systems

MDPI

Article

Developing an IoT Identity Management System Using Blockchain

Sitalakshmi Venkatraman * and Sazia Parvin

Melbourne Polytechnic, 77 St Georges Rd, Preston, VIC 3072, Australia; saziaparvin@melbournepolytechnic.edu.au

* Correspondence: sitavenkat@melbournepolytechnic.edu.au; Tel.: +61-3-9269-1171

Abstract: Identity (ID) management systems have evolved based on traditional data modelling and authentication protocols that are facing security, privacy, and trust challenges with the growth of Internet of Things (IoT). Research surveys reveal that blockchain technology offers special features of self-sovereign identity and cryptography that can be leveraged to address the issues of security breach and privacy leaks prevalent in existing ID management systems. Although research studies are recently exploring the suitability of blockchain based support to existing infrastructure, there is a lack of focus on IoT ecosystem in the secured ID management with data provenance of digital assets in businesses. In this paper, we propose a blockchain based ID management system for computing assets in an IoT ecosystem comprising of devices, software, users, and data operations. We design and develop a proof-of-concept prototype using a federated and distributed blockchain platform with smart contracts to support highly trusted data storage and secure authentication of IoT resources and operations within a business case scenario.

Keywords: IoT; identity management; blockchain; security; privacy; trust

Citation: Venkatraman, S.; Parvin, S. Developing an IoT Identity Management System Using Blockchain. *Systems* **2022**, *10*, 39. https://doi.org/10.3390/systems10020039

Academic Editor: William T. Scherer

Received: 29 January 2022
Accepted: 15 March 2022
Published: 18 March 2022

1. Introduction

Identity management is a method used to recognise and validate confidential data, as well as determine and authorise user access to such data. Since there is lack of an identity management protocol via the Internet, several service providers are given the responsibility of providing identities and maintain user credentials with granting access rights [1,2]. This method is not efficient as information is duplicated across different service providers and some centralised identity protocol could also be used by several organisations. Further, personal information is constantly being collected without user's knowledge or consent for various purposes, such as profiling and data mining, that could be exploited. There is difficulty in maintaining security and privacy of data as evidenced by data breaches and malicious attacks over the Internet [3,4]. Hence, such a centralised identity management system has serious issues when users are deprived of the identity and rightful ownership of data. In this paper, we propose the use of a new concept of self-sovereign identity where a person's consolidated digital identity is owned and managed entirely by the individual. It includes verified attributes and cryptographically trusted parties thereby enabling users to possess rights and control of their own data and usage. Such a federated and distributed digital identity management system is possible with the recent state-of-the-art blockchain based identity management and authentication frameworks [5,6]. Blockchain provides a secure solution as users can have ownership of their own data and, also, allow or revoke any individual's consent for access [7,8].

In this digital world, the Internet of Things (IoT) that connects devices, individuals, and businesses services presents escalating security and privacy risks due to the current Internet digital identity management solutions [9]. We are gaining importance of IoT in the cyber world for various online transactions such as banking, shopping, tele-health,

and many more day-to-day services. In such an IoT intertwined cyber-physical system that primarily focus on scalability, interoperability and mobility, the growing need of digital identity and data privacy could be addressed using a blockchain platform. It is important for the owner/authorised user of an IoT device to know its identity and have secure access of their own data. Device democracy could be achieved using blockchain to enable self-management of data, as well as access control policies for each IoT device [10]. Public blockchains such as Bitcoin and Ethereum, create public addresses independently to represent the device and latest activities could be used for verification purposes [11]. Multiple virtual nodes in blockchains could represent each physical node. On the other hand, in private blockchains, the devices need to be authorised before being added into the blockchain network. Overall, there is a need for an identity management of private blockchains. Blockchain opensource platforms, such as Hyperledger Fabric provides identity management and implementation of smart contracts for data transactions. However, there are limitations with such private and permissioned blockchain platforms [12,13]. The pros and cons of existing platforms forms the motivation of this research to develop a blockchain based distributed system as a proof-of-concept for IoT users to have full control of their own data and access control policies. Recent models in developing programmable smart contracts emphasise the use of blockchain-based approaches to support device democracy [14–16]. Smart contracts for data accountability and provenance tracking are based on the identity of the data controller or a particular data. Blockchain technology could also be used as a database for storing transactions and access control policies. For each IoT access request, the transaction for granting access could be broadcast to the blockchain network for either approving or rejecting the request, notifying the user accordingly. These approaches form the motivation of our proposed IoT ID management using blockchain technology.

Overall, with the recent growth in IoT, applications, and services, the lack of a robust dynamic identity management solution calls for much research in this direction [17]. Many previous studies have focused on privacy-preserving approaches and its applications particularly to healthcare scenarios [18,19]. In this paper, we propose and develop a blockchain based identity management system for an organisation's IoT ecosystem giving importance to device democracy access control, data privacy, and trust. The main contributions of our paper are: (a) We present a novel blockchain-based modelling for IoT ID management to overcome the data privacy, and security concerns associated with centralised architectures; (b) we demonstrate the application of smart contracts to enable data accountability and privacy preserving transactions with access control policies, and (c) we show the implementation of our proposed model for a business case scenario as a proof-of-concept prototype.

The rest of the paper is organised as follows. In Section 2, we provide a literature review of the recent works on blockchain based identity management solutions and the lack of studies in the context of IoT. We describe a business case scenario requiring a blockchain sovereign identity solution for IoT and propose a suitable blockchain structured model in Section 3. We present the implementation of our proof-of-concept prototype for the IoT case scenario in Section 4. Finally, in Section 5, we summarise our work and the promising research plans for the future in building more features in IoT identity management systems.

2. Literature Review

In the cyber world of today's digital age, digital identity is of paramount importance as there is a growing reliance on the Internet to perform online transactions involving multiple devices and communication protocols. We review the recent studies on various upcoming blockchain sovereign identity solutions. We present below a summary of the state-of-the-art blockchain based identity solutions and their limitations, thereby identifying the gaps found in the literature.

A blockchain-based personal data and identity management system (BPDIMS) is proposed in [20] based on human-centric personal data. The identity management using

blockchain and smart contracts is based on the MyData initiative under the European Union's new General Data Protection Regulation (GDPR). The BPDIMS approach is limited towards establishing the transparency and control over personal data alone and lacks consideration of IoT devices and various interactions among different users of the system. To address this lacuna, our proposed approach considers authorisation and identity management of IoT and various users of the system. Our proposed approach will develop the required smart contract rules to safeguard the IoT resources and end-user authentication.

An encrypted member authentication scheme is proposed in [21] in order to support blockchain concept of identity management systems using a cryptographic membership authentication scheme. In this approach, a new transitively closed undirected graph authentication (TCUGA) scheme is used to enhance the security and efficiency of the proposed scheme. This scheme can dynamically add or remove nodes and edges and demonstrate the security of proposed TCUGA in the standard blockchain oriented model. However, this scheme does not deal with the data minimisation and any request of nodes uses the false positive method to send the certificates to other nodes in the system. Hence, network congestion in sending several certificates during transactions could be a potential practical bottleneck. To overcome this, our proposed approach would be to use blockchain technology as it is efficient in creating encrypted hash for secure digital identities, as well as to use the concept of smart contracts and group policy for member authentication.

