The Case for Blockchain in IoT Identity Management

Patrícia R. Sousa*, João S. Resende*, Rolando Martins*, Luís Antunes*
*DCC-FCUP/CRACS-INESC TEC
{patricia.sousa, jresende, rmartins, lfa}@fc.up.com

Abstract

Purpose - The aim of this paper is to evaluate the use of Blockchain for Identity Management (IdM) in the context of the Internet of Things (IoT) while focusing on privacy-preserving approaches, and its applications to healthcare scenarios.

Design/methodology/approach - The paper describes the most relevant IdM systems focusing on privacy-preserving with or without Blockchain and evaluates them against 10 selected features grouped into three categories: privacy, usability and IoT. Then, it is important to analyse whether Blockchain should be used in all scenarios, according to the importance of each feature for different use cases.

Findings - Based on analysis of existing systems, *Sovrin* is the IdM system that covers more features and is based on Blockchain. For each of the evaluated use cases, *Sovrin* and *UniquID* were the chosen systems.

Research implications - This paper opens new lines of research for IdM systems in IoT, including challenges related to device identity definition, privacy-preserving, and new security mechanisms.

Originality/value - This paper contributes to the ongoing research in IdM systems for IoT. The adequacy of Blockchain is not only analyzed considering the technology; instead we analyse its application to real environments considering the required features for each use case.

Keywords - Identity Management, Privacy-preserving, Security, Blockchain, Internet of Things, Healthcare

Paper type - Research paper

I. Introduction

IoT is a technological concept where devices from our daily lives, such as watches, appliances or even clothes, are connected to/through the Internet. We envision an increase of efficiency when we interconnect these devices. Anecdotally, a fridge can warn its owner when the food is close to the due date and can search the web which markets are offering the best prices for this item. Another possible example is a thermostat that can adjust the temperature according to environmental conditions. In addition, it is important that devices can communicate whenever appropriate. A thermostat, for example, can send information to the owner's smartphone to show how the air conditioner is being used or to apply custom settings.

The rapid adoption of these Internet-connected devices is raising concerns regarding their ability to pry. This is agonized by the relative ease to compromised them due to their lacking security robustness. There are several scenarios of IoT applications that can be grouped into multiple domains, namely Transportation and Logistics, Healthcare, Smart Environment, and Personal/Social domain (Atzori et al., 2010). The health domain is one of the most motivational application field because patients expect certain private information to remain confidential, but there is a lack of adequate mechanisms to ensure the privacy of personal and/or confidential information (Miorandi et al., 2012). In terms of security, if these types of systems are hacked or fail, it can lead to catastrophic consequences (Laplante & Laplante, 2016). For example, if a home security system is compromised or disabled, the security of the entire house is compromised as well. Another example is the traffic in a smart city, where an attack or system failure can cause traffic signal changes and lead to "chaos" in minutes.

Past works discuss different challenges in IoT, including security and privacy issues. Lack of privacy protection mechanisms mainly refers to weak authentication and confidentiality (Frustaci et al., 2017), and this leads to problems related to the privacy of user data. It is important to improve data transparency for users and detection of potential attacks (Khan & Salah, 2018). Also, there are other challenges related to resource limitations, heterogeneous devices, interoperability of security protocols, single points of failure, hardware/firmware vulnerabilities and reliable management and updates (Aksu et al., 2018).

There is a set of IoT security requirements that must be integrated by design, such as user and device IdM, service availability, data integrity and confidentiality, and network access control to ensure only authorized devices (Babar et al., 2010).

Traditional human-centered IdM systems cannot be directly integrated with IoT environments (Trnka & Cerny, 2016). Humans are distinguished by their physical characteristics, nationality and personality, just to name a few, and have an identification document that is used to prove their identity. In addition to an identification document, which has personal information (name, nationality or birth date), there are also other characteristics that define the identity of a person, such as preferences (food, clothes, books) or reputation among the community (honest or reliable) (El Maliki & Seigneur, 2007). Digital identity is equivalent to the physical identity of a person or entity, when used for identification and transactions over the Internet. However, there are services and applications that do not require all the information associated with an user. E-Bay, for example, only needs to know

if the seller's reputation is good and that the seller can prove that controls his digital identity (El Maliki & Seigneur, 2007). In this case, attributes like date of birth, gender, address or nationality are not required (less important). Once the link between the personal entities and their online interactions is established, the use of a digital identity involves authentication. Subsequently, human authentication methods can be classified into three categories (Brainard et al., 2006): *Something you have*, *Something you know* and *Something you are*.

However, for devices it is required to define a digital identity. Therefore, mechanisms for device identification and authentication, as well as relevant forms of authorization, are required to address privacy and security issues in IoT. With a unique and strong identity, sensors and/or devices can be authenticated online, promoting safer communication between devices, services and users, thus proving their integrity.

Theft, tampering and disguise are some of the issues that challenge IoT identity protection. In addition, there is a lack of clear definitions of how sensors or devices are identified, represented, searched and accessed in IoT. This gap makes IoT vulnerable to multiple identity attacks, such as a Sybil attack, which occurs when a sensor or device illegally uses multiple identities. Thus, several traditional security solutions need to be reviewed to determine their feasibility and applicability in IoT.

Blockchain technology has the potential to meet the aforementioned challenges because of its distributed, private and secure nature (Dorri, Kanhere, Jurdak, & Gauravaram, 2017a). Several works (Banerjee et al., 2018; Jesus et al., 2018; Walker et al., 2017) claim that the integration between Blockchain and IoT should exist to achieve safer and more efficient systems. As such, Blockchain technology can provide a way around centralization issues by providing a secure solution without the need for a trusted central authority.

This paper focuses on exploring the use of Blockchain for IdM in IoT and its application to healthcare scenarios. We want to evaluate the feasibility of Blockchain-based solutions being integrated with IoT, particularly in healthcare scenarios, as it is one of the largest application scenarios where privacy issues need to be addressed. To analyze these solutions, we have defined a set of required features to build an IdM system for IoT that guarantees privacy-preserving.

In brief, this paper attempts to explore the following research questions:

RQ1: What are the requirements to build a privacy-preserving IdM system for IoT?
RQ2: Can Blockchain be used to meet these requirements?
RQ3: Can Blockchain-based IdM systems be applied to healthcare scenarios?

The paper is divided into the following sections: Section 1 is the introduction, Section 2 discusses related work, Section 3 describes traditional IdM systems, Section 4 introduces the concept of Identity of Things, Section 5 attempts to explore ongoing research on privacy-preserving IdM for IoT, Section 6 describes the Blockchain concept and explores the integration between Blockchain and IoT, as well as a systematic review of Blockchain-based IdM systems, Section 7 presents the comparative table and methodologies for system and feature selection, Section 8 shows the findings according to the healthcare scenarios, Section 9 opens new directions for further research, and finally, Section 10 presents the conclusions.

II. Related Work

Traditional IdM systems have already been compared to privacy-focused IdM systems (Bernabé et al., 2017), however, our work focuses also on examine whether using Blockchain can help satisfying security and privacy, IoT and usability issues. As such, we analyse Blockchain systems and their practical application in healthcare scenarios.

From the point of view of a set of native IoT features, such as scalability, interoperability, mobility, security and privacy, past work (Zhu & Badr, 2018) analyzed traditional IdM systems and investigate recent surging blockchain sovereign identity solutions, to pin-point challenges in building IdM systems for IoT. Privacy is still a challenge for Blockchain and IoT, and they argue that multiparty computation and zero knowledge proofs could bring the selective disclosure and perfect online identity privacy into reality, because nowadays, public Blockchain can still expose identity information. Therefore, integrating Blockchain with IoT is still an open challenge.

Current research aims to find new solutions to IdM problems by using and optimizing Blockchain to work on practical use cases, such as a manufacturing company (Nuss et al., 2018). Blockchain is surging as a possible solution to solve the problem of data exchange and trading or to streamline the negotiation processes, eliminating the need for reliable intermediaries. However, also has scalability issues, for example (Panarello et al., 2018). Regarding IdM, the same authors also analyse IdM systems grouped into two categories: Blockchain and Blockchain-Based Public Key Infrastructure (PKI), which may be interesting for the overview of centralized and decentralized solutions.

III. Traditional IdM

IdM can be understood as a set of processes and technologies used to protect the identity of an entity (user or device), ensure the quality of identity information (identifiers, credentials and attributes) and provide authentication and access privileges to information systems within the limits defined by an organization. An entity can have multiple identities and each identity can

have different attributes; each attribute can be unique or non-unique. We call this section ”Traditional IdM” as it is not focused on IoT.

The IdM concept is already deployed in services, such as: Active Directory Management; Service Providers; Identity Providers; Web Services; Access Control; Digital Identities; Password Management; Single-Sign On (SSO); Security Tokens; Security (STS); OpenID; WS-Security; WS-Trust; SAML 2.0; OAuth and Role-Based Access Control (RBAC).

An IdM system consists of a three-tier architecture: User or Device, Identity Provider (IdP) and Service Provider (SP) (Angin et al., 2010; Cao & Yang, 2010; El Maliki & Seigneur, 2007).

One of the most common ways to manage authentication and authorization of individuals and devices is by using *Federated IdM* (Chadwick, 2009). *OAuth 2.0* and *OpenID Connect 1.0* are two standardized authentication and authorization frameworks used by most services. The *OAuth 2.0* framework is intended to delegate conditional authorization, that is, resource owners authorize temporary access to a predetermined set of resources without revealing their credentials. Access tokens are provided to third-party clients by an authorization server with the resource owner's approval. Clients then use their access tokens to access protected resources hosted on the resource server. Basically, this service is commonly used by users to access third party websites using their Facebook, Google and Twitter accounts, without exposing their credentials (Hardt, 2012).

OpenID Connect adds an identity layer to the *OAuth 2.0* (Sakimura et al., 2014). The protocol provides two notable identity constructs to *OAuth* token issuance mode (“Paul Madsen. (2015) ”Standardized Identity Protocols and the Internet of Things””, n.d.):

- A client can retrieve the desired identity attributes for a given user;
- Obtaining an identity token delivered from one party to another. This can enable a federated SSO experience for a user.

Security Assertion Markup Language (SAML) is an XML-based standard developed by the OASIS Security Services Technical Committee for the purpose of exchanging authentication and authorization data between security domains. It can be used to support Identity Federation and carry out identity propagation within a company or between companies. *SAML* is currently being adopted as a vehicle for propagating identity information through Service Oriented Architecture (“Security Assertion Markup Language (SAML) V2.0 Technical Overview. Working Draft 10, 9 October 2006.” 2006).

