus nodes from the peer's nodes to make it a modular design, less time consuming, and configurable by introducing the execute-order-validate architecture. Ordering service is central to this process, as it establishes the total order of all the transaction in fabric.

4.4. Channels

Every three organizations on the proposed infrastructure form a channel configuration (CC) that control a matching channel (C), for instance, R1, R2, and R3 form CC1, which controls the channel C1, while R2, R3, and R4 form CC2, which controls the channel C2, equally R1, R3, and R4 form CC3, which controls the channel C3. A channel in Hyperledger Fabric is a private communication tunnel between the network members; it assures high privacy and confidentiality of the data exchanged. Network members define the channels and the policies of each channel, and the participating peers, which lead to wholly separate ledgers, yet it is always possible to applications and Chaincodes to access different ledgers and establish communication between the different channels.

4.5. Chaincode (Smart Contract)

Hyperledger fabric introduced the concept of decentralized governance for a smart contract, where the consortium defines the parameters of the contract and verifies them before any interaction with the network (S). The consortium ledger only contains the necessary information to manage the identity of an entity, and the needed data are collected during the registration phase using the registration chaincode S1. Meanwhile, the authentication phase consists of accessing the data and verifying the authenticity of the entity using the authentication chaincode S2.

5. Results

5.1. Experiment Setting

We implemented the identity model on the top of Hyperledger fabric, the distributed operating system for permissioned blockchains, in order to investigate our proposed identity design. In the experiment, we did not consider a large number of sensors and services as the Hyperledger fabric showed an excellent scalability performance [20]. We implement the solution in a virtual machine running Ubuntu with 24 GB of RAM and 12 vCPU Intel Xeon e5-2620 v2 2.10 GHz, and we use Golang language to write the chaincodes.

5.2. Payload Data

All of the sensors and services in the smart home have to register to the distributed identity network once and authenticate each time they react with another object. We attached the payload of sensor registration as shown in Figure 6, which is a JSON document that contains the essential information regarding the organization issued the document, owner, and associated sensor information. Another critical point is that only admins that are approved by the consortium can perform the registration procedure and the membership service provider (MSP) system in Hyperledger Fabric is responsible for creating users and administrators of the network.

```
{
  "@context": [
    "www.example.com/v1",
    "www.example.com/credentials/examples/v1"
  ],
  "type": "VerifiablePresentation",
  "proofPurpose": "Registration",
  "verifiableCredential": [
    {
      "entityID": "urn:uuid:cd9f930e-a3b4-423a-850b-3c81135f0f7e",
      "entityType": "sensor",
      "issuer": "org1.example.com/issuers/565049",
      "issuanceDate": "2019-08-29T19:73:24Z",
      "credentialSubject": {
        "entityName": {
          "en-us": "Temperature sensor",
          "*": "Cooling Water Temperature"
        },
        "measureUnit": "°C",
        "measureType": "numeric",
        "measureDisplayUnit": {
          "en-us": "°F",
          "*": "°C"
        },
        "measureUnitPrefix": {
          "en-us": "Tmp"
        },
        "measureUnitSuffix": {
          "jp": "Dgr",
          "en-us": " °F",
          "*": " °C"
        },
        "measureUnitSuffixEx": {
          "en-us": " degrees Fahrenheit",
          "*": " degrees Celsius"
        }
      }
    }
  ]
}
```


Figure 6. A payload represents a temperature sensor for registration phase.

5.3. Payload Size

We conduct four experiments to measure the invocation time and query time while using different payload size in two channels (registrations and authentication), while, in each experiment stage, we use trials of 100 transactions for each given payload size, as shown in Table 1. The table resumes the results of the four experiments, including the payload size, transaction action, the average time of the trials, minimum and maximum of the transaction latency, and throughput. The time that is required to execute-order-validate a transaction in fabric changes according to the payload size, the number of peers, orderers, and the endorsement policy. We can observe that the payload size is a critical fabric parameter that affects both transaction latency and throughput.

Table 1. The payload size (PLS), transaction action, the average time of the trials, minimum and maximum of the transaction latency, and throughput (transaction per second) for registration and authentication ledgers.