Another blockchain-based identity management in [22] proposed access control mechanisms within blockchain for edge computing. Their provision of data security is aimed toward industrial Internet of things (IIoT) by including authentication, auditability, and confidentiality. In order to ensure the IIoT security, their approach at first embeds the generated implicit certificate to its identity and constructs the identity and certificate management mechanism based on blockchain. Secondly, an access control mechanism based on the Bloom filter is designed and integrated with identity management. However, it lacks key agreement protocol and certificate management mechanism. Further, there is a need to have key optimisation mechanism for improving the performance for practical deployments. These drawbacks can be addressed in our proposed approach by creating smart contracts and business rules in order to incorporate an efficient authentication of IoT users.

A hybrid blockchain gateway solution is proposed and developed in [23] in order to support legal compliance and traditional identity management features and also to deal with issues caused by centralised trust systems in organisations. The solution establishes a secure and privacy friendly middle ground between the blockchain and the mundane world (off-chain) using a hybrid solution that comprises of a blockchain gateway and a blockchain framework. However, the undefined and inappropriate interests, policies, and responsibilities between different agents or end-users may cause some challenging issues for authentication and authorised users. This identified problem can be resolved in our proposed approach by managing user access to the blockchains through well-established smart contracts and group policy.

A smart contract-based identity management system (DNS-IdM) [24] is proposed which is able to enable users to maintain their identities associated with certain attributes, accomplishing the self-sovereign concept. The secure and trustworthy management of identities have been maintained by the use of authenticated and unauthenticated blockchains along with smart contracts. However, there are no management policies identified in order to maintain and develop the compliance with digital standards. This problem can be addressed in our proposed approach by embedding standard business rules/policies in a blockchain network in order to ensure the authentication of every IoT user.

A smart contract on a blockchain is used in various domain in order to enable an architecture for the flexible solution, where authentication no longer involves the credential service provider (CSP) [25]. In this approach, an identity management system (IDMS) is proposed by using the features of federated identity management (FIM) that helps users to access multiple systems using a single login credential. In such an approach, a user can

authenticate and transfer attributes to a relying party without having the involvement of a CSP (thereby heightening privacy and reducing costs). One of the limitations of this work is revealing a user's identity by creating clone identity for another user. Any prior knowledge about a user's identity attributes could be used to make this clone identity for some other users. In our proposed approach, this problem can be addressed as a user's identity will be verified and access will be granted only for IoT devices with encrypted digital identities.

A comprehensive literature review has been conducted on the study of blockchain-based identity management systems by [26]. Many possible challenges have been identified in order to outline the risks involved in the blockchain-based identity management system reviewing recent state-of-the-art advances on the topic. Critical analysis and surveys have been conducted based on blockchain-based identities in a professional environment. The abovementioned studies have provided some holistic guidelines that are mostly met with a fair amount of criticism and reservation in professional environments. In [27], an evaluation framework consisting of 75 criteria has been applied to assess 43 blockchain-based identity solutions and their state-of-the-art approaches. The outcome of the investigation has been related to different features, prerequisites, market availability, readiness for enterprise integration, costs, and (estimated) maturity. However, the study lacks any suggestion of possible generic blockchain based solutions for the identified challenges from other research work considered in the survey. We find gaps in literature exploring blockchain based solutions specifically for identity management of IoT.

In [28], it has been argued that self-sovereign identity (SSI) solutions based on blockchain technology have a more technical motivation that obscures key challenges and long-term repercussions. With ubiquitous private data collection in the context of IoT, a range of ethical issues surrounding human identity have been identified. To address privacy and ethical concerns, any proposed approach should cater towards a secure sharing of private and sensitive information and identity of IoT users within a blockchain based identity management system. Every digital asset within an IoT network requires trusted security and user access. In [29], an end-to-end trust has been aimed by applying blockchain to IoT devices. Blockchain has been used by IoT devices to automatically register, organise, store, and share streams of data. However, the solution is restricted towards providing end-to-end trust only for trading and it identifies future research challenges in developing a trustworthy trading platform for IoT ecosystems. Another recent research has focused on designing the main functions of identity management, such as registration, authentication, and revocation using lightweight considerations [30].

Modelling choices for blockchain-based data accountability and provenance tracking have been explored with respect to the design of smart contracts and for addressing performance and authentication issues [31]. The solution choices relate to managing transactions, such as authorisation and auditability properties while adopting a public, consortium/semi-public, or private blockchains. The study was limited to considering contract design, implementation, and performance of the solution to the open source Ethereum Virtual Machine (EVM) only.

Another blockchain solution platform called Hyperledger Fabric is a permissioned blockchain platform where the network members use transactions controlled by the chaincode, a software code installed and executed on its nodes for secure access to the shared ledger. The IoT identity management along with transactions and data are restricted to a separate subset of the network members called a channel. This way the shared ledger of transactions of digital assets is maintained within the channel members only. The subnetworks of a Hyperledger Fabric contain blockchains in the file system of the node and a database of current states of all keys residing in memory to make chaincode interactions efficient [31]. However, different algorithms are used for reaching consensus with ambitious scalability and performance targets. Another work focuses on efficient distributed computing power and network bandwidth for blockchain and smart contracts based on edge computing [22]. Similarly, recent works have proposed a blockchain based framework for Software-Defined Cyber Physical Systems (SD-CPS) as a distributed resource management

solution towards addressing the storage and computing issues of IoT devices [32,33]. These studies lack the consideration of specific issues, such as ID management for a business IoT ecosystem.

In recent years, implications of blockchain technologies in business ecosystems, such as within the supply chain and power industries, have been explored [34–36]. Blockchain technology has also been considered as providing support infrastructure for security considerations in e-government services [37]. However, it has been identified that implementing a robust blockchain-based identity (ID) management for IoT ecosystem in businesses as future research [38,39].

Overall, there is lack of studies in literature for developing a trusted IoT ecosystem in a business scenario using a blockchain platform. In this work, we aim to take an initial step by proposing a blockchain based design and implementation of a decentralised ledger with smart contracts in providing a trusted ID management for an organisation's IoT ecosystem. The purpose is to develop a blockchain based ID management modelling for a simple IoT case scenario as a proof-of-concept prototype development. Our proposed solution aims to provide an integrated blockchain based IoT ecosystem for the organisation's ID management of IoT computing resources, such as devices, software, users, and data assets.

3. Blockchain Based Modelling for an IoT Identity Management System

We consider an organisation facing problems with the identity management system currently in use as our business case scenario. There is lack of technical solutions to support the growth in computing resources with several IoT devices connected to the organisation's network infrastructure. Their current identity management system does not automatically keep track of transactions of the usage or upgradation of company's assets in a highly secure and federated or distributed trust framework. Currently, manual auditing and tracking of their transaction records for each computing resource or digital asset is susceptible to accountability issues and threats of unauthorised usage of information. With antivirus and firewall systems, there is minimal security provided for the IoT networks from certain threats. More recently, possible data breaches and unauthorised access due to hackers breaking in through the network to manipulate the information require attention. Further, misuse of confidential information and difficulty to keep track of the users involved in the IoT transactions form the key motivation in considering blockchain technology to protect the organisation's computing assets from hackers and unauthorised users.

We model ID management system for the organisation as the business case scenario in developing a blockchain based proof-of-concept prototype. The main objectives in our proposed model are three-fold. Firstly, blockchain identity management is to be modelled to store the necessary information and key transactions of all IoT devices and computing assets in blocks which use strong cryptographic hashing to share the information securely within the system. The information stored in a block cannot be tampered since it allows a user to obtain the information from the blockchain through an automatic verification and matching of the hash that links one block to the next. Secondly, our model is designed to have provisions for business rules as smart contracts developed in a blockchain platform with various agreements required to be met while performing the core transactions on the IoT computing assets. Thirdly, our distributed trust model is to address security, privacy, and identity theft issues by managing identity verification of not only IoT assets but also authorised users of various digital assets and recovery of lost identities.