WS-Security specifies how to apply encryption to *SOAP* messages, ensuring that information is transported in a secure manner to guarantee confidentiality and integrity. The form of security applied here depends on the authentication format used between the subject and the identity provider. As interoperability is one of the most important aspects, *WS-Security* encrypts messages through token profiles, which describe how to map the authentication technologies that currently exists (Kerberos, UserNames, certificates, etc.) to a generic model.

WS-Trust defines a trust model with operations to acquire, issue, renew, and validate security tokens and ways to create new trust relationships through an intermediary service (“Web Services Trust Language (WS-Trust)”, Microsoft, IBM, OpenNetwork, Layer 7, Computer Associates, VeriSign, BEA, Oblix, Reactivity, RSA Security, Ping Identity, VeriSign, Actional”, 2005).

WS-Federation organizes *WS-Trust* and *WS-Security* standards into a top-level language and defines service federations to share identity, attributes, authentication, and authorization information across different trusted domains (“Web Services Federation Language (WS-Federation) Version 1.0, OASIS”, 2003).

There are some research papers with framework ideas to solve identity problems. Chibelushi et al., 2013 propose a healthcare IdM framework built into Mobile Ad-hoc Network (MANET), assuming the devices are connected wirelessly and allowing users and devices to be distinguished based on personal identifiers and device profiles, respectively. The framework also considers bandwidth limitations, ensuring that the minimum amount of information is exchanged at one time. A sandboxing [1] technique is employed to protect user content when sharing a device. Most IdM systems are based on PKI's, which links public keys to entities' identity (like people and organizations). As claimed by DigiCert, a PKI security solution, when properly implemented, provides strong device identity and encryption for in-transit data, and protects devices and networks from exploits.

Nowadays, the *OAuth* and *SAML* for example, are the basis for building an IdM system, such as *Shibboleth* or *Keycloak*.

Shibboleth (“What's Shibboleth?”, n.d.) is an open source project that provides federated SSO and attribute exchange systems implementing widely used federated identity standards (as described in the Section III) by exploiting *SAML*. As far as we know, this is the second most cited and used system, preceded only by OpenID (Morgan et al., 2004). To use a service provider connected to a federation, users must authenticate using their organizational credentials (Shibboleth Identity). This way, an organization (identity provider) will pass the least amount of information to the service provider manager, whether allowing user access. As a result, authenticated users will have access to any service provider that is connected to this federation. This tool focuses on user authentication based on attribute exchange (Mahalle et al., 2010). *Shibboleth* consists of several individual components: an IdP, SP, and Discovery Service (DS). Users may choose to deploy one or more of these components depending on their needs. Currently, *Shibboleth* is not being considered as an IdM for IoT scenarios because, although SSO may be useful as users only need to authenticate once to interact with various devices, the traditional Web 2.0 SSO is not designed to meet certain IoT requirements (Roman et al., 2011).

[1] Sandbox can be considered as an essential layer to the protection system. A system is able to concentrate its operations in a restricted area where all unreliable programs, records, and activities can run completely isolated from the computer's operating system. (Prevelakis & Spinellis, 2001)

Keycloak ("Open Source Identity and Access Management - For Modern Applications and Services", n.d.) is an open source Identity and Access Management (IAM) solution focused on modern applications and services. It is already set to be used with support for User Federation, Identity Brokering, SSO and Social Login. SSO allows a user to log in only once and then access all systems that are configured in *Keycloak*. *Keycloak* is based on standard protocols and provides support for OpenID Connect, OAuth 2.0 and SAML.

PRIME (PRIME, 2008) is a system that focuses on effectively managing and protecting users' private data. This system uses *Idemix* (Camenisch & Van Herreweghen, 2002) which allows the creation of anonymous credentials that can be deactivated.

Even with the existence of SSO, such as *OpenID* or *Shibboleth*, security and privacy still need to be fully addressed in IoT (Alqassem & Svetinovic, 2014). This leads to the need to analyze IdM systems for IoT and define an identity for "things".

IV. Identity of Things

There is an area of endeavor in IoT that includes assigning a Unique Identifier (UID) with metadata associated with devices and objects (items) that allows them to effectively connect and communicate with other entities on the Internet ("Web Fraud Prevention, Online Authentication & Digital Identity Market Guide", 2015). Unlike the three categories of human multi-factor authentication (see section I), the approach in IoT is more complex. Lam and Chi, 2016 present an idea for Identity of Things based on four categories: *inheritance*, *association*, *knowledge* and *context*.

Inheritance category is equivalent to biometrics in humans, so it is necessary to find an identical mechanism that identifies devices. The suggested mechanism is the Physically Unclonable Function (PUF) (Devadas et al., 2008; Tuyls & Batina, 2006; Van Herrewege et al., 2012), however, there are some known attacks to this mechanism, such as those described in previous works (Ganji et al., 2018; Helfmeier et al., 2014; Ikezaki et al., 2016; Rührmair et al., 2010). Also, it is not as flexible as the other categories as it depends on the chip/hardware manufacturers.

The *association* and *knowledge* categories do not have as many hardware requirements as *inheritance*. *Association* is equivalent to the *"something you have"* category of human multi-factor authentication, but it is not easy for an IoT device to process something external (such as a hardware token). Similar to the *"something you know"* category, the authors present the *knowledge* category where there is, for example, the phone's International Mobile Equipment Identity (IMEI).

However, what attracts more attention in IoT is the *"context"* category, which the authors also refer to as the fourth category of authentication methods. *Context* can be defined according to device location, for example.

V. Ongoing research on privacy-preserving IdM for IoT

Power and bandwidth limitations of IoT devices makes the task of applying IdM to IoT much more complex and challenging (Lam & Chi, 2016).

There are many IdM systems for IoT, and we have reviewed some of the most cited projects. Researchers have been working on IdM solutions but are not focused on solving privacy issues. Although there are new frameworks (Mahalle et al., 2010) that guarantee certain defined security objectives, more implementation and evaluation details are lacking to analyze the privacy properties it contains. Another approach focuses on user-centric IdM framework consisting of user identity, device identity and the relationship between them (Butkus et al., 2014). It correlates a user's identity with a device's identity, but does not address privacy issues.

Our focus is primarily on properties that can help preserve data privacy, especially confidential data, by addressing the data minimization principle, which is a central aspect of the recent General Data Protection Regulation (GDPR) ("Art. 5 GDPR Principles relating to processing of personal data." n.d.).

Partial identity is a basic principle of privacy adopted by previous works (Sarma & Girão, 2009; Such et al., 2011). However, these works do not preserve anonymity because entities are identified by a certificate that is fully disclosed to other party. For example, most works use X.509 certificates as credentials to model real identities and *SAML* security tokens to encode partial identities to be used later to prove ownership of certain attributes (Bernabé et al., 2017).

As privacy is a focus of our research, we have decided to highlight systems and projects based on the Anonymous Credential concept ("Melissa Chase "Anonymous Credentials: How to show credentials without compromising privacy" Microsoft Research", 2011), where we can display credentials without compromising privacy. The idea behind the concept is that users can obtain credentials and display some of their own properties without revealing additional information or allowing tracking. Each token, as well as credentials, are designed to be used only once. There are several examples, such as subway tokens, electronic money (e-cash), movie tickets and access passes for online services. This way, users are anonymous and several tokens used by the same users are unlinkable. Note that, if at some point a token is used twice, the identity of a user using that token will be revealed.

For example, in a movie theater, there are age restrictions on buying tickets for certain movies. If a person wants to prove that he or she is over 18 years old, the movie theater does not need to have access to more information (such as an identification card with all personal information, full date of birth or even exact age) than expected, instead, it only needs to obtain proof of age over 18 years.

There are two implementations that address privacy issues through the concept of anonymous credentials: *Idemix* (Camenisch & Van Herreweghen, 2002) and *UProve* (Paquin & Zaverucha, 2011). The schemes implemented by each model, through protocols

and cryptographic mechanisms, allow the presentation of credential authentication through credentials and proofs of attributes, preserving anonymity.

Recent works (Bernabé et al., 2017; Sanchez et al., 2018) use *Idemix* in their implementations. There is a holistic IdM system (Bernabé et al., 2017) that handles heterogeneous IoT scenarios that require traditional online access control and authentication, along with a claims-based approach to privacy-preserving M2M interactions. The system follows a claims-based approach with attribute-based credentials. This project has been tested and implemented within the European research project *SocIoTal*. The IdM system features the IBM's cryptographic library *Idemix* (Camenisch & Van Herreweghen, 2002), providing a privacy-preserving solution that addresses IoT scenarios in which consumers and vendors may not only be traditional computers, but also smart objects (e.g. smartphones). In addition, *SocIoTal IdM* has been integrated with *FIWARE Keyrock IdM* ("Identity Management - KeyRock", 2018) to support traditional IdM management operations in scenarios where claims-based access is not required. The implementation is in Java and, as described in the official implementation of this project ("SocIoTal IdentityManager", n.d.), there are five main components that make up the IdM. However, the *SocIoTal* (Bernabé et al., 2017) system is not suitable for resource-limited devices because, despite being a real redeployment to integrate *Idemix* into IoT, it is intended for Android devices and is written in Java, which requires high computational and memory resources to run.

Other work (Sanchez et al., 2018) proposes a solution for authentication and authorization with privacy-preserving and is based on the concept of anonymous credentials. The idea of this concept is to have the IdM inside a device, avoiding consult external trusted third party, even to check attributes; it has zero-knowledge proofs and, for example, vehicles could authenticate their owner by verifying a proof from their wearable, such as a smart watch. The example that the authors give is based on a verification of whether someone inquiring is entitled to get some information (e.g. the owner full ID), by being a police officer, while some of that information is restricted in another context (e.g. just confirming that the owner lives in a particular area to a residential area concierge without providing the owner full ID). To sum up, a device can choose whether some information is shared or not in each case (minimal disclosure).

VI. Blockchain

Blockchain can be seen as a distributed database that maintains a list of sorted records in an increasing sequence. Different transactions are written in a block data structure. Each block is linked to the previous with a cryptographic hash function, thereby forming a Blockchain (Wüst & Gervais, 2018; Yli-Huumo et al., 2016). Each block has unique, immutable and irreversible data values, ensuring that they are not changed in the process.