Channel	PLS (MB)	Action	Avg (Ms)	Min (Ms)	Max (Ms)	Tps
Registration	0.5	Invoke	170	142	198	6
Registration	1	Invoke	205.5	191	220	5
Registration	1.7	Invoke	255.5	243	268	4
Registration	0.5	Query	52.5	41	64	19
Registration	1	Query	69	56	82	14
Registration	1.7	Query	104.5	89	120	10
Authentication	0.5	Invoke	145	129	161	7
Authentication	1	Invoke	161	141	182	6
Authentication	1.7	Invoke	204.5	190	219	5
Authentication	0.5	Query	49.5	41	58	20
Authentication	1	Query	59.5	52	67	17
Authentication	1.7	Query	85	74	96	12

5.4. Invoke and Query Operations Cost

The transaction logic that is used in this work is simple and only covers the essential features of registration and authentication functions. Besides, the smart contract developed is not computer-intensive, in order to avoid any complexity, as it affects the operation time. In particular, the authentication transaction needs to fetch information from the registration ledger to match the credentials of the requester, which is the only dependency of the coded smart contract (chaincode).

In this experiment, we adopt 0.5 MB as a block size for maximizing the throughput of both registration transactions and authentication transactions, executing 100 trials for each action. The average time of registration invocation transactions is 170 (Ms), with a throughput of six transactions per second, as shown in Figure 7. Meanwhile, the average time of query transactions is 52.5 (Ms) with a throughput of 19 transactions per second, as shown in Figure 8. The average time of authentication invocation transactions is 145 (Ms),

with a throughput of seven transactions per second, as shown in Figure 9. Meanwhile, the average time of query transactions is 49.5 (Ms) with a throughput of 20 transactions per second, as shown in Figure 10.

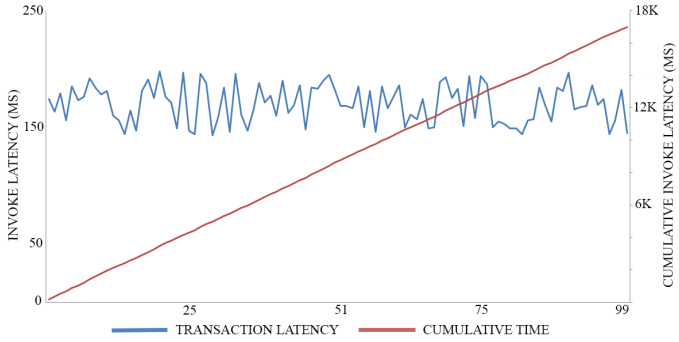

Figure 7. Registration invocation cost.

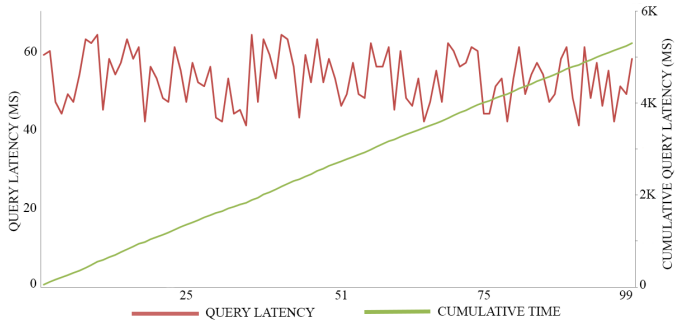

Figure 8. Registration invocation cost.

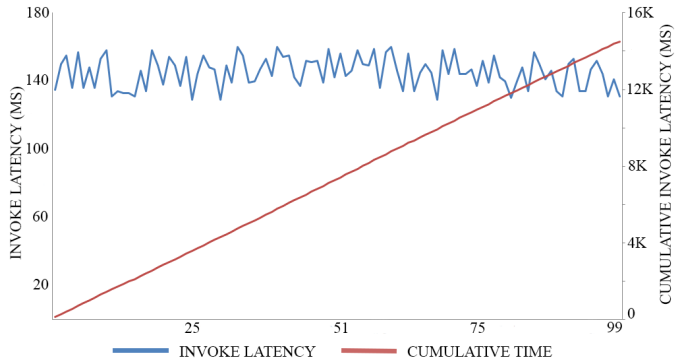

Figure 9. Authentication invocation cost.

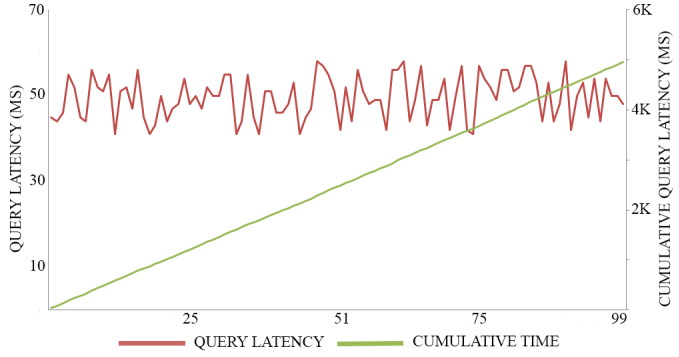

Figure 10. Authentication query cost.