In our business case scenario, we focus the core transactions to protect the computing assets, such as computing hardware including IoT devices, the software running on them, the users operating these resources and the digital asset backup/update transactions. In our blockchain identity management model for such an IoT landscape, the identity attributes for hardware resources, software, users, and digital asset transactions stored in each block will be verified in order to control the disclosure of the attributes which depend upon the acceptability. Our model would enable the employees/authorised users to manage their identities to make use of the existing identity attributes [40]. In addition, a trusted

compliance platform using smart contract modelling would be created to incorporate the business rules for enforcing privacy, security, and trust. A smart contract consists of executable codes and memory from where it is invoked by blockchain identity (ID) management system providing the required trust. Smart contract platform would be secured using cryptographic code and the data or information stored on the blockchain which would be audited automatically [41]. Our blockchain model does not store the business events in the contract. Instead, based on temporal and other smart status changes, the block's data through the previously observed events will be updated. For this purpose, we develop reactive policies to trigger an event using smart contracts.

Figure 1 provides a pictorial representation of a high-level modelling of our proposed blockchain ID management system. In this model, the different IoT resource owners or users (employees) shown in Figure 1 represent authorised users who can transfer access control rights and management of identities by implementing smart contracts within the blockchain platform. In both permissioned as well as permissionless blockchain solutions, the identity of IoT/computing resources, digital assets and users can be stored and updated in the specific blocks of the blockchain and a strong cryptographic link (chain) connects one block to the next block securely. Thus, authenticated users have the right to update the ID information of an organisation's IoT assets stored in the blocks without compromising privacy. Users could self-generate identity attributes in a block and update them or endorse other users for transactions via a smart contract. With the rise of adopting blockchain technology for ID management to eradicate trust issues, the organisation would require modelling the business rules for the smart contract platform to handle the identity management process.

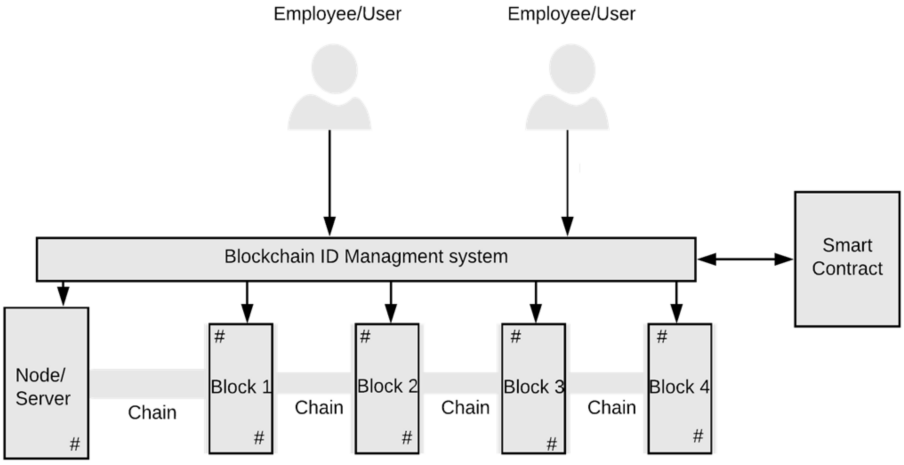

Figure 1. High-level modelling of proposed blockchain ID management system.

Figure 2 shows a typical representation of a unique ID denoted as "Computer ID" that represents each IoT resource and the related information stored in data blocks in a blockchain, with Block 1 acting as a Node (server). Information of each IoT added to the network will be stored subsequently as Block 2, Block 3, and so on as a chain via the encrypted unique hash that links the blocks securely. For example, the blocks in Figure 1 store the attributes of an IoT, such as computer ID, hardware type, ISP, VPN, resources, and contains the encrypted block hash.

In blockchain based ID management modelling, blocks use a cryptography link (Chain) to share the information securely within the system. The strong cryptography method of links every block as identified with a hash for allowing any authorised user to obtain the information from these blocks. It needs to verify the hash from the previous block so these blocks must have the same hash to give the information. Overall, public and private keypairs are used for generating this, which are correlated to the mined blockchain identity. Therefore, our proposed model prevents attacks from malicious third-party

identity providers and ensures user privacy and trust. Figure 3 provides an overview of how new blocks become added to the existing blockchain ledger when the transaction is verified by the network of blockchain nodes.

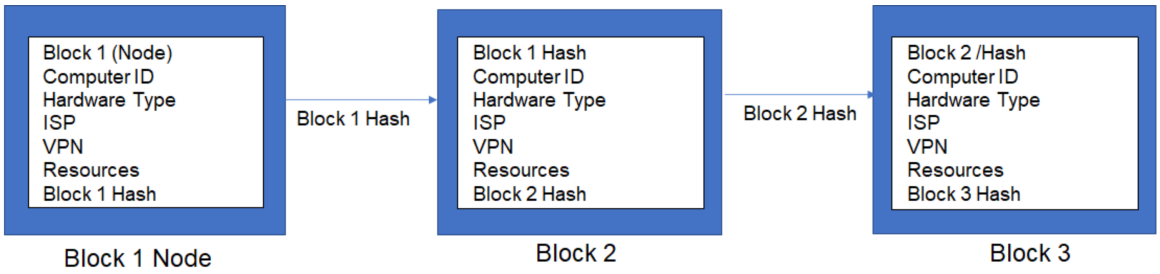

Figure 2. Modelling ID management of IoT resources using blockchain.

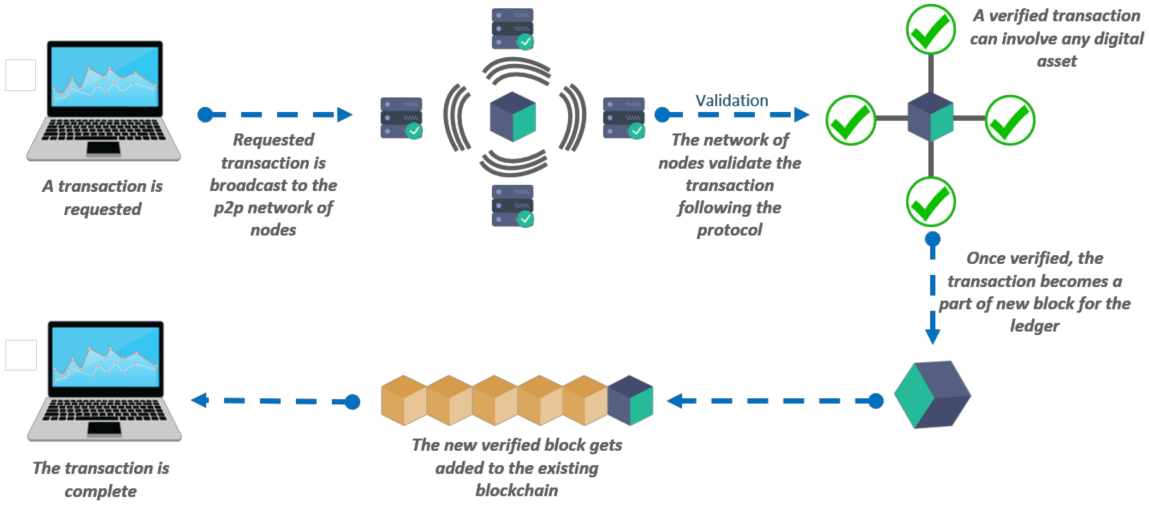

Figure 3. Overview of verified transactions in a blockchain.