There are currently two types of Blockchain technologies, namely, permissionless (public chains) and permissioned (private chains). In a permissionless Blockchain, anyone can become part of the network without requiring an identity (and associated trust model); On the other hand, on a permissioned Blockchain, only trusted agents can write and possibly read those records (Mainelli & Smith, 2015), thus requiring a well-established identity and trust among the cooperating nodes.

Previous work has studied and evaluated private and public Blockchain from the point of view of a joint venture (Nuss et al., 2018). The authors claim that private Blockchain improves scalability in terms of large numbers of clients and transactions. In a permissioned blockchain, it is not necessary to compute difficult consensus mechanisms, such as Proof-of-Work. This can be done as participants are known and white-listed and must initially be authorized by a trusted authority. To improve throughput, the ordering of blocks requires a broadcast protocol that offers total order. Depending on the type of faults being targeted, these protocols can provide protection against crash faults, such as Kafka Garg, 2013, or stronger assurances by providing fault-tolerance against byzantine (arbitrary) faults (Lamport et al., 1982). This makes private Blockchain more efficient.

Public Blockchains are decentralized and independent of a central authority. It needs consensus mechanisms that refer to the process of reaching a unified agreement (consensus) on the current state of the distributed ledger (Zheng et al., 2017). It facilitates verification and validation of the information being added. This ensures that only authentic transactions are written to Blockchain, achieving reliability and establishing trust between unknown peers in a distributed computing environment.

In terms of security, it is important to deal with tampering and impersonation issues, which can lead to information leakage or tampering. A 51% attack refers to an attack on a Blockchain when a person or group of miners controls more than 50% of the computing power of the network because it would have the same mining capacity as all other mining groups. Public Blockchain protocols are vulnerable to attacks that can take advantage of the need for consensus. If miners can control 51% of nodes operating on the network, they can manipulate core rules and take control of the system, being able to attack the network and rewrite the Blockchain recent history, sensor transactions (e.g. for name registrations), and steal cryptocurrency using double spend attacks (Ali et al., 2016).

A. Motivation for using Blockchain with IoT

Most previous works related to IdM, authentication, and authorization focus on heavy and complex communication protocols in terms of computation and memory requirements and have Single Point of Failure (SPOF) problems, where one component failure can compromise the entire system. PKI-based solutions are complex, expensive, and not easy to manage. This is not desired due to resource constraint issues on IoT devices. PKI also relies on a Certification Authority (CA) that represents a SPOF problem. If an attacker could create a fake CA, it would provide digital certificates that would be accepted as true by

many browsers. A browser can then claim that a site is legitimate when it is a fraud. By using fake CAs and exploiting the MD5 algorithm flaw, crackers can use the well-known Domain Name System (DNS) flaw to create unidentifiable phishing attacks.

For example, in 2011, these failures already occurred when it became clear that a security breach resulted in fraudulent certificate issuance by *DigiNotar* (Prins & Cybercrime, 2011; Zetter, 2011). More than 500 fraudulent certificates were issued by *DigiNotar* and 300,000 addresses were compromised. As a result, a hacker may impersonate someone else to gain access to sensitive information.

Federated user-centered IdM using relationships is a paradigm that has helped in the development of IdM systems reducing the complexity of users who manage their identities. However, the trust is centered on identity providers, who can see all activity between users and their online service providers. It is important to eliminate the SPOF problems inherent in trusted third parties and create a decentralized solution. Adopting a standardized peer-to-peer communication model for processing hundreds of billions of device-to-device transactions will significantly reduce the costs associated with installing and maintaining large centralized data centers. In addition, it will distribute computing and storage needs among billions of devices that form IoT networks, preventing the SPOF problems (Sem-III, n.d.).

Currently, there is also some IoT sensor data stored in traditional centralized databases that have access control protocols that define who can access this data. However, data can be changed fraudulently and is vulnerable to the SPOF problem. Blockchain enables the creation of more secure network meshes in which IoT devices are securely interconnected, avoiding threats, such as spoofing and device impersonation. With each legitimate node being registered in Blockchain, devices will be able to identify and authenticate themselves. This block-based approach is more agile, and each registered identity can be associated with the device's public key, allowing for a more secure communication scenario. However, it is possible to suffer a Sybil attack with Blockchain, so it is important to know that the nodes are secure. When there is no central authority, a reputation system is required. In Blockchain-based reputation systems, a user account can be created as a real identity, while the real identity is not disclosed. Attackers may leave the system after attempting to inject fraudulent subjective information, but will not be able to rejoin and create a new account to launder their previous rating history (Cai & Zhu, 2016). Leveraging Blockchain's capabilities, each device with an identity has an immutable reputation and history when the device's certification agency audits the device and registers its identity with Blockchain from birth.

Otherwise, centralized systems have a hierarchical context addressed (device @ host, with the host gaining its identity by assigning an IP address or registering a DNS) ("How can blockchains improve the Internet of Things?", 2016). Blockchain can ensure unique IDs and object authenticity by providing interoperability between devices.

There are other advantages to IoT environments (Atlam et al., 2018), that do not focus solely on identity. Blockchain ensures decentralization, which means sensors can exchange data directly with each other rather than using a third-party system to establish digital trust, which also reduces implementation and operation costs by eliminating intermediaries. This is recommended due to resource-limited devices in IoT environments. In addition, non-manipulation is also guaranteed by an immutable ledger, which is one of the key advantages of Blockchain technology. Any changes to a distributed ledger should be checked by most network nodes to ensure security. Finally, technology gives devices autonomy through smart contracts and, in case of problems, a record is easily accessible and non-manipulable.

B. Limitations of integrating Blockchain with IoT

While Blockchain can solve identity issues, we also need to understand if Blockchain can be integrated with IoT. We want to analyze the benefits and drawbacks of this integration.

There are some advantages to integrating Blockchain with IoT environments (see the section VI-A). However, Blockchain is computationally heavy and costly in terms of power consumption (O'Dwyer & Malone, 2014). It must be adapted to be suitable for resource-limited IoT devices. With the huge amount of data on IoT, Blockchain must handle billions of transactions between IoT devices. Scalability needs to be improved and there have been a lot of efforts to solve this issue, but there is still a lot of research to be done to come up with a comprehensive solution.

Some optimizations can be made to Blockchain, such as throughput management, lightweight consensus and distributed trust (Dorri, Kanhere, Jurdak, & Gauravaram, 2017b). To ensure that network utilization is within a prescribed operating range, throughput management can be done to provide self-scalability, and as the network grows, more transactions can be added to the public Blockchain.

In addition, the design of a new distributed trust method improves processing time to validate new blocks as it gradually decreases as they build trust with each other. It is also possible to enhance these optimizations with a tiered architecture that uses a private, centralized immutable ledger to reduce overhead and a decentralized public with high-end devices for greater confidence. This does not lead to further delays in transaction processing (Dorri, Kanhere, & Jurdak, 2017).

Another optimization is to eliminate the need to solve any puzzle before attaching a block to the Blockchain (proof-of-work). Complex mathematical puzzles require a substantial amount of computational power. Recently, a decentralized privacy-preserving healthcare Blockchain system for IoT (Dwivedi et al., 2019) eliminates PoW to make it suitable for IoT. Blockchain transactions are public and there is additional information about senders and recipients on the Blockchain network. Thus, this work uses a ring signature scheme that preserves privacy to provide anonymity to users.

Fog and Edge computing concepts are also important for data processing optimizations, improving latency and scalability. The idea is to relocate part of the computing power in the data center to network boundaries. In the Blockchain concept, computing can be transferred to edge servers near miners (Xiong et al., 2018) to overcome substantial CPU time and power consumption issues.

The combination of smart contracts with Blockchain is proposed to automate time-consuming workflows, achieving verifiable encryption and significant cost and time savings in the process (Christidis & Devetsikiotis, 2016). Blockchain offers a resilient distributed peer-to-peer system and the ability to interact with peers reliably and audibly. Smart contracts allow to automate complex multi-step processes.

Blockchain's current approaches focus on process optimization based on Byzantine Fault Tolerant (BFT) and propose *Bitcoin NG* (Eyal et al., 2016) to support billions of devices without the need for additional features. However, BFT protocols often have problems with node scalability (Brewer, 2000), which is significant for Blockchain over IoT applications. In terms of scalability, for example, BFT is worse than Bitcoin because Bitcoin scales well for thousands of nodes, while BFT scales only for a few dozen nodes (Yeow et al., 2017). In terms of complexity, they have the opposite behavior, as BFT has less complexity than Bitcoin. However, it is also impractical to integrate Bitcoin directly into IoT. Previous work integrates Bitcoin with IoT to provide a multi-layered Blockchain-based method for sharing IoT user data with organizations and people (Hashemi et al., 2016). The authors assume that IoT devices do not have enough resources to solve PoW because it requires very sophisticated hardware and we cannot consider direct integration as it requires facing some resource, latency, bandwidth and scalability challenges. The performance of Practical Byzantine Fault Tolerance (PBFT) is also analyzed as a consensus algorithm, however it can be a bottleneck in networks with a large amount of peers (Sukhwani et al., 2017).

There are some proposals for redefining consensus algorithms to be more suitable for IoT integration. Hardware can improve the performance of consensus methods (Vukolić, 2015). A concept called Proof of Luck (Milutinovic et al., 2016) is a consensus mechanism that relies on Trusted Execution Environments (TEE) capabilities with a Blockchain design proof of concept that offers low latency transaction validation, reduced power consumption and evenly distributed mining. There is ongoing research on consensus protocols to achieve scalability (Panarello et al., 2018). Proof-of-Trust (Zou et al., 2018), for example, attempts to address scalability problems, particularly associated with BFT-based algorithms, and avoids the low throughput and resource-intensive associated with PoW mining.

In brief, a standard solution to the limitations of Blockchain integration does not yet exist. For example, there are no solutions to the 51% attack or a standard definition of a lightweight Blockchain yet (Roy et al., 2018). Future research directions are related to these limitations, namely in the areas of security and privacy, connectivity and scaling, energy consumption, resource allocation, Blockchain standardization and model optimization.

C. Blockchain-based Identity Management systems

In this section, we systematically review Blockchain-based IdM systems. Past works critically analyzes and compares the different Blockchain-based IdM and authentication systems from 2014 to 2018 (Lim et al., 2018).

These solutions can be categorized into *permissioned* and *permissionless* Blockchain (Zhu & Badr, 2018). The authors highlight two systems in each of the categories: *uPort* ("Uport: A platform for self-sovereign identity." 2017) and *Sovrin* (Khovratovich & Law, 2017).