5.5. Discussion

In this paper, we proposed a distributed identity system that is based on consortium blockchain technology, and we implemented it while using hyperledger fabric platform. Our design consists of splitting the main functions of identity management, such as registration, authentication, and revocation in three separated ledgers that can communicate with each other and exchange information privately. The aim of splitting the ledgers is to meet the scalability of IoT fast-growing environment by ordering the transactions and minimizing the waiting time, for example, executing a registration transaction of sensor A and an authentication transaction of sensor B can take place simultaneously, as the ledgers and communication channels are separated.

From the experiment, the query time (reading from blockchain) is less then invocation time (writing on the blockchain), which can be another benefit of splitting the functions in different ledgers. For instance, when an authentication transaction initiated a query transaction will be executed in the registration ledger to check the existence of the object, as the results registration ledger only contains the registred object, which can save time from querying one ledger containing all of the information to querying a specific ledger containing a precise data.

Another critical point of splitting the ledgers is to minimize the payload size of the transaction as the experiment shows poor performance when invoking or querying a big block size. Hyperledger fabric transactions are of considerable size, because they carry certificate information. In the experiment, we used the unique object identifier in order to aggregate the information of different payloads of the same object.

Scalability in IoT is a pivotal performance aspect for meeting the fast-growing era. In our proposed solution, we split one primary ledger holding all identity transactions into three separate ledgers containing registration, authentication, and revocation transaction data. The aim of splitting the ledger is to allow simultaneous execution by design and reduce the payload size of thousands of transactions to support fast querying and invoking operations on the network. Moreover, consortium blockchain is faster, as it has fewer nodes to participate in ordering service and writing on the ledger. Besides, it provides better scalability, as it supports adding nodes on demand (modular design) and uses different consensus algorithms for better performance, as there is no double speeding problem to avoid or 51% attack and hard fork. However, consortium blockchain nature can be more toward centralizing some aspects, which constitutes manipulating the blockchain at a high level to meet the business needs and protect the network from malicious actors.

Besides the block size, the transaction success rate (TSR) is another critical parameter in a transactional system, like blockchain, in our experiment, the TSR is 100% as we executed 100 trials and all were successful. Equally, many other parameters may affect the transaction cost and the performance of blockchain-based identity management, such as:

- The consensus protocol is a crucial component of the blockchain network, being responsible for completing overall system reliability between the consortium members. Hyperledger fabric features an ordering service that is responsible for transaction flow ordering and maintaining the list of the participated organization in each channel. The modularity and pluggable architecture of hyperledger fabric gives it the advantage of using different consensus algorithms, such as KAFKA, RAFT, and Practical Byzantine Fault Tolerant (PBFT), while each protocol may have a typical use case. In the experiment, we used the Solo ordering for testing our implementation, but we cannot use it for production.
- Geographic distribution of nodes is another important aspect, as it involves the network setup and the hardware configuration of each node. Such parameters may affect the transaction latency and throughput. In our experiment, we could not measure such parameters, as all of the nodes have the same network and configuration.
- The type of database used for the world state store is not less important from the other parameters that can affect both transaction latency and throughout. Hyperledger Fabric, by default, uses LevelDB to store simple key-value pairs and it has many

options to use for structured documents, such as relational data, JSON, graph store, or any other type of database, because fabric has a pluggable architecture.

5.6. Comparison with Related Works

Alongside the seven key aspects that are granted by adopting a blockchain-based identity management system, we compare our solution with related works based on the benchmarks for blockchain-based identity management systems [21]. Table 2 presents the comparison.

Table 2. Comparison of our identity solution with other relevant blockchain-based identity frameworks.

Works	BC Platform	Domain	Computing Power	Block Size	Trial	Transaction Time
[13]	Cooja Simulator	Smart home	-	16–36 Bytes	-	69 ms
[14]	Ethereum	-	Intel Core i5 12 GB RAM	-	100	Create: 27.25 ms Verify: 120.17 ms
[14]	Chainspace	-	-	Create: 1.38 KB, Verify: 1.76 KB	10,000	Create: 12.1 ms, Verify: 19.3 ms
[15]	Contiki 2.7 Simulator	-	-	0.8 MB	-	Write: 6 s, Read: 9 s
[16]	IOTA protocol	Health activities	Intel i7–7700 HQ @ 2.80 GHz	500 Char	300	Create: 386 ms, Attach: 12.8s
[16]	IOTA protocol	Health activities	ARMv7 Processor rev 5 (v7l)	500 Char	300	Create: 6.07 s, Attach: 16.6s
Our Work	Hyperledger Fabric	Smart home	Intel Xeon e5-2620 v2 2.10 GHz–24 GB RAM	1 MB	100	Reg-Invoke: 205.5 ms, Reg-Query 69 ms, Auth-Invoke: 161 ms Auth-Query: 59.5 ms