Existing works have predominantly deployed smart contracts in a public blockchain that makes the contract state variables and transactions publicly available leading to anyone's access to all data related to the IoT. Rather than having a focus on the pros and cons of blockchain platforms, their constraints, performance comparisons, and other related issues, our proposed blockchain system modelling for IoT ID management aims at ensuring the integrity of data provenance records in the system using smart contracts. Data ownership is maintained by deploying smart contracts on a blockchain as tokens representing the digital asset of the organisation [42,43]. In the next section, we provide a proof-of-concept implementation of our proposed blockchain model coded in Solidity, a smart contract programming language and deployed in Kaleido, a blockchain platform as an enterprise system for the business case scenario.

4. System Implementation

In this section, we present a system implementation as a proof-of-concept prototype of our proposed blockchain-based IoT ID management for the business case scenario described in Section 3. With a growing number of IoT devices in the organisation's network, our blockchain ID management solution aims at identifying, authenticating, and authorising employees to have access to applications, systems, or networks by associating user rights and restrictions with established identities. ID verification costs corporations and governments billions of dollars annually and yet is prone to malicious attacks. Using open source blockchain platforms, such as Kaleido and Solidity, our model implementation provides a cost-effective and secure identity and authentication for the organisation's IoT

devices. Figure 4 shows the configuration of our ID management system for IoT resources in a blockchain platform called Kaleido.

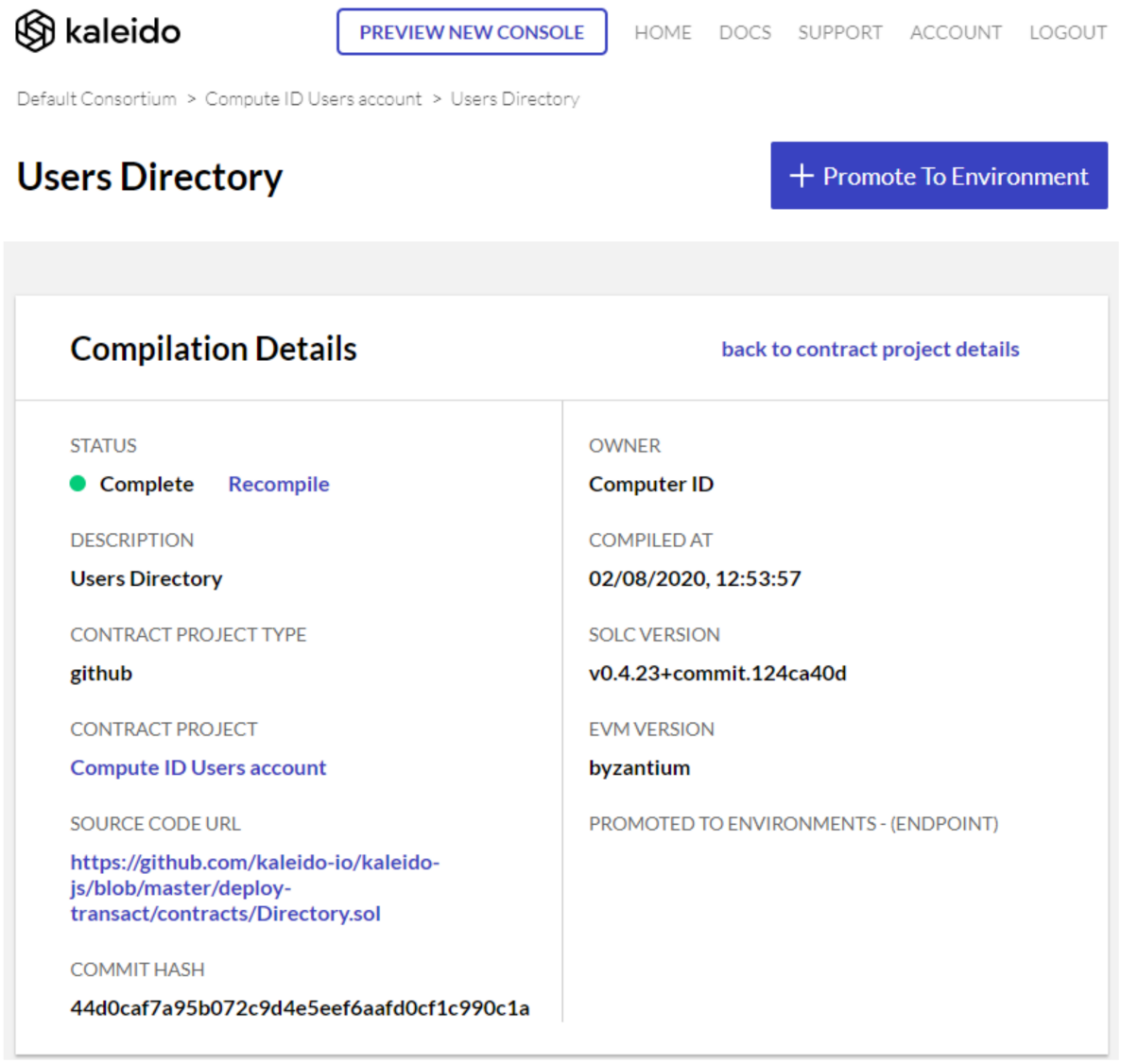

Figure 4. A configuration setup of ID management of IoT resources using blockchain platform.

The system involves blockchain-based implementation of ID management confining to four main categories of IoT related resources of the business case scenario as listed below:

1. Computer ID management which includes all the IoT devices;
2. Software ID management which includes various software resources associated with IoT;
3. User ID management which includes employees of the organisation assigned to the IoT resources;
4. Data backup ID management which includes digital operations, such as backup, recovery, and other transactions of the IoT resources.

Each ID management listed above is composed of attributes and smart contracts. Figure 5 lists the above four data models implemented and deployed in the blockchain environment. Figure 6 illustrates Computer ID block deployed in Kaleido blockchain platform.

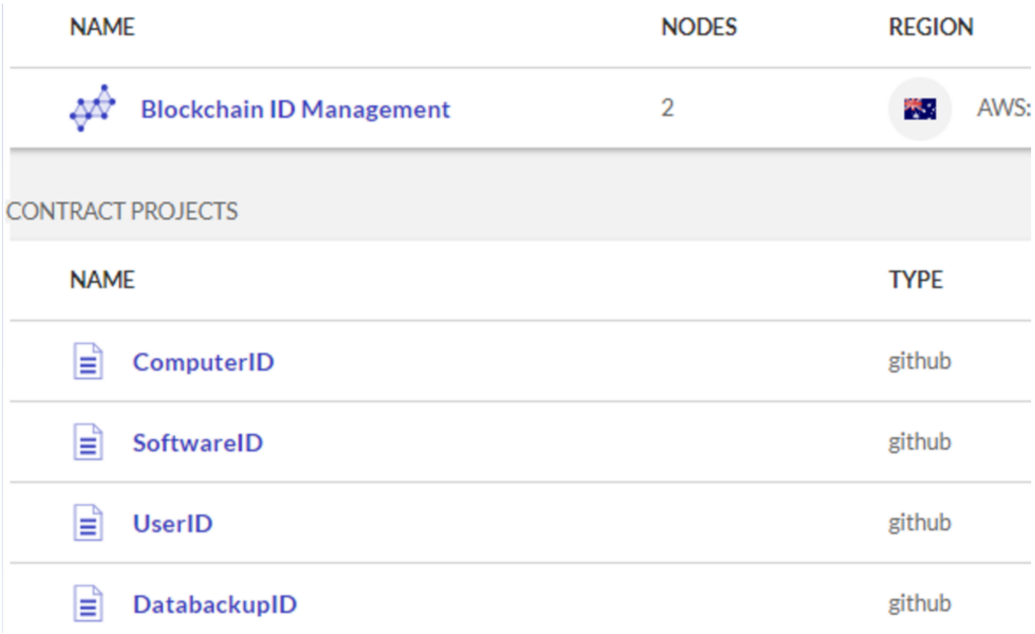

Figure 5. Data model of IoT ID management system deployed in a blockchain environment.