Another categorization (Dunphy & Petitcolas, 2018) for IdM solutions can be done between: *Self-Sovereign identity* and *Decentralized Trusted Identity*. The authors highlight three DLT-based IdM schemes, namely, *ShoCard*, *uPort* and *Sovrin*, and evaluates their benefits and shortcomings by providing a detailed description of the three systems.

While *ShoCard* focuses on digital identity for humans, there is another system called *UniquID* ("Uniquid: A peer-to-peer trust model for IoT Protocol Primer." 2017) that is similar but attempts to fill the gap between human and digital entities (Shrier et al., 2016). For this reason, we also include this system in this description.

A recent paper proposes a decentralized privacy-preserving healthcare Blockchain in IoT (Dwivedi et al., 2019). It is utmost important to describe this system, because our work also focuses on the privacy-preserving properties and healthcare use case.

Therefore, a detailed description of five Blockchain-based Identity Management systems will be provided in this section: *Sovrin*, *uPort*, *ShoCard*, *UniquID*, *A Decentralized Privacy-Preserving Healthcare Blockchain for IoT*.

Sovrin

Sovrin (Khovratovich & Law, 2017) is a public permissioned distributed ledger dedicated to self-sovereign identity.

The consensus protocol used in *Sovrin* is called *Plenum* and is an improvement over RBFT (Aublin et al., 2013) based on the BFT protocol.

This choice of permissioned and the application of different consensus protocols is an enhancement for low-cost computation, thus reducing the energy cost of running a node and improving transaction throughput. This is beneficial for integrating *Sovrin* with IoT, specifically for resource-limited IoT devices.

In *Sovrin*, a user can generate any number of required identities. This way, it can guarantee privacy because identities are separate, unlinkable and controlled by a different asymmetric key pair. These identities are managed by *Sovrin* and follow the

Decentralized Identities (DID) specification. DID is a set of features that define objects in a unique way. In this specification, there is no central register that gives to the receiving entity a "positive signal" in the validity of the data. DID is completely under the authority of the user.

It integrates unforgeability, performance, unlinkability and a distributed ledger, adopting the best practices of both Ethereum (Wood et al., 2014) and BFT protocols. However, one of Blockchain's problem is that it is easy to violate privacy in a public ledger by correlating transactions to make inferences about users. To mitigate this risk, it also includes the concept of anonymous credentials ("Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. Sovrin Foundation." 2018) which gives users full control over all aspects of their identity.

uPort

Unlike *Sovrin*, *uPort* ("Uport: A platform for self-sovereign identity." 2017) does not provide a full stack for managing distributed ledger identities for devices. It is based on an Ethereum smart contract to design a digital identity model and is a public permissionless Blockchain where anyone can be a validator node. *uPort* allows users to register their own identity on Ethereum, submit and request credentials, sign transactions, and manage keys and data securely. The system aims to abstract end-user public key cryptography to make the user experience intuitive. It provides self-sovereign identity, meaning that users can store their own identity data on their own devices and efficiently provide it to those who need to validate it without relying on a central repository of identity data. A mobile app holds the user's private key and a smart contract address acts as its identifier (Bertram & Georg, 2018). It ensures identity reliability and usability through a set of operations (key and identity recovery) (Zhu & Badr, 2018).

ShoCard

ShoCard ("Travel Identity of the Future - White Paper." 2016) is a different approach, more focused on user identity and helping individuals and business quickly validate identities without having to use passports or other physical identification documents. It allows it to work as a mobile identification that can be verified in real time while using a combination of encryption and Bitcoin ledger immutability. Perhaps most importantly, the company claims that identifying information can be verifiable without requiring users to relinquish control of their data.

Users create their identities on Blockchain using their personal details and must be validated by a known and trusted organization with the ability to verify identities. Users can use their own identity to travel, and their travel agency can search Blockchain and verify that their identity has been validated by a trusted organization.

In terms of privacy, the authors claim that user data is not stored in Blockchain but has their own cryptographic proofs to show that the data is correct. It also provides selective disclosure, to create a key pair for each of the fields that user is storing in *ShoCard*, so that the user has a private master key and private keys for individual data fields. The fingerprint of data on Blockchain is protected by a private key; therefore, only the user who owns the private key can modify the data.

UniquID

Another work called *Uniquid* ("Uniquid: A peer-to-peer trust model for IoT Protocol Primer." 2017) is building a technology that identifies devices themselves while offline, through very clever use of Blockchain technology and smart contracts.

Instead of using PKI, *UniquID* applies Pretty Good Privacy (PGP) and Web of Trust (Caronni, 2000) principles. The identification of each device is generated by themselves using pseudo-random functions, following the same principle as PGP. However, as there are no third parties in this process, *UniquID* devices must rely on a *secure element* (Anantha et al., 2016) to generate their own identity and maintain integrity. Finally, *UniquID*, following Web of Trust principles, requires a decentralized mutual recognition process using cryptographic signatures. *UniquID* devices must first complete an Imprinting Ceremony Giaretta et al., 2019 with other previously enabled devices, closer to the time of manufacture, to exchange public keys in a secure environment and reduce the risk associated with man-in-the-middle attacks.

This system focuses on IoT and the authentication process is performed between devices without the need for third party intermediaries, allowing devices to be independent (Lim et al., 2018).

A Decentralized Privacy-Preserving Healthcare Blockchain for IoT

Dwivedi et al., 2019 feature a decentralized privacy-preserving healthcare Blockchain system for IoT. By eliminating PoW, the authors made some adaptations to Blockchain to make it suitable for IoT. The authors implement some techniques to help preserving privacy in identity, such as a ring signature scheme to provide anonymity to user data. There is still no evaluation or implementation of this system to really analyze the functionality of the system and if the Blockchain adaptation worked, i.e., if it is light enough for IoT, for example.

VII. Building a Privacy-Preserving IdM System

This section will present a comparative table of IdM systems for some features that will be defined according to a selection methodology. We also present a methodology for systems selection.

A. Methodology for feature selection

This section describes the feature selection criteria that help to evaluate IdM systems.

We chose several features into three categories:

- Privacy features: Self-Sovereign, Unlinkability, Revocation, Selective Disclosure, Untraceability and Unforgeability;
- Usability features: Offline and Scalability;
- IoT features: Device Identity and Designed for IoT.

The main feature that we chose to evaluate the IdM systems for IoT is ***Device Identity***. We are not only interested in the IdM of a human, but in the IdM of a human connected to a device or a standalone device. ***Device Identity*** allows to understand who the device is and to avoid possible attacks, such as impersonation, among others. IoT devices control critical systems, such as smart city traffic or healthcare situations. For this reason, device identity is important due to security and privacy issues. IoT devices must be able to perform mutual authentication with users, other devices, and the cloud without the need for central coordination by servers. In a healthcare context, for example, we need the device to be able to connect to multiple entities (other devices or medical assistants) that perform an end-to-end authenticated treatment, without allowing malicious/unauthorized parties to attack the sensors and cause the system to malfunction. We will consider that with this feature, systems that manage a device's identity do not require a user-managed application, allowing devices to communicate with each other without the intervention or credentials of a specific user.

In addition to the device identity, it is important to understand if the system was ***Designed for IoT***. This concept is important because, in a system designed for IoT, entities must apply technical and organizational measures in the early stages of design to ensure correct compliance with IoT requirements throughout the construction process.

Another feature set is focused on privacy-preserving and is inspired on the concept of anonymous credentials ("Melissa Chase "Anonymous Credentials: How to show credentials without compromising privacy" Microsoft Research", 2011) (see section V) to ensure minimal disclosure of information.

One of the key features for privacy-preserving is ***Unlinkability***, as the adversary should not be able to determine if two blinded credentials are produced from the same self-blindable credential (Yang et al., 2015). Therefore, this property ensures that different presentations of the same credential cannot be linked (Khovratovich & Law, 2017).

Another important feature inspired by the concept of anonymous credentials is ***Selective Disclosure***. In terms of credentials, only a few attributes are required to complete authentication. To protect confidential information, only bits of information are presented to the verifiers (Garcia-Alfaro et al., 2017). This can be called a "partial identity". An interesting example is the identification of a person (prover) in a movie theater (verifier) (see section V).

Inspired by the same concept, we selected three more properties: ***Revocation***, ***Untraceability*** and ***Unforgeability***.

Untraceability ensures that a user can display a credential for a verifier without the verifier being able to reconstruct the credential back to the protocol instance in which it was issued (Layouni & Vangheluwe, 2007).

The concept of anonymous credentials has a solution to protect user privacy (Lapon et al., 2011). However, to ensure accountability, it is necessary to have ***Revocation*** mechanisms. The system should provide users with a way to manage the information contained in their identities and revoke it. Users or any verifiers may know, within a reasonable time, that their credential has been revoked (Khovratovich & Law, 2017).

A system must have the ***Unforgeability*** property, where a certificate must be issued by a legitimate person. Therefore, a malicious user cannot forge certificates, it is simply impossible (Chung et al., 2011).

Inspired by Blockchain, we also added ***Self-Sovereign*** to the privacy feature set. With a self-sovereign identity, individuals no longer depend on a third entity to issue an "identifier" to them. The individuals will create their own "identifiers", maintaining their control and ownership, as well as the information they wish to share, with whom and under what conditions. In terms of privacy, *Self-Sovereign* pushes identity ownership of centralized services across borders so that identities are under the control of their owners, and this is important because, with a decentralized solution, attackers cannot exploit a SPOF problem.

In terms of system usability and availability, one of the most interesting properties is the way to define and verify an identity ***Offline***. Let's take a look at an example of unlocking a car with a smartphone. If there is no Internet connection, owners would need to take their cars to a location with an Internet connection to download the certificate and establish a connection between the owner's car and phone. To avoid this, it is necessary to implement a mechanism to unlock a car even if there is no Internet connection. Researching the concept, we found a paper stating that Blockchain can solve this problem ("How Blockchain Startups Will Solve The Identity Crisis For The Internet Of Things." 2017).

Given the large number and variety of devices involved in IoT, these systems need to be built to meet the requirements of ***Scalability*** to support many connected devices and store the huge amount of data they produce. A scalable data system is one that can continue to work well when its context changes in size or volume to meet user needs. ***Scalability*** can also take advantage of this, moving from a smaller to a larger system and making the most of the latter in terms of performance.