For instance, Sonnino et al. [14] used Ethereum to evaluate their work that displayed fast transaction time. However, they noticed and considered the limitations of using Ethereum, such as high cost and transaction long latency, which is around 6 min. in the Ethereum production network. Brogan et al. [16] used the IOTA protocol in order to conduct their experiment where the transaction time took a few seconds for the block size of 500 characters. Moreover, IOTA analyzed as a centralized solution as the coordinator node (consensus node) is operated by the IOTA foundation, leading to a single point of failure. Bao et al. [15] used a simulator to evaluate their achievement. However, the reading and writing time take 6 to 9 s, which is not a good result for an IoT IdM solution supporting billions of devices. Similarly, Dorri et al. [8] also used a simulator to evaluate their work. They adopted 16 to 36 bytes transactions without including the payload the certificate data.

In our work, we used a permissioned blockchain to leverage a decentralized, secure, and fast solution. The average writing time of 1 MB transaction can take around 205 milliseconds, while the average reading time is 69 milliseconds. Although, we may still need to geographically distribute the blockchain nodes to different locations to obtain the estimates latency for a production network.

6. Conclusions and Future Works

This paper presents a lightweight identity management approach that is based on consortium blockchain for the internet of things. In the first place, we present the identity management design and architecture. We explain the different identity management functions that are covered in our design and the matching protocol, and discuss the identity life cycle inside the system. We discuss the principal characteristics for establishing IoT identity management at the top of the permissioned blockchain. Besides, we implement our solution and justify the use of private blockchain over the public one and discuss the

different parts of the implementation. Moreover, we discuss the results of the experiment. We highlight the advantages of our identity model design, tackling the interoperability, and entities' interaction, also the advantages of using a permissioned blockchain to answer the scalability and security issues. We also provide a detailed comparison with related work. The results show that the approach is suitable for business adoption.

Future research and the milestones of implementing robust blockchain-based identity management will include:

- Provide an automatic registration process by defining the level of trust:
  IoT is a fast-growing environment that connects people, sensors, services, and application in order to perform an infinite number of activities in the aim to simplify the surrounding and assist people life. Nowadays, each person may have more than one device, and each service may use thousands of connected sensors, which is making it difficult for a human to manage the large connected objects. Providing an automatic process to register the different objects is a must for meeting the fast growth of the IoT environment by defining a system that can calculate and define the trust level. In order to calculate the trust level of each entity, we see the entire life-cycle of the entity in the network, the authentication success rate, and the security updates received from the IoT vendors.
- Multi-factor authentication using the concept of community validation:
  Increasing the security of blockchain identity management and protecting the identities of the different objects is a critical aspect, a multi-factor authentication method should take place utilizing the capabilities of blockchain to answer the security and privacy of the identities. The concept of community validation is about validating an entity by making use of other entities that may have similarities like location, function, using time, owner, and other parameters. Firstly, the consortium network will define the governance strategy and the verification methodes, and then the arbitrary entities will send random verification transactions and determine the authenticity of the entities based on received responses.
- An identity lookup mechanism for searching sensors:
  The fast-growing number of IoT connected devices and sensors can be an issue when searching for devices and sensors while using different characteristics, such as location, function, time, and transducers (sensors or actuators). The IoT is designed to give personalized and flexible application and adapt to any changes by collecting data based on different scenarios to enhance to quality of provided services. The existing search mechanisms are centralized by design, which makes them not unfit for a decentralized architecture. Providing an identity lookup and resolver to search and query sensors based on different characteristics and scenarios in a decentralized fashion is a pivotal aspect in enabling the potential of IoT.