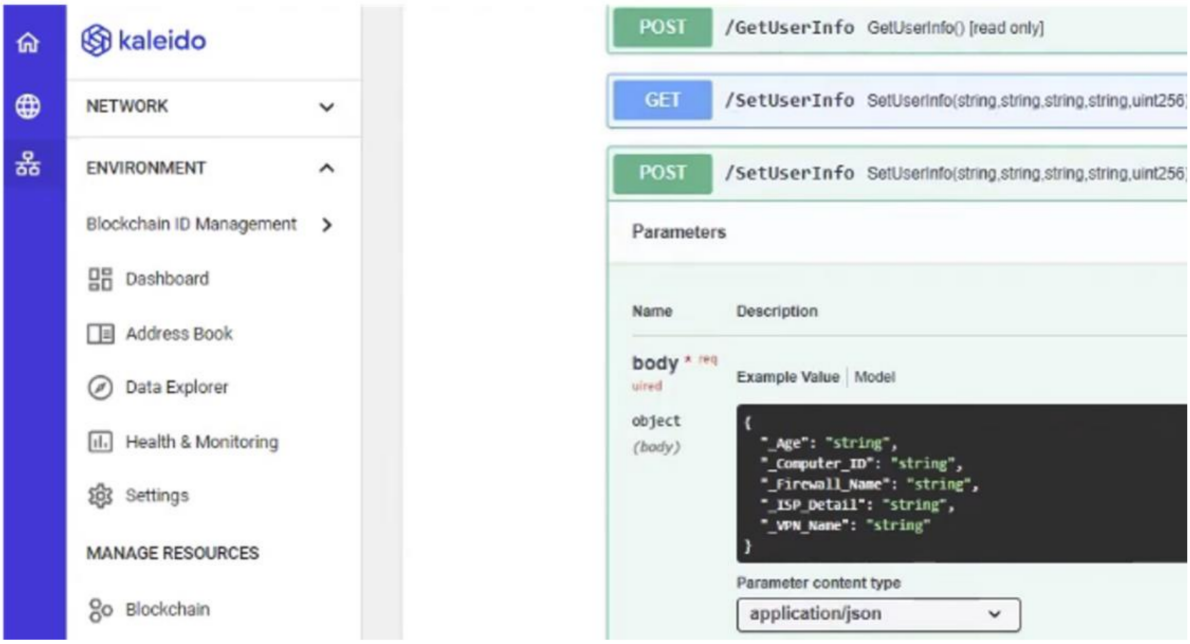

Figure 6. Computer ID block deployed in the Kaleido blockchain platform.

An authorised user can create a blockchain identity and update attributes as an individual user or a collective group of users according to the business rules implemented as smart contracts. Figure 7 shows the configuration of our system with four smart contract projects in the blockchain environment. Some of the smart contract rules for the above four categories of the IoT ID management system are listed below:

1. Computer ID management smart contracts. A smart contract rule could be used to authorise transactions, such as addition, update, or deletion of a Computer ID block in the blockchain. An example rule implemented makes checks before adding a new block into the blockchain when a new IoT device is procured in the organisation for an employee use. Another rule could be to check if the number of connections made

with computer IoT devices in the network does not exceed the threshold limit for optimum performance of the system.

2. Software ID management smart contracts. A typical smart contract could be associated with the software license of an IoT's software resource or a common software used in the organisation via the IoT network. An example smart contract rule implemented was an automatic notification to an authorised person to extend the license or to upgrade the software two weeks before expiry date. Another rule could enforce load balancing of software upgrades in a phased out manner to lessen the burden of software maintenance management.
3. User ID management smart contracts. It is a common practice to incorporate user login rules as a security measure for restricting unauthorised access when certain number of login attempts fail. An example smart contract rule implemented verifies if a user's login attempts fail with three attempts, when user access will be denied. The implementation of this smart contract using Solidity programming language and within the blockchain environment is illustrated in Figure 8. In such instances, the user is denied access to the MAC address of the organisation's network or make any further transactions with the system. However, smart contracts could also be implemented for an authorised person's user ID to be reinstated with a new password for resolving the denial of access issue for any legitimate user of the organisation.
4. Data backup ID management smart contracts. When a user attempts to back-up a data storage or makes an update to the data records, a smart contract could allow such transactions only if there is no data breach. Further, for any data breach occurring, a smart contract could be created for assisting the user to quarantine the data from future user transactions with the organisation's data records. An example smart contract implemented was to optimise the backup storage by checking based on the timestamp of previous backup and to archive only those data records that were updated after the previous backup. Figure 9 shows the code of a data backup rule implemented in Solidity as a smart contract that was successfully deployed in Kaleido blockchain environment. Further, a smart contract could be allowing for data retrieval from the backup storage to be possible with two security questions that need to be answered correctly.