Statistically, we want to compare the ***Commercial/Open Source use*** or number of ***Citations*** of the projects, that also enhance the interest of analysis. ***Commercial/Open Source use)*** is based on the number of GitHub forks and the number of ***Citations*** is based on Google Scholar (as of 2019-10-16).

B. Methodology for system selection

This section describes the system selection criteria. First, we need at least two traditional IdM systems to compare with others, because it is important to know what kind of resources they can handle, even without focusing on IoT and privacy.

In addition to the traditional IdM systems, we chose two more system sets to compare. The choice of Blockchain systems is based on the focus of our research questions, and the idea is to analyse whether these systems should be used in IoT and can help meet the selected privacy features. For a comparison term, and as there are recent systems that use *Idemix*, it is important to also include the concept of anonymous credentials in the comparison.

The three system groups can be named: "Traditional IdM systems", "IdM systems based on the concept of " and "Blockchain-based IdM systems".

- **Traditional IdM systems:** ***OpenID*** (Recordon & Reed, 2006) and ***Shibboleth*** (Morgan et al., 2004; "What's Shibboleth?", n.d.);
- **Anonymous credentials-based IdM systems:** ***SocIoTal Identity Manager*** (Bernabé et al., 2017) and ***Anonymous Credential Systems in IoT*** (Sanchez et al., 2018);
- **Blockchain-based IdM systems:** ***UniquID*** ("Uniquid: A peer-to-peer trust model for IoT Protocol Primer." 2017), ***uPort*** ("Uport: A platform for self-sovereign identity." 2017), ***Sovrin*** (Khovratovich & Law, 2017) ("Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. Sovrin Foundation." 2018), ***Decentralized Privacy-Preserving Healthcare Blockchain for IoT*** (Dwivedi et al., 2019).

Traditional IdM systems

OpenID is the most widely used ("OpenID Organization", 2017) and one of the most cited IdM system (Recordon & Reed, 2006). ***Shibboleth*** (Morgan et al., 2004) is also one of the most cited among many existing traditional IdM systems. For this reason, we decided to analyze the features of these two systems. Commercial use is not available because the system is closed and there is no information on how many users or companies are using it.

Anonymous credentials based IdM systems

Due to the features we selected based on the concept of anonymous credentials, that contribute to solve privacy-preserving issues, we discovered two academic research projects (***SocIoTal Identity Manager*** and ***Anonymous Credential Systems in IoT***) using *Idemix* technology and focused on privacy issues and IoT. ***Anonymous Credential Systems in IoT*** has a few citations, but it does include an advantage over *SocIoTal Identity Manager*, for example, being lightweight for IoT, so we think it is important to include it.

Blockchain-based IdM systems

Finally, we selected four Blockchain-based IdM systems. *ShoCard* is part of systems that have not been selected for comparison. For example, in this system, bootstrap is done through a trusted identification document (passport or government identification for example). IdM is done through users that give devices an identity (a device is linked to a specific user). Therefore, this system is more focused on user identity than device identity, being farther from an IoT integration than others, so it is not as interesting for our comparison.

UniquID has been selected based on the *Offline* feature and because it is attempting to integrate with IoT technology. We are not only interested in systems designed for IoT, but when we have several Blockchain systems to choose from, we prefer those that are closest to possible integration. ***UniquID*** can solve the *Offline* problem (see section VII-A) and focus entirely in IoT as it makes IAM of connected things.

uPort and ***Sovrin*** are two interesting systems to be in the comparison table. Both are always referenced whenever the literature is about IdM in Blockchain. It is interesting to see how the current state of the integration between IoT and Blockchain and its applicability to privacy issues.

Decentralized Privacy-Preserving Healthcare Blockchain for IoT covers three very interesting concepts: Healthcare, Identity and Blockchain for IoT. We find it interesting to include in the comparison because, in addition to encompassing the three concepts we are addressing, it also addresses privacy issues and attempts to take a new approach to trying to loosen up Blockchain to achieve the desired lightweight for resource-constrained devices.

C. IdM systems comparison

In this section, we will present a comparison table with the systems we have selected (see section VII-B):

1) *OpenID*;
2) *Shibboleth*;
3) *SocIoTal Identity Manager*;
4) *Anonymous Credential Systems in IoT*;
5) *UniquID*;

6) *uPort*;
7) *Sovrin*;
8) *Decentralized Privacy-Preserving Healthcare Blockchain for IoT.*

	1	2	3	4	5	6	7	8
Commercial usage (forks)	940 ("OpenID Organization", 2017)*	N.A.	5 ("SOCIOTAL", 2015)	0 (Sanchez et al., 2018)	N.A.	56 ("uPort Contracts for managing identity", 2017)	184 ("Hyperledger INDY", 2016)	N.A.
Citations	596 (Recordon & Reed, 2006)	225 (Morgan et al., 2004)	11 (Bernabé et al., 2017)	N.A.	N.A.	14 ("Uport: A platform for self-sovereign identity." 2017)	1 (Khovratovich & Law, 2017)	0 (Dwivedi et al., 2019)
Unlinkability	○	○	●	●	○	○	●	○
Revocation	●	●	●	●	○	●	●	●
Selective Disclosure	○	○	●	●	○	○	●	○
Unforgeability	○	○	●	●	○	○	●	●
Untraceability	●	●	●	●	○	○	●	○
Self-Sovereign	○	○	○	○	○	●	●	●
Offline	○	○	○	○	●	○	○	○
Scalability	●	○	●	●	●	●	●	●
Device Identity	○	○	●	●	●	○	●	○
Designed for IoT	○	○	●	●	●	○	●	●

●= Included;
○= Not Included.
* The sum of number of forks of different implementations of OpenID. ("OpenID Organization", 2017)
1) *OpenID*;
2) *Shibboleth*;
3) *SocIoTal Identity Manager*;
4) *Anonymous Credential Systems in IoT*;
5) *UniquID*;
6) *uPort*;
7) *Sovrin*;
8) *Decentralized Privacy-Preserving Healthcare Blockchain for IoT.*

TABLE I. TABLE OF FEATURES

The first two features of the Table I show the impact of systems on the community. The first feature is more related to commercial usage, while the second is most related to the scientific community. *OpenID* is the most widely used and cited system, according to statistics, but it is also the oldest. On systems 2, 5 and 8, there is no information on commercial use because it is closed source or not yet implemented. All systems have a considerable number of references and/or usage, which helped in systems selection for this table because of their relevance. However, systems 4 and 5 do not have much usage information and citations are scarce. However, the importance of these works is related to their characteristics.

Traditional IdM systems do not cover any of the feature sets.

In terms of IoT features, the authors of *Anonymous Credential Systems in IoT* ensure that the system can satisfy device identity and is designed for IoT. The authors of this paper compare it to *SocIoTal Identity Manager* and create a different lightweight solution because they claim that *SocIoTal Identity Manager* is implemented in Java and has no enhancement to be lightweight. We can see this system as an improvement of *SocIoTal Identity Manager*. In addition, both systems are designed for IoT.

UniquID and *Sovrin* have device identity, however, we consider that *uPort* does not. The authors state in a *Consensys* ("Consensys, Identity for Blockchain vs Blockchain for Identity", 2016) presentation that device identity can easily be done without a typical username/password combination, but it does not provide a detailed description of how to do it and how advanced is. *uPort* is not designed for IoT, but for the focus of user identity.

In the case of *A Decentralized Privacy-Preserving Healthcare Blockchain for IoT*, we also consider that the feature is not present. Although the system is designed for IoT and has the concern of being lightweight and simplifying multiple protocols to fit few resources, we consider that device identity is not present because device management is done by users who have healthcare devices attached to them. As far as we know, integrating devices between them requires a lot of effort.

In terms of usability, the two anonymous credential-based systems have the scalability feature but do not have the offline feature because it is not indicated in any specification of each system. Usability features are presented only as a whole in *UniquID*. The other three Blockchain-based systems do not have the offline feature. In terms of scalability, we consider that all the systems have this feature.

In terms of privacy, anonymous credential-based systems cover much the same and do not cover more Blockchain-specific features, such as self-sovereign. *Sovrin* covers almost all the privacy features presented in the table.

D. Summary of Findings

This section presents a set of features that we need to build a complete privacy-preserving IdM system for IoT (see section VII-A) which is the answer to **RQ1**. Then we also present a methodology for selecting systems (see section VII-B).

With the results from Table I (see section VII-C), *Sovrin* is the closest production system for IoT with privacy concerns. *Offline* is the only feature *Sovrin* lacks, however this can be adapted because the system is based on Blockchain.

With these conclusions, the answer to **RQ2** is yes because *Sovrin* is based on Blockchain and address more features than others.

VIII. Discussion on application scenarios

According to the conclusions of the section VII, *Sovrin* is the system that covers the most features presented in the table I.

There is a research area on IdM for IoT that is not focused on Blockchain. For this reason, we want to apply an order of importance to the selected features to analyze whether using Blockchain is necessary, depending on a specific application case. Therefore, instead of defining whether Blockchain can help meet all features, we find it more important to define whether Blockchain should be used in two different IoT scenarios. For this reason, we decided to do a comparative study of two use cases in the healthcare area.

Healthcare is adapting to the IoT paradigm. This means that in the future, a Hospital will be equipped with IoT sensors and actuators spread across some rooms and on the patients. Several solutions give patients the ability to have more control over their health, educating them about the importance of maintaining a healthy diet and exercising frequently, for example. An example of a wearable device is the *Fitbit*, which monitors signals, such as heart rate and sleep quality. Also, there are simple health apps on smartphones that measure the number of steps, for example. By continually receiving medical data, patients become more aware of their physical condition and better prepared to take care of themselves.

It is not the first time we have seen news from activity trackers that have made a difference in health and disease detection, such as Apple Watch, which warned an 18-year-old girl that her resting heart rate was 190 beats per minute and that she should seek immediate help ("Apple Watch saves the life of Florida teen with a life-threatening disease." 2018).

From pacemakers to blood pressure cuffs, IoT health services can also help doctors better manage disease, monitor patients, and improve treatment outcomes – but the security of health data is a substantial risk that must be addressed.

Identity theft can be one of IoT's biggest issues, as one device can impersonate another to receive privileged information or bypass access controls. Addressing this situation is critical as it endangers the health and privacy of patients.

We choose different healthcare scenarios to define different identity and security needs. We will define a scenario that fits intensive care (where treatment should be urgent and instantaneous) and continuous care (treatment is continuous and not instantaneous. Patients' health data is shared with doctors to let them know their health over time for additional assertive treatment based on more data).