Author Contributions: Conceptualization, M.A.B. and Q.L.; Methodology, M.A.B. and Q.L.; Project administration, Q.L. and H.N.; Resources, M.A.B. and S.D.; Supervision, S.D. and H.N.; Validation, Q.L. and H.N.; Writing—original draft, M.A.B.; Writing—review & editing, M.A.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not Applicable, the study does not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hu, P.; Dhelim, S.; Ning, H.; Qiu, T. Survey on fog computing: Architecture, key technologies, applications and open issues. *J. Netw. Comput. Appl.* **2017**, *98*, 27–42. [CrossRef]
2. Ning, H.; Ye, X.; Sada, A.B.; Mao, L.; Daneshmand, M. An Attention Mechanism Inspired Selective Sensing Framework for Physical-Cyber Mapping in Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 9531–9544. [CrossRef]
3. Farha, F.; Ning, H.; Liu, H.; Yang, L.T.; Chen, L. Physical unclonable functions based secret keys scheme for securing big data infrastructure communication. *Inf. Sci.* **2019**, *503*, 307–318. [CrossRef]
4. Zhang, Y.; Xu, X.; Liu, A.; Lu, Q.; Xu, L.; Tao, F. Blockchain-Based Trust Mechanism for IoT-Based Smart Manufacturing System. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1386–1394. [CrossRef]
5. Sivagnanam, S.; Nandigam, V.; Lin, K. Introducing the Open Science Chain: Protecting Integrity and Provenance of Research Data. In Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (Learning), PEARC '19, Chicago, IL, USA, 28 July–1 August 2019; Association for Computing Machinery: New York, NY, USA, 2019.
6. Ning, H.; Liu, X.; Ye, X.; Zhang, J.H.W.; Daneshmand, M. Edge Computing Based ID and nID Combined Identification and Resolution Scheme in IoT. *IEEE Internet Things J.* **2019**, 6, 6811–6821. [CrossRef]
7. Hu, P.; Ning, H.; Qiu, T.; Xu, Y.; Luo, X.; Sangaiah, A.K. A unified face identification and resolution scheme using cloud computing in Internet of Things. *Future Gener. Comput. Syst.* **2018**, *81*, 582–592. [CrossRef]
8. Del-Valle-Soto, C.; Durán-Aguilar, G.; Cortes-Chavez, F.; Rossa-Sierra, A. Energy-Efficient Analysis in Wireless Sensor Networks Applied to Routing Techniques for Internet of Things. In Proceedings of the International Conference on Applied Human Factors and Ergonomics, Washington, DC, USA, 24–28 July 2019; pp. 312–321.
9. Fongen, A. Identity management and integrity protection in the internet of things. In Proceedings of the 2012 Third International Conference on Emerging Security Technologies, Lisbon, Portugal , 5–7 September 2012; pp. 111–114.
10. Zhao, G.; Si, X.; Wang, J.; Long, X.; Hu, T. A novel mutual authentication scheme for Internet of Things. In Proceedings of the 2011 International Conference on Modelling, Identification and Control, Shanghai, China, 26–29 June 2011; pp. 563–566.
11. Bernal Bernabe, J.; Hernandez-Ramos, J.L.; Skarmeta Gomez, A.F. Holistic privacy-preserving identity management system for the internet of things. *Mob. Inf. Syst.* **2017**, *2017*, 6384186. [CrossRef]
12. Lo, S.K.; Liu, Y.; Chia, S.Y.; Xu, X.; Lu, Q.; Zhu, L.; Ning, H. Analysis of Blockchain Solutions for IoT: A Systematic Literature Review. *IEEE Access* **2019**, *7*, 58822–58835. [CrossRef]
13. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
14. Sonnino, A.; Al-Bassam, M.; Bano, S.; Meiklejohn, S.; Danezis, G. Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers. *arXiv* **2018**, arXiv:1802.07344.
15. Bao, Z.; Shi, W.; He, D.; Chood, K.K.R. IoTChain: A three-tier blockchain-based IoT security architecture. *arXiv* **2018**, arXiv:1806.02008.
16. Brogan, J.; Baskaran, I.; Ramachandran, N. Authenticating health activity data using distributed ledger technologies. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 257–266. [CrossRef] [PubMed]
17. Lin, I.C.; Liao, T.C. A Survey of Blockchain Security Issues and Challenges. *IJ Netw. Secur.* **2017**, *19*, 653–659.
18. Dhelim, S.; Ning, H.; Bouras, M.A.; Ma, J. Cyber-enabled human-centric smart home architecture. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 8–12 October 2018; pp. 1880–1886.
19. Dhelim, S.; Ning, H.; Cui, S.; Ma, J.; Huang, R.; Kevin, I.; Wang, K. Cyberentity and its consistency in the cyber-physical-social-thinking hyperspace. *Comput. Electr. Eng.* **2020**, *81*, 106506. [CrossRef]
20. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; p. 30.
21. Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. *Sensors* **2020**, *20*, 483. [CrossRef] [PubMed]