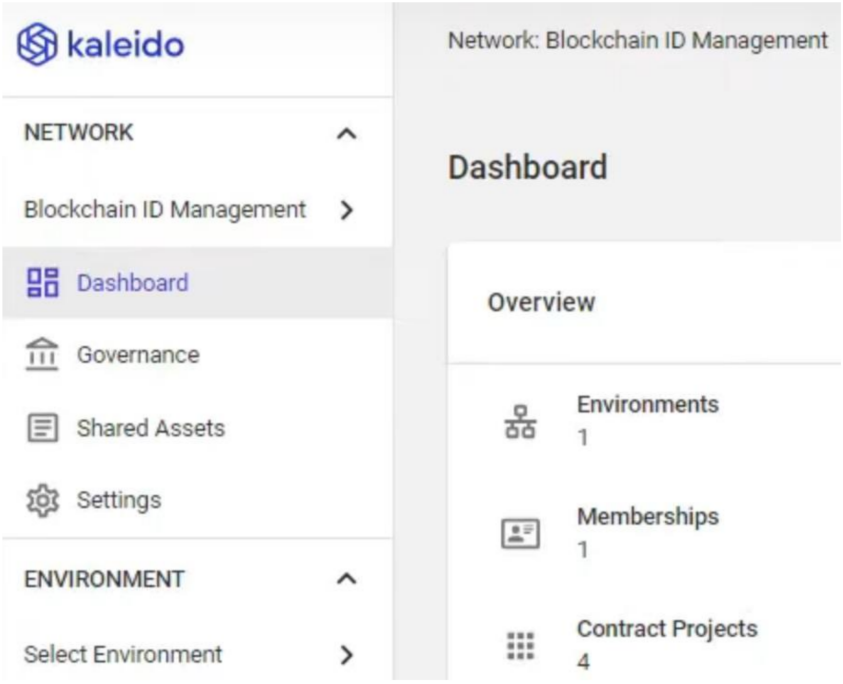

Figure 7. Configuration of smart contracts for ID management in a Blockchain environment.

```
pragma solidity ^0.5.0;

contract   UserID{

    uint Employee_ID;
    string Name;
    string HomeAddress;
    uint LoggingAttemps;
    bool Authorized_Person;
     bool LessThan3Attemps;

    function SetUserInfo(uint _Employee_ID, string memory _Name, string
          memory _HomeAddress) public {
        Employee_ID = _Employee_ID;
        Name = _Name;
        HomeAddress = _HomeAddress;

    //Authorized_Person
      if (Employee_ID >= 80){Authorized_Person = false;
    }
          else Authorized_Person = true;
     }

    //Logging attemps
    function LogAttemps (uint _LoggingAttemps) public {
        LoggingAttemps = _LoggingAttemps;

     if (LoggingAttemps >= 3) {LessThan3Attemps = false;
     }
     else (LessThan3Attemps = true);
    }
    //Getting all the data
    function GetUserInfo() public view returns (uint, string memory, string
          memory, uint, bool, bool) {
   return (Employee_ID, Name, HomeAddress, LoggingAttemps, Authorized_Per-
          son, LessThan3Attemps);
    }
}
```

Figure 8. Example implementation of a User ID smart contract in blockchain platform using Solidity.

```
Home  ComputerID.sol  UserID.sol  DataBackupID.sol  SoftwareID.sol
1  pragma solidity ^0.5.0;
2
3  contract  DataBackupID{
4
5     uint twostepInput;
6     bool twoStepVer;
7     uint Date;
8     string Data_size;
9     string Backup_length_time;
10    bool SoftwareNeedstobeUpdated;
11
12
13
14
15    function SetUserInfo ( uint _Date, string memory _Data_size,string memory _Backup_length_time) public {
16        Date = _Date;
17        Data_size = _Data_size;
18        Backup_length_time = _Backup_length_time;
19       // 1= 1 Month - 2 = 2 month   (months lesft before backup expires)
20        if (Date >= 6 ){SoftwareNeedstobeUpdated = false;
21           }
22           else SoftwareNeedstobeUpdated = true;
23     }
24     // Two stepverification / less than if token returns less than 2= authentication is satisfied, else NOT
25     function twoStepVerif ( uint _twostepInput) public {
26     twostepInput = _twostepInput;
27
28     if (twostepInput >=2 ) {twoStepVer = false;
29
30     }
31     else (twoStepVer = true);
32
33
34    }
35
36    function GetUserInfo() public view returns (uint, string memory,string memory, bool, bool) {
37 return (Date, Data_size, Backup_length_time, SoftwareNeedstobeUpdated, twoStepVer);
38    }
39
40 }
```

Figure 9. Example implementation of a User ID smart contract in blockchain platform using Solidity.

Overall, our blockchain based ID management system for IoT resources for an organisation was implemented as a proof-of-concept prototype. The purpose was to address some of the critical challenges of privacy and security of traditional ID management system based on relational database modelling. Even though blockchain-based ID management solutions are emerging, developing an effective ID management for IoT remains a challenge in terms of managing access controls, privacy, and trusted transactions. Our blockchain based shared and distributed ledger stores the identity information of IoT resources and transactions that are verified through smart contracts to establish the required data provenance. Further, the latest transactions mined could be monitored in the blockchain platform, as shown in Figure 10. This helps to verify the status of each transaction, when mined and from which block with a commit hash that maintains the required security using blockchain encryption of the system. Hence, the system implementation of our proposed blockchain modelling of ID management of digital assets could provide a solution to the existing issues of identity theft, information leakages, and other malicious practices over the organisation's networked IoT resources.

Latest Transactions

Transaction	From	Status	Date Mined
0xcbcc...74cf33	Melbo... | bdc01f	✓ Success	2 days ago
0xa2c9...e79f48	Melbo... | bdc01f	✓ Success	a month ago
0xb013...926501	Melbo... | bdc01f	✓ Success	a month ago
0xc954...b41a4b	Melbo... | bdc01f	✓ Success	a month ago
0xa885...14fc03	Melbo... | bdc01f	✓ Success	a month ago

Figure 10. Transaction monitoring in the implemented blockchain system.

This paper reports the successful completion of a pilot research work with limited scope as mentioned above. Our blockchain based proof-of-concept prototype for a business case scenario was tested and is suitable to be deployed on any EVM-compatible blockchain

platform. Although some recent works [31,44] have developed a proof-of-concept implementation of smart contract in public permissionless blockchains, such as Ethereum and Ethereum Classic, the focus in this research work was towards developing ID management for IoT ecosystem in a business case scenario. The described model and system implementation could be deployed on any blockchain platform that supports scripting capabilities and other open-source software including Github. Figure 11 shows the CPU utilisation that was quite reasonable performance of the proof-of-concept prototype deployment in Kaleido blockchain platform. The blockchain platform can be integrated with AWS CloudWatch to monitor the performance of the running system. Figures 10 and 11 give examples of such performance metrics, such as transaction monitoring and CPU time. In addition, monitoring log activities and other actionable system-wide insights could provide a unified view of the system's operational health. Further, Kaleido provides a seamless integration with AWS CloudWatch to visualise several key performance metrics that would help businesses to optimise resource utilisation quickly and aid in prompt and accurate diagnostics to resolve any problem that may occur. A recent study considered several performance metrics for measuring the performance of blockchain platforms using measures, such as latency, throughput, computation, storage, and communication costs, scalability, and other security and privacy comparison factors [45].

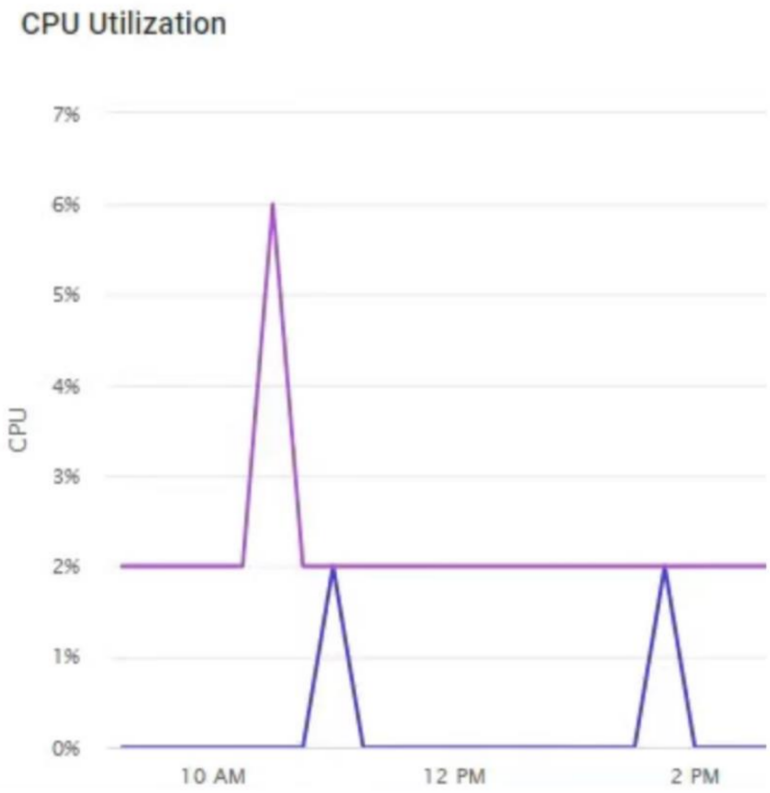

Figure 11. CPU utilisation of the prototype deployment of the proposed blockchain system.