A. Intensive Care Medicine

Generally, patients in an Intensive Care Unit (ICU) need careful observation and need intense and constant concern. As patients in this situation have suffered serious injuries or have recently undergone surgery, it is critical to monitor patients with sensors attached to their body to detect their vital signs. If there is a problem, alarms should be issued to inform a doctor that a patient needs treatment (Chiuchisan et al., 2014).

We describe an identical scenario in which a patient is being treated only with the aid of a machine. Thus, there is no human presence to assist patients and machines. In this scenario, a set of roles and trust embodiment should be controlled from a control room where surgery data is kept and analyzed based on patient recovery, for example, in a recovery room (the scenario is illustrated by the Figure 1). For example, if a patient has a heart rate below a threshold, the room detects this autonomously and alerts the attending or nearest medical doctor. However, at the same time, room actuators may undergo some type of patient treatment, such as Basic Life Support (BLS).

These types of systems are very critical because, based on the type of surgery and the postoperative methodology, the systems may end up being different even for surgeries with similar people (age,gender,size) and may change accordingly to similar facts seen in surgery room. These tasks should be learned from previous data mining rules and fed with the most up-to-date information collected from the patient.

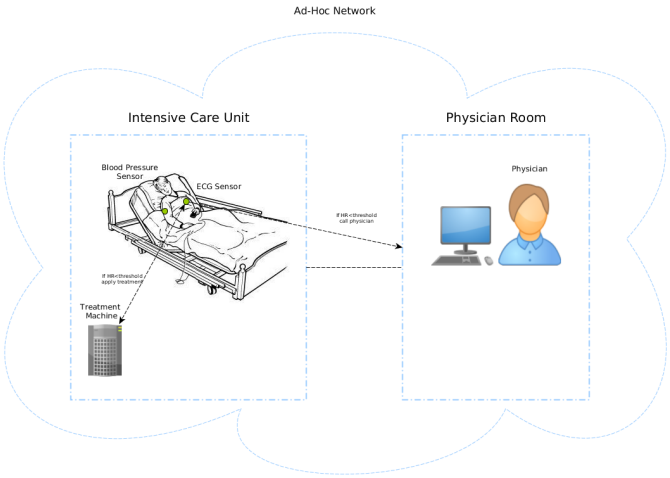

Fig. 1. Intensive Care Unit - Healthcare

("Intensive Care Unit", 2017)

This scenario may suffer impersonation issues, because an attacker could falsify patient data and the room's heart rate sensors, causing machines connected to the sensors (actuator) to provide unnecessary treatments, such as BLS, that can cause injury to patients.

We list the features in order of importance for this specific application scenario:

1) Offline - Offline is the most important feature in this scenario because if there is a failure on the Internet, it makes no sense to interfere with the warning of abnormal heart rate values, which can cause serious harm to the patient. In case of failure, the doctor assigns the treatment that should be inferred by a specific set of devices that can be tracked in the future;
2) Device Identity - With a device identity, things can be authenticated with each other or with humans. This feature is important primarily because of device lifecycle management, authentication and access control. If there is no authentication, for example, an attacker's heart rate sensor can impersonate a real sensor and produce erroneous values, sending dispatch alarms to doctors and inferring incorrect remedies for the patient;
3) Unforgeability - This feature is necessary because if a device with a sensor is susceptible to a Sybil attack, it may mislead the treatment;
4) Self-Sovereign - Along with the device identity feature, decentralization is important to prevent the attacker from exploiting a central point of failure.
5) Revocation - IoT devices may have a long lifespan, but some are disposable sensors; Therefore, it is necessary that at any time during the period of use, the system may define a sensor as revoked;
6) Selective Disclosure - IoT devices should only disclose relevant information about owners for communication with other parties. However, it may be important to access other details about the patient. For this reason, and if necessary, by the doctor, it may be possible to break security and access data;
7) Unlinkability/Untraceability - These are the least important features for this healthcare scenario. It may be important to know the owner of a sensor, or different sensors, for an urgent treatment situation. However, these features should be integrated by default, but it may be possible to break security and access data if necessary.

B. Continuous Healthcare

Continuous healthcare is a scenario that can prevent some fatal cases due to early detection and rapid response (Azimi et al., 2017). Health devices, such as ECG monitors, glucose monitors, pulse oximeters and blood pressure monitors exist, and will soon be supplemented with micro and nano-chemical sensors, which will provide ongoing medical diagnostics (Fernandez & Pallis, 2014) (the scenario is illustrated by figure 2). This type of healthcare can help detect some illnesses through medical monitoring (e.g. diabetic patients, other metabolic diseases, skin diseases and drug pharmacokinetics).

In this kind of scenario, the treatment is continuous. Patients' health data are shared with medical doctors for continuous surveillance and more assertive treatment based on more data. Generally, patients requiring this type of treatment are chronic or healthy patients who are undergoing continuous treatment or are continuously monitored, just in case. That way, if patients have a 24-hour tracking service every day, it will help doctors adjust treatment according to the patient's health condition.

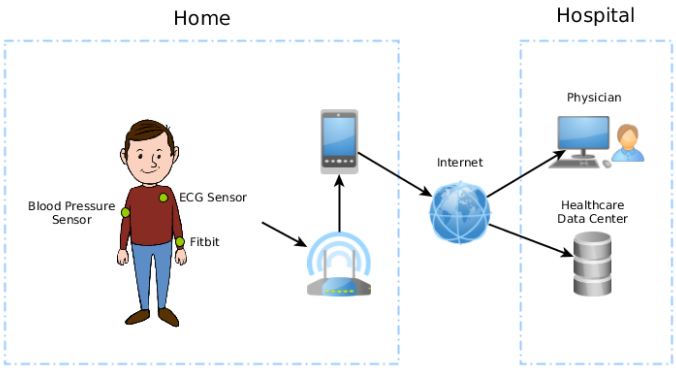

Fig. 2. Continuous Healthcare

("How to Draw for Kids", 2017)

As already described, there are some wearable devices, such as Fitbit or Apple Watch, that help in continuous monitoring of a patient, even being healthy. More recently, *Fitbit* and *Google* have invested in healthcare and the two have teamed up to improve the way fitness trackers handle their users' health data. According to some news ("Fitbit Strikes Deal With Google That Could Lead to Wearables Collaboration." 2018), a fitness manufacturer announced that it will implement the *Google Healthcare API* to provide health data directly to the electronic medical record systems used by doctors and hospitals. The aim of the union is to provide healthcare professionals with more detailed patient information so that they can receive personalized, efficient and tailored care. Thus, companies expect that with this constant stream of user health data, this technology will help doctors diagnose a disease and respond effectively.

This is already an evolution of this technology, as in recent years it has been used only to track user well-being and activity, or to be used by personal trainers to view activity and track athlete's data.

To classify features in this application scenario, we use a different methodology because we think all privacy features have the same importance and we also need to have the device identity. The only feature we consider less important would be Offline which belongs to the usability feature set. Unlike the previous scenario, Offline is not a high priority property and continuous care does not require offline communication in case of Internet failure, as it is not critical to act immediately. In this scenario, alerts and data taken from the patient's health can be stored to be sent to the medical doctor later.

C. Conclusions about the use of Blockchain in healthcare

This section analyzed different healthcare scenarios and prioritized features according to these scenarios to answer to **RQ3**. However, according to the results, the answer is: it depends on the application scenario.

In IoT healthcare, in general, it may be beneficial to use Blockchain in IoT scenarios, as it can also provide more reliable and secure strategies for an IoT medical device to promote Identity of Medical Things applications and smart contracts to automate device life cycle management (Dorri, Kanhere, & Jurdak, 2017). As healthcare works with a lot of sensitive user information, Blockchain can help with that. It is also important to use Blockchain to eliminate the SPOF problems and allow users to control all their information and transactions. It provides security access, scalability and data privacy, allowing a greater agility in transaction records, traceability of medical supplies (such as medicines, orthotics and prostheses), sharing data from patients to reduce repeated examinations, etc.

Intensive Care Medicine

More specifically, in intensive care, we can say that it is not necessary to use *Sovrin* for example, because *UniquID* has the most appropriate features according to priorities and is also the only one that has the offline feature. However, this system neglects some privacy issues, which also concern user data. While privacy features are minor in this application case, maintaining them is still important.

UniquID system may integrate a system based on *Idemix*, for example, such as *Sovrin* does, and may have the properties of Selective Disclosure, Unlinkability and Untraceability. However, it is important that in some emergency scenarios, the medical doctor may break this security for a larger purpose. This mechanism is called *Break the glass*, which means that users can gain access to some information in an emergency even if they are not allowed to access it. This option should be given to the medical doctor to access patient data in an emergency (assuming the risk of continuing and recording such action). Therefore, methods for this must be implemented. This is an interesting future research direction to apply to these systems or equivalent.

In addition, traceability is important to detect machine failures that can cause patient injury. We need to ensure that there is access to device data, such as vendor name, model and serial number, version, physical location, support contacts, or any other

relevant data points that can help specialists to quickly identify the device (device identity) and minimize damage that can occur in the worst case scenario. We do not want a malfunctioning machine to be in a future surgery room just because we completely anonymized the information and can no longer track the device.

Continuous Healthcare

In a continuous care healthcare setting, data can be archived and consulted later. It is not necessary to have all the urgency-related features, such as the Offline property that guarantees access to data even without an Internet connection. Therefore, this is not a priority.

Subsequently, we rank the order of priority according to the purpose of privacy. In this case of application, it is more important to ensure the privacy and anonymity of personal data, as it is often an ongoing treatment where critical health data is not needed (or what is needed is already being shared). For example, in the case of a personal trainer, it is not necessary to have access to data, such as the patient's blood type, for example.

Therefore, we assume that, as far as we know, ***Sovrin*** is the most complete system and what should be used. However, it would be unfair if we did not say that we could also choose system 4, as only the feature of self-sovereignty is lacking. In this case, the feature is important, but once we have features like unlinkability and selective disclosure, which ensure the privacy and anonymity of data, we can loosen up the model. If there are problems integrating Blockchain into implementations due to performance or scalability issues, we can adopt a solution that is not based on it.

Final decision

Regarding the question **RQ3**, this section begins with the answer: it depends on the application scenario, and the final decision follows the same parameters even after evaluating each use case.

Sovrin and ***UniquID*** were the main systems chosen because of their characteristics. However, if some developers do not want to use Blockchain to build a privacy-preserving IdM implementation for healthcare devices, because it is expensive in terms of computing and often involves high costs and width delays which are not directly suited for most IoT devices, developers may adopt different solutions (Dorri, Kanhere, & Jurdak, 2017).