Studying the scalability of the blockchain based real-time communication in real-life business environments is becoming important [46]. Scalability, adaptability, and other blockchain based business use case development would be the focus of future research work. In this context, business oriented blockchain-based platforms, such as Hyperledger supported by leading companies is a noteworthy avenue for further investigation [42]. Our future study would consider evaluating the use of our business blockchain approach as a Hyperledger solution comparing the performance of different consensus algorithms. Some existing studies have investigated Hyperledger's scalability and performance with an ambitious achievement of thousands of transactions per second [32,33,47]. However,

such studies are yet to deploy and evaluate scalability and performance issues in any blockchain platform with several related smart contracts added in real-life business scenarios. Recent studies have focused on proposing blockchain frameworks for specific business applications, such as supply chains in the distribution industry and forensics in vehicle management contexts [41,48]. Business process oriented blockchain development is gaining importance [49,50]. Intelligent automation of business processes using smart contracts is yet to explored. Our motivation towards another future research direction would be to consider automating an Agile process of developing and maintaining smart contracts from business and security policies and applying their updates dynamically whenever there are changes happening from time to time. The future of the IoT ecosystem sees blockchain as an enabling technology in a distributed cyber physical system to achieve the required privacy, trust, and data provenance targets for businesses [51–53]. Some such studies have considered comparison measures of power consumption, latency, and throughput of transactions in a blockchain tree, including concepts of sidechains and parallel data provenance, including the impact of trust and consensus algorithms [54,55]. A performance analysis of the running system in a real-life business would consider specific metrics for a deeper insight into the context to aid in a quicker evaluation and diagnosis of any problem. Although this work does not duplicate existing works, the discussions highlighted in this paper opens up many research directions for future investigations.

5. Conclusions and Future Work

In this paper, we have presented a proof-of-concept prototype in developing a blockchain based IoT ID management system. We provided the data modelling for the ID management of IoT resources in an organisation as a business case scenario. The implementation of the system in a blockchain platform demonstrated the practical viability of the system. In addition, the four different identities related to IoT resources, such as Computer (Device) ID, Software ID, User ID, and Data Backup ID in a blockchain along with customised smart contracts have established the required information security, privacy, and trust in a networked organisation.

This research is limited to establishing a design model and development of IoT ID management using blockchain technology for a business case scenario. There is a need to study the extendibility and adaptability for large scale business operations. Future work would explore the scalability issue, which is one of the key limitations of blockchain technology. With the non-availability of any existing work related to our business scenario, our restricted scope of this research with a proof-of-concept prototype development would be expanded in the next phase of our ongoing research. Future work will also explore the performance and computation time of blockchain transactions and running time for the proposed method in real-life business environments and compared with other possible emerging works. Several performance metrics would be considered to compare, evaluate and benchmark the running our system.

Author Contributions: Conceptualisation, S.V.; resources, S.V. and S.P.; writing—original draft preparation, S.V.; writing—review and editing, S.V. and S.P.; supervision, S.V. and S.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

Acknowledgments: This work contains processed information from opensource software components provided by Github and Kaleido for which the authors wish to thank towards supporting this ongoing research work. The authors also thank Aldo Cecilio for associating with the implementation for a business case scenario. The authors also wish to acknowledge the reviewers and editors for their invaluable inputs and support rendered for this paper.

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

References

1. Carnley, P.R.; Kettani, H. Identity and Access Management for the Internet of Things. *Int. J. Future Comput. Commun.* **2019**, *8*, 129–133. [CrossRef]
2. Tian, Q.; Lin, Y.; Guo, X.; Wang, J.; Alfarraj, O.; Tolba, A. An Identity Authentication Method of a MIoT Device Based on Radio Frequency (RF) Fingerprint Technology. *Sensors* **2020**, *20*, 1213. [CrossRef] [PubMed]
3. Aleisa, M.A.; Abuhussein, A.; Sheldon, F.T. Access Control in Fog Computing: Challenges and Research Agenda. *IEEE Access* **2020**, *8*, 83986–83999. [CrossRef]
4. Butun, I.; Osterberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 616–644. [CrossRef]
5. Sousa, P.R.; Resende, J.S.; Martins, R.; Antunes, L. The case for blockchain in IoT identity management. *J. Enterp. Inf. Manag.* **2020**. [CrossRef]
6. Mamdouh, M.; Awad, A.I.; Khalaf, A.A.; Hamed, H.F. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. *Comput. Secur.* **2021**, *111*, 102491. [CrossRef]
7. Tan, H.; Chung, I. Secure Authentication and Key Management With Blockchain in VANETs. *IEEE Access* **2019**, *8*, 2482–2498. [CrossRef]
8. Tsai, W.Y.; Chou, T.C.; Chen, J.L.; Ma, Y.W.; Huang, C.J. Blockchain as a platform for secure cloud computing services. In Proceedings of the 2020 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea, 16–19 February 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 155–158. [CrossRef]
9. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2018**, *36*, 55–81. [CrossRef]
10. Brody, P.; Pureswaran, V. Device Democracy: Saving the Future of the Internet of Things. IBM. 2014. Available online: https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/globalbusi-ness-services-global-business-services-gb-executive-briefgbe03620usen-2017.pdf (accessed on 17 January 2021).
11. Daza, V.; Di Pietro, R.; Klimek, I.; Signorini, M. CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1986–1991. [CrossRef]
12. Wang, X.; Zha, X.; Yu, G.; Ni, W.; Liu, R.P. Blockchain for Internet of Things. In *Book Chapter in Blockchains for Network Security: Principles, Technologies and Applications*; IET: London, UK, 2020; pp. 87–136. [CrossRef]
13. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630. [CrossRef]
14. Neisse, R.; Steri, G.; Nai-Fovino, I. A Blockchain-based Approach for Data Accountability and Provenance Tracking. *arXiv* **2017**, arXiv:170604507.
15. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. In *Europe and MENA Cooperation Advances in Information and Communication Technologies*; Springer: Cham, Switzerland, 2016; pp. 523–533. [CrossRef]
16. Ouaddah, A.; Abou Elkalam, A.; Ait Ouahman, A. FairAccess: A New Blockchain-based access control framework for the In-ternet of Things. *Secur. Commun. Netw.* **2016**, *9*, 5943–5964. [CrossRef]
17. Ning, H.; Ye, X.; Ben Sada, A.; Mao, L.; Daneshmand, M. An Attention Mechanism Inspired Selective Sensing Framework for Physical-Cyber Mapping in Internet of Things. *IEEE Int. Things J.* **2019**, *6*, 9531–9544. [CrossRef]
18. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and per-mission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
19. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med. Syst.* **2018**, *42*, 1–7. [CrossRef] [PubMed]
20. Faber, B.; Michelet, G.C.; Weidmann, N.; Mukkamala, R.R.; Vatrapu, R. BPDIMS: A blockchain-based personal data and identity management system. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA, 8–11 January 2019.
21. Lin, C.; He, D.; Huang, X.; Khan, M.K.; Choo, K.-K.R. A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems. *IEEE Access* **2018**, *6*, 28203–28212. [CrossRef]
22. Ren, Y.; Zhu, F.; Qi, J.; Wang, J.; Sangaiah, A.K. Identity Management and Access Control Based on Blockchain under Edge Computing for the Industrial Internet of Things. *Appl. Sci.* **2019**, *9*, 2058. [CrossRef]
23. Nyante, K. Secure Identity Management on the Blockchain. Master's Thesis, University of Twente, Enschede, The Netherlands, 2018. Available online: https://essay.utwente.nl/ (accessed on 20 February 2021).
24. Alsayed, K.J.; Sayeed, S.; Marco-Gisbert, H.; Pervez, Z.; Dahal, K. DNS-IDM: A blockchain identity management system to secure personal data sharing in a network. *Appl. Sci.* **2019**, *9*, 2953. [CrossRef]
25. Mell, P.; Dray, J.; Shook, J. Smart contract federated identity management without third party authentication services. *arXiv* **2022**, arXiv:1906.11057.

26. Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Raymond Choo, K.-K. Block-chain-based identity management systems: A review. *J. Netw. Comput. Appl.* **2020**, *166*, 102731. [CrossRef]
27. Kuperberg, M. Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1008–1027. [CrossRef]
28. Ishmaev, G. Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethic Inf. Technol.* **2020**, *23*, 239–252. [CrossRef]
29. Yu, B.; Wright, J.; Nepal, S.; Zhu, L.; Liu, J.; Ranjan, R. IoTChain: Establishing Trust in the Internet of Things Ecosystem Using Blockchain. *IEEE Cloud Comput.* **2018**, *5*, 12–23. [CrossRef]
30. Bouras, M.A.; Lu, Q.; Dhelim, S.; Ning, H. A Lightweight Blockchain-Based IoT Identity Management Approach. *Future Internet* **2021**, *13*, 24. [CrossRef]
31. Khalil, A.A.; Franco, J.; Parvez, I.; Uluagac, S.; Rahman, M. A Literature Review on Blockchain-enabled Security and Op-eration of Cyber-Physical Systems. *arXiv* **2021**, arXiv:2107.07916.
32. Vukolić, M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In *Lecture Notes in Computer Science*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2016; pp. 112–125.
33. Kong, M.; Zhao, J.; Sun, X.; Nie, Y. Secure and efficient computing resource management in blockchain-based vehicular fog computing. *China Commun.* **2021**, *18*, 115–125. [CrossRef]
34. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. *IEEE Access* **2018**, *6*, 13565–13574. [CrossRef]
35. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, A.; Di, J.; Li, Q.; Lee, Y. An overview of cyber-physical security of battery manage-ment systems and adoption of blockchain technology. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *10*, 1270–1281. [CrossRef]
36. Cole, R.; Stevenson, M.; Aitken, J. Blockchain technology: Implications for operations and supply chain management. *Supply Chain Manag. Int. J.* **2019**, *24*, 469–483. [CrossRef]
37. Ølnes, S.; Jansen, A. Blockchain technology as a support infrastructure in e-government. In *International Conference on Electronic Government*; Springer: Cham, Switzerland, 2017; pp. 215–227.
38. Lim, S.Y.; Fotsing, P.T.; Almasri, A.; Musa, O.; Kiah, M.L.M.; Ang, T.F.; Ismail, R. Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 1735. [CrossRef]
39. Zehir, S.; Zehir, M. Internet of Things in Blockchain Ecosystem from Organizational and Business Management Perspectives. In *Digital Business Strategies in Blockchain Ecosystems*; Springer: Cham, Switzerland, 2020; pp. 47–62.
40. Gao, Z.; Xu, L.; Turner, G.; Patel, B.; Diallo, N.; Chen, L.; Shi, W. Blockchain-based identity management with mobile de-vice. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 15 June 2018; pp. 66–70.
41. Wu, H.; Li, Z.; King, B.; Ben Miled, Z.; Wassick, J.; Tazelaar, J. A Distributed Ledger for Supply Chain Physical Distribution Visibility. *Information* **2017**, *8*, 137. [CrossRef]
42. Cooper, K. Hyperledger Burrow. 2020. Available online: https://wiki.hyperledger.org/display/burrow/Burrow+-+The+Boring+Blockchain$\backslash$ (accessed on 8 June 2021).
43. Cryptographic Tokens. 2019. Available online: https://blockchainhub.net/tokens/ (accessed on 16 November 2021).
44. Wang, D.; Zhao, N.; Song, B.; Lin, P.; Yu, F.R. Resource Management for Secure Computation Offloading in Softwarized Cyber–Physical Systems. *IEEE Internet of Things J.* **2021**, *8*, 9294–9304. [CrossRef]
45. Ferrag, M.A.; Shu, L. The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial. *IEEE Int. Things J.* **2021**, *8*, 17236–17260. [CrossRef]
46. Qiu, H.; Qiu, M.; Memmi, G.; Ming, Z.; Liu, M. A Dynamic Scalable Blockchain Based Communication Architecture for IoT. In *International Conference on Smart Blockchain*; Springer: Cham, Switzerland, 2018; pp. 159–166. [CrossRef]
47. Vukolić, M. Rethinking Permissioned Blockchains. In *ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC'17)*; Association for Computing Machinery: New York, NY, USA, 2017; Available online: http://vukolic.com/rethinking-permissioned-blockchains-BCC2017.pdf (accessed on 25 June 2021).
48. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57. [CrossRef]
49. Prybila, C.; Schulte, S.; Hochreiner, C.; Weber, I. Runtime verification for business processes utilizing the Bitcoin blockchain. *Future Gener. Comput. Syst.* **2017**, *107*, 816–831. [CrossRef]
50. Mendling, J.; Weber, I.; Van Der Aalst, W.; Brocke, J.V.; Cabanillas, C.; Daniel, F.; Debois, S.; Di Ciccio, C.; Dumas, M.; Dustdar, S.; et al. Blockchains for Business Process Management—Challenges and Opportunities. *ACM Trans. Manag. Inf. Syst.* **2018**, *9*, 1–16. [CrossRef]
51. Isaja, M.; Cal, A. Blockchain as a Key Enabling Technology for Decentralized Cyber-Physical Production Systems. 2020. Available online: https://www.edge4industry.eu/wp-content/uploads/2018/11/Blockchain-as-a-Key-Enabling-Technology-for-Decentralized-CPPS.pdf (accessed on 28 January 2022).
52. Sigwart, M.; Borkowski, M.; Peise, M.; Schulte, S.; Tai, S. A secure and extensible blockchain-based data provenance framework for the Internet of Things. *Pers. Ubiquitous Comput.* **2020**, 1–15. [CrossRef]
53. Misra, S.; Mukherjee, A.; Roy, A.; Saurabh, N.; Rahulamathavan, Y.; Rajarajan, M. Blockchain at the Edge: Performance of Resource-Constrained IoT Networks. *IEEE Trans. Parallel Distrib. Syst.* **2020**, *32*, 174–183. [CrossRef]

54. Cao, B.; Zhang, Z.; Feng, D.; Zhang, S.; Zhang, L.; Peng, M.; Li, Y. Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digit. Commun. Netw.* **2020**, *6*, 480–485. [CrossRef]
55. Al-Rakhami, M.; Al-Mashari, M. A Blockchain-Based Trust Model for the Internet of Things Supply Chain Management. *Sensors* **2021**, *21*, 1759. [CrossRef]