From these analyzes, we conclude that the most important in these systems are the privacy features, and these can be found in the systems 3 and 4 with solutions based on the concept of anonymous credentials. The Blockchain can be implemented when there is a need to have specific features of this type of technology. There are many benefits of using Blockchain, as we describe during the analysis, and this should be considered when choosing the technologies for each use case.

IX. Limitations and Future Research Directions

After analyzing and answering the research questions presented in this paper, more questions have presented themselves that can potentially improve the research being done in this area.

1) Implementing break the glass mechanisms or policies to gain access to required user data: It is necessary to implement *break the glass* mechanisms to enhance an IdM system, complementing the features we have chosen. Depending on the use case for which the implementation is to be used, privacy features must always be present and implemented, regardless of the use case, the system must meet the requirements. The most common use of a *break the glass* mechanism is related to fire alarms, where a user must break a thin glass layer before being able to do anything, discouraging unnecessary activation. In healthcare, this concept already exists and is associated with the practice of opening confidential records and being recorded on an accounting disclosure form. In this paper, we provide an example of using *break the glass* in an intensive care use case (see section VIII-C), but may apply to other use cases. As far as we know, there is not yet an IdM system with privacy features that does this, and we believe it would be an improvement and a major innovation to the proposed requirements for building a complete IdM system for IoT in order to guarantee privacy preservation.

2) Context-based Device Identity: It is of utmost importance to consider how to manage IoT identity and authentication, as multiple entities need to authenticate with each other to create and provide trustable services. As billions of things will be interconnected, their identities need to be managed in a highly scalable way. Note that in IoT, identity of things should be based not only on their attributes but also on their **context**. We have identified some systems that have context-based identity, however, many of them have context based only on attributes, policies, or rules. Context can define different identities for a device and/or access control policies. Context attributes can be based on the environment in which the device is, for example, its location. Users who have access to a wearable technology (such as fitness trackers) may choose to use smart lock technology to unlock their smartphone through a set of trusted devices when connected via Bluetooth. However, users may want to enable this technology only at home as it is a controlled environment and only the family can mess with their smartphone and turn it off at work. In short, users would have different access control for each use, depending on the users' location.

3) Device Identity without depending of an owner: Given the introduction of context, it is also necessary to implement proprietary device identities without relying on an owner of that device. It would be interesting to be able to manage a device identity so it could have multiple identities, depending on the context, with different and multiple *personas*. Currently, IdM systems have some of these properties, but it always depends on the owner of a sensor, and it would be interesting to eliminate this dependency.

4) Anonymous Credential concept on IoT devices: After this definition of identity, it would be very interesting to integrate the properties of the concept of Anonymous Credential into the device. These properties are currently applied to the personal data of the device owner, but it is important to be able to do this privacy control of device properties and data as well.

5) Standard Blockchain-based solutions for IoT: Blockchain presents many promising opportunities for the future of IoT. The challenges, however, remain in the form of consensus models and computational transaction verification costs. Using Blockchain would be possible in all scenarios, but in order to make the systems usable and less computationally intensive, as suggested by Roman et al., 2011 in IoT, systems should be as simple and as small as possible, but without decreasing security levels / properties. Although there are already some approaches to the integration of Blockchain with IoT, a default definition is required.

X. Conclusions

IoT has become a common household name with its continuous and ever-growing adoption in our daily lives, fuelled mainly by the convenience and efficiency it brings. However, the large amounts of data it generates, including sensitive information, requires more fail-safes than the currently employed, e.g., proper identity management is required to prevent impersonation attacks.

There are several IdM approaches to IoT, with and without Blockchain. We have seen that blockchain can help resolving issues related to centralizing and registering legitimate nodes, by allowing devices will to identify and authenticate themselves.

Given the postulated research questions, we have determined a set of features needed to define an IoT-focused privacy-preserving IdM system. We have concluded that Blockchain, despite having many benefits, should not be used as a panacea for all scenarios.

As a culmination of this work, novel future research questions were brought related to the creation of a device IdM system, drive by the need of a device having to have a owner and be unable to have an identity by itself. In addition, context-based identity can enhance a better management of authentication and access controls.

To improve IdM systems, we propose implementing privacy features by default, including the properties of the concept of anonymous credentials. Also, the integration of *break the glass* mechanisms that can break associated security mechanisms for a greater good, even in sensitive healthcare settings where medical doctors may need to access some encrypted confidential patient information.

Regarding the usage of Blockchain, there is a substantial amount of ongoing research with different solutions for integrating this technology with IoT. However, a standard solution that deals with complexity and adaptability of resource-limited devices is needed.

Acknowledgement

The work of Patrícia R. Sousa and João S. Resende was supported by a scholarship from the Fundação para a Ciência e Tecnologia (FCT), Portugal (scholarships number SFRH/BD/135696/2018, PD/BD/128149/2016).

This work is also financed by National Funds through the FCT—Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) within the project CMU/CS/0042/2017.

This work has been supported also by the EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe (cybersec4europe.eu), Project "Safe Cities", ref. POCI-01-0247-FEDER-041435, financed by Fundo Europeu de Desenvolvimento Regional (FEDER), through COMPETE 2020 and Portugal 2020.

References

Aksu, H., Babun, L., Conti, M., Tolomei, G., & Uluagac, A. S. (2018). Advertising in the iot era: Vision and challenges. *IEEE Communications Magazine*, *56*(11), 138–144.

Ali, M., Nelson, J., Shea, R., & Freedman, M. J. (2016). Blockstack: A global naming and storage system secured by blockchains, In *2016 usenix annual technical conference (usenix atc 16)*.

Alqassem, I., & Svetinovic, D. (2014). A taxonomy of security and privacy requirements for the internet of things (iot), In *2014 ieee international conference on industrial engineering and engineering management*. IEEE.

Anantha, A., Krishnan, M. R., Marshall, A. L., Zargahi, K. R., & Abel, M. T. (2016). Secure element authentication [US Patent 9,509,686]. Google Patents.

Angin, P., Bhargava, B., Ranchal, R., Singh, N., Linderman, M., Othmane, L. B., & Lilien, L. (2010). An entity-centric approach for privacy and identity management in cloud computing, In *2010 29th ieee symposium on reliable distributed systems*. IEEE.

Apple watch saves the life of florida teen with a life-threatening disease. [(Accessed 28 June 2018)]. (2018).

Art. 5 gdpr principles relating to processing of personal data. [(Accessed 24 January 2018)]. (n.d.).

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. (2018). Blockchain with internet of things: Benefits, challenges, and future directions. *International Journal of Intelligent Systems and Applications*, *10*(6), 40–48.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787–2805.

Aublin, P.-L., Mokhtar, S. B., & Quéma, V. (2013). Rbft: Redundant byzantine fault tolerance, In *2013 ieee 33rd international conference on distributed computing systems*. IEEE.

Azimi, I., Anzanpour, A., Rahmani, A. M., Liljeberg, P., & Tenhunen, H. (2017). Self-aware early warning score system for iot-based personalized healthcare, In *Ehealth 360°*. Springer.

Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed security model and threat taxonomy for the internet of things (iot), In *International conference on network security and applications*. Springer.

Banerjee, M., Lee, J., & Choo, K.-K. R. (2018). A blockchain future for internet of things security: A position paper. *Digital Communications and Networks*, *4*(3), 149–160.

Bernabé, J. B., Ramos, J. L. H., & Gómez-Skarmeta, A. F. (2017). Holistic privacy-preserving identity management system for the internet of things. *Mobile Information Systems*, *2017*, 6384186–1.

Bertram, S., & Georg, C.-P. (2018). A privacy-preserving system for data ownership using blockchain and distributed databases. *arXiv preprint arXiv:1810.11655*.

Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2006). Fourth-factor authentication: Somebody you know, In *Proceedings of the 13th acm conference on computer and communications security*. ACM.

Brewer, E. A. (2000). Towards robust distributed systems, In *Podc*.

Butkus, P. Et al. (2014). A user centric identity management for internet of things, In *2014 international conference on it convergence and security (icitcs)*. IEEE.

Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: A perspective from blockchain technology. *Financial Innovation*, *2*(1), 20.

Camenisch, J., & Van Herreweghen, E. (2002). Design and implementation of the idemix anonymous credential system, In *Proceedings of the 9th acm conference on computer and communications security*. ACM.

Cao, Y., & Yang, L. (2010). A survey of identity management technology, In *2010 ieee international conference on information theory and information security*. IEEE.

Caronni, G. (2000). Walking the web of trust, In *Proceedings ieee 9th international workshops on enabling technologies: Infrastructure for collaborative enterprises (wet ice 2000)*. IEEE.

Chadwick, D. W. (2009). Federated identity management, In *Foundations of security analysis and design v*. Springer.

Chibelushi, C., Eardley, A., & Arabo, A. (2013). Identity management in the internet of things: The role of manets for healthcare applications. *Computer Science and Information Technology*, *1*(2), 73–81.

Chiuchisan, I., Costin, H.-N., & Geman, O. (2014). Adopting the internet of things technologies in health care systems, In *2014 international conference and exposition on electrical and power engineering (epe)*. IEEE.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, *4*, 2292–2303.

Chung, C., Lee, K., Yun, J., & Won, D. (2011). An improved anonymous electronic prescription scheme, In *International conference on future generation information technology*. Springer.

Consensys, identity for blockchain vs blockchain for identity [(Accessed 2 February 2018)]. (2016).

Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., & Khandelwal, V. (2008). Design and implementation of puf-based" unclonable" rfid ics for anti-counterfeiting and security applications, In *2008 ieee international conference on rfid*. IEEE.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for iot, In *Proceedings of the second international conference on internet-of-things design and implementation*. ACM.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017a). Blockchain for iot security and privacy: The case study of a smart home, In *2017 ieee international conference on pervasive computing and communications workshops (percom workshops)*. IEEE.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017b). Lsb: A lightweight scalable blockchain for iot security and privacy. *arXiv preprint arXiv:1712.02969*.

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, *16*(4), 20–29.

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for iot. *Sensors*, *19*(2), 326.

El Maliki, T., & Seigneur, J.-M. (2007). A survey of user-centric identity management technologies, In *The international conference on emerging security information, systems, and technologies (secureware 2007)*. IEEE.

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol, In *13th usenix symposium on networked systems design and implementation (nsdi 16)*.

Fernandez, F., & Pallis, G. C. (2014). Opportunities and challenges of the internet of things for healthcare: Systems engineering perspective, In *2014 4th international conference on wireless mobile communication and healthcare-transforming healthcare through innovations in mobile and wireless technologies (mobihealth)*. IEEE.

Fitbit strikes deal with google that could lead to wearables collaboration. [(Accessed 26 June 2018)]. (2018).

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the iot world: Present and future challenges. *IEEE Internet of Things Journal*, *5*(4), 2483–2495.

Ganji, F., Tajik, S., & Seifert, J.-P. (2018). A fourier analysis based attack against physically unclonable functions, In *International conference on financial cryptography and data security*. Springer.

Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., & Herrera-Joancomartıé, J. (2017). Data privacy management, cryptocurrencies and blockchain technology. Springer.

Garg, N. (2013). *Apache kafka*. Packt Publishing Ltd.

Giaretta, A., Pepe, S., & Dragoni, N. (2019). Uniquid: A quest to reconcile identity access management and the internet of things. *arXiv preprint arXiv:1905.04021*.

Hardt, D. (2012). The oauth 2.0 authorization framework.

Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016). World of empowered iot users, In *2016 ieee first international conference on internet-of-things design and implementation (iotdi)*. IEEE.

Helfmeier, C., Boit, C., Nedospasov, D., Tajik, S., & Seifert, J.-P. (2014). Physical vulnerabilities of physically unclonable functions, In *2014 design, automation & test in europe conference & exhibition (date)*. IEEE.

How blockchain startups will solve the identity crisis for the internet of things. [(Accessed 8 June 2018)]. (2017).

How can blockchains improve the internet of things? [(Accessed 1 June 2018)]. (2016).

How to draw for kids [(Accessed 29 June 2018)]. (2017).

Hyperledger indy [(Accessed 4 May 2018)]. (2016).

Identity management - keyrock [(Accessed 1 July 2018)]. (2018).

Ikezaki, Y., Nozaki, Y., & Yoshikawa, M. (2016). Deep learning attack for physical unclonable function, In *2016 ieee 5th global conference on consumer electronics*. IEEE.

Intensive care unit [(Accessed 29 June 2018)]. (2017).

Jesus, E. F., Chicarino, V. R., de Albuquerque, C. V., & Rocha, A. A. d. A. (2018). A survey of how to use blockchain to secure internet of things and the stalker attack. *Security and Communication Networks*, *2018*.

Khan, M. A., & Salah, K. (2018). Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411.

Khovratovich, D., & Law, J. (2017). Sovrin: Digital identities in the blockchain era. *Github Commit by jasonalaw October*, *17*.

Lam, K.-Y., & Chi, C.-H. (2016). Identity in the internet-of-things (iot): New challenges and opportunities, In *International conference on information and communications security*. Springer.

Lamport, L., Shostak, R., & Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382–401.

Laplante, P. A., & Laplante, N. (2016). The internet of things in healthcare: Potential applications and challenges. *It Professional*, *18*(3), 2–4.

Lapon, J., Kohlweiss, M., De Decker, B., & Naessens, V. (2011). Analysis of revocation strategies for anonymous idemix credentials, In *Ifip international conference on communications and multimedia security*. Springer.

Layouni, M., & Vangheluwe, H. (2007). Anonymous k-show credentials, In *European public key infrastructure workshop*. Springer.

Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L. M., Ang, T. F., & Ismail, R. (2018). Blockchain technology the identity management and authentication service disruptor: A survey. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(4-2), 1735–1745.

Mahalle, P., Babar, S., Prasad, N. R., & Prasad, R. (2010). Identity management framework towards internet of things (iot): Roadmap and key challenges, In *International conference on network security and applications*. Springer.

Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (aka blockchain technology). *Journal of Financial Perspectives*, *3*(3).

Melissa chase "anonymous credentials: How to show credentials without compromising privacy" microsoft research [(Accessed 17 January 2019)]. (2011).

Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016). Proof of luck: An efficient blockchain consensus protocol, In *Proceedings of the 1st workshop on system software for trusted execution*. ACM.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks*, *10*(7), 1497–1516.

Morgan, R. L., Cantor, S., Carmody, S., Hoehn, W., & Klingenstein, K. (2004). Federated security: The shibboleth approach. *Educause Quarterly*, *27*(4), 12–17.

Nuss, M., Puchta, A., & Kunz, M. (2018). Towards blockchain-based identity and access management for internet of things in enterprises, In *International conference on trust and privacy in digital business*. Springer.

O'Dwyer, K. J., & Malone, D. (2014). Bitcoin mining and its energy footprint.

Open source identity and access management - for modern applications and services [(Accessed 19 July 2017)]. (n.d.).

Openid organization [(Accessed 4 May 2018)]. (2017).

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. *Sensors*, *18*(8), 2575.

Paquin, C., & Zaverucha, G. (2011). U-prove cryptographic specification v1. 1. *Technical Report, Microsoft Corporation*.

Paul madsen. (2015) ”standardized identity protocols and the internet of things” [(Accessed 7 February 2019)]. (n.d.).
Prevelakis, V., & Spinellis, D. (2001). Sandboxing applications., In *Usenix annual technical conference, freenix track*.
PRIME, P. (2008). Identity management for europe.
Prins, J. R., & Cybercrime, B. U. (2011). Diginotar certificate authority breach'operation black tulip'. *Fox-IT, November*.
Recordon, D., & Reed, D. (2006). Openid 2.0: A platform for user-centric identity management, In *Proceedings of the second acm workshop on digital identity management*. ACM.
Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer*, (9), 51–58.
Roy, S., Ashaduzzaman, M., Hassan, M., & Chowdhury, A. R. (2018). Blockchain for iot security and management: Current prospects, challenges and future directions, In *2018 5th international conference on networking, systems and security (nsyss)*. IEEE.
Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S., & Schmidhuber, J. (2010). Modeling attacks on physical unclonable functions, In *Proceedings of the 17th acm conference on computer and communications security*. ACM.
Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014). Openid connect core 1.0 incorporating errata set 1. *The OpenID Foundation, specification*.
Sanchez, J. L. C., Bernabe, J. B., & Skarmeta, A. F. (2018). Integration of anonymous credential systems in iot constrained environments. *IEEE Access*, *6*, 4767–4778.
Sarma, A. C., & Girão, J. (2009). Identities in the future internet of things. *Wireless personal communications*, *49*(3), 353–363.
Security assertion markup language (saml) v2.0 technical overview. working draft 10, 9 october 2006. [(Accessed 27 January 2017)]. (2006).
Sem-III, N. (n.d.). Privacy based public key infrastructure (pki) using smart contract in blockchain technology.
Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & infrastructure (identity, data security). *Massachusetts Institute of Technology-Connection Science*, *1*(3), 1–19.
Sociotal [(Accessed 4 May 2018)]. (2015).
Sociotal identitymanager [(Accessed 2 February 2019)]. (n.d.).
Sovrin: A protocol and token for self-sovereign identity and decentralized trust. sovrin foundation. [(Accessed 1 June 2018)]. (2018).
Such, J. M., Espinosa, A., Garcia-Fornes, A., & Botti, V. (2011). Partial identities as a foundation for trust and reputation. *Engineering Applications of Artificial Intelligence*, *24*(7), 1128–1136.
Sukhwani, H., Martıénez, J. M., Chang, X., Trivedi, K. S., & Rindos, A. (2017). Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric), In *2017 ieee 36th symposium on reliable distributed systems (srds)*. IEEE.
Travel identity of the future - white paper. [(Accessed 9 October 2019)]. (2016).
Trnka, M., & Cerny, T. (2016). Identity management of devices in internet of things environment, In *2016 6th international conference on it convergence and security (icitcs)*. IEEE.
Tuyls, P., & Batina, L. (2006). Rfid-tags for anti-counterfeiting, In *Cryptographers' track at the rsa conference*. Springer.
Uniquid: A peer-to-peer trust model for iot protocol primer. [(Accessed 1 June 2018)]. (2017).
Uport contracts for managing identity [(Accessed 4 May 2018)]. (2017).
Uport: A platform for self-sovereign identity. [(Accessed 1 June 2018)]. (2017).
Van Herrewege, A., Katzenbeisser, S., Maes, R., Peeters, R., Sadeghi, A.-R., Verbauwhede, I., & Wachsmann, C. (2012). Reverse fuzzy extractors: Enabling lightweight mutual authentication for puf-enabled rfids, In *International conference on financial cryptography and data security*. Springer.
Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, In *International workshop on open problems in network security*. Springer.
Walker, M. A., Dubey, A., Laszka, A., & Schmidt, D. C. (2017). Platibart: A platform for transactive iot blockchain applications with repeatable testing, In *Proceedings of the 4th workshop on middleware and applications for the internet of things*. ACM.
Web fraud prevention, online authentication & digital identity market guide [(Accessed 18 January 2017)]. (2015).
Web services federation language (ws-federation) version 1.0, oasis [(Accessed 27 January 2017)]. (2003).
Web services trust language (ws-trust)”, microsoft, ibm, opennetwork, layer 7, computer associates, verisign, bea, oblix, reactivity, rsa security, ping identity, verisign, actional [(Accessed 2 February 2019)]. (2005).
What's shibboleth? [(Accessed 2 February 2019)]. (n.d.).
Wood, G. Et al. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1–32.
Wüst, K., & Gervais, A. (2018). Do you need a blockchain?, In *2018 crypto valley conference on blockchain technology (cvcbt)*. IEEE.
Xiong, Z., Zhang, Y., Niyato, D., Wang, P., & Han, Z. (2018). When mobile blockchain meets edge computing. *IEEE Communications Magazine*, *56*(8), 33–39.

Yang, Y., Ding, X., Lu, H., Weng, J., & Zhou, J. (2015). Self-blindable credential: Towards anonymous entity authentication upon resource constrained devices, In *Information security*. Springer.

Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J., & Ko, K. (2017). Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. *IEEE Access*, *6*, 1513–1524.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), e0163477.

Zetter, K. (2011). Diginotar files for bankruptcy in wake of devastating hack. *Wired magazine, September*.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends, In *2017 ieee international congress on big data (bigdata congress)*. IEEE.

Zhu, X., & Badr, Y. (2018). Identity management systems for the internet of things: A survey towards blockchain solutions. *Sensors*, *18*(12), 4215.

Zou, J., Ye, B., Qu, L., Wang, Y., Orgun, M. A., & Li, L. (2018). A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services. *IEEE Transactions on Services Computing*.