Blockchain-Based Identity Management Systems: A Review

Yang Liu[a,b], Debiao He[a,b,], Mohammad S. Obaidat[c,d,e] *Fellow of IEEE and Fellow of SCS*, Neeraj Kumar[f], Muhammad Khurram Khan[g], Kim-Kwang Raymond Choo[h]

[a] *School of Cyber Science and Engineering, Wuhan University, Wuhan, China*
[b] *Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin, China*
[c] *College of Computing and Informatics, University of Sharjah, UAE*
[d] *KASI, University of Jordan, Amman, Jordan*
[e] *University of Science and Technology Beijing, Beijing, China*
[f] *Department of Computer Science and Engineering, Thapar University, Patiala*
[g] *Center of Excellence in Information Assurance, King Saud University, Saudi Arabia*
[h] *Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, USA*

Abstract

Identity management solutions are generally designed to facilitate the management of digital identities and operations such as authentication, and have been widely used in real-world applications. In recent years, there have been attempts to introduce blockchain-based identity management solutions, which allow the user to take over control of his/her own identity (i.e. self-sovereign identity). In this paper, we provide an in-depth review of existing blockchain-based identity management papers and patents published between May 2017 and January 2020. Based on the analysis of the literature, we identify potential research gaps and opportunities, which will hopefully help inform future research agenda.

Keywords: Identity management system, blockchain, blockchain-based identity management, self-sovereign

*Corresponding author

1. Introduction

Digital identity plays an increasingly important role in our interconnected, digitalized society. For example, most of us have a number of digital identities, associated with our workplace, our personal life, and other professional-related activity(ies). This partly contributes to the growing reliance on identity information management (also referred to as identity management, identity management and access control, etc, in the literature), designed to manage and secure our identity information and to provide relevant services. Building on the success of blockchain, there have also been attempts to integrate blockchain in the design of the next generation of identity management solutions[1, 2, 3].

In a typical blockchain-based identity management system, there are a large number of distributed nodes [4]. Such nodes can be utilized to provide distributed storage, reliable access and computation capabilities. The user in such a system acts as a node in the network; thus, allowing the storage of sensitive user data to shift from servers (in the conventional identity management solutions) to user devices / nodes (in the new blockchain-based paradigm). This facilitates self-sovereign identity(SSI), since the users will now have the capability to regain control of their own identity. Consequently, this minimizes various risks inherent of conventional identity management solutions (e.g. user identity abuse) [1, 2, 5].

Given the relatively recent trend in designing blockchain-based identity management solutions, it is not surprising that a number of challenges remain. For example, how can users convince organizations to willingly accept attributes of pseudonymous individuals of uncertain reputation? There are also potentially legal and financial implications, if a transaction is subsequently found to be fraudulent or criminal and the organizations have not conducted their due diligence in verifying the identity of the users involved in the transaction. We observe that self-sovereign identity is a topic that has been explored in the literature [4, 6, 7].

Therefore, in this paper we focus on the study of blockchain-based identity management systems, by reviewing recent state-of-the-art advances on the topic. Specifically, we search for relevant English-language articles and patent documents published between May 2017 and January 2020 on the various academic databases (e.g. ACM Digital Library, IEEE Explore, ScienceDirect, and Springer Link) and Google Scholar, using keywords such as (”blockchain” AND ”identity management”). Of the sixty articles found, we only include 50 articles for discussion in this paper.

In Section 2, we will introduce relevant concepts of identity management and the building blocks in blockchain. Then, in Section 3, we will first introduce three existing blockchain-based identity management systems, prior to reviewing the related literature. In Section 4, we will identify and discuss potential research challenges and opportunities. We conclude this paper in the last section.

2. Preliminaries

2.1. Identity Management

As previously discussed, identity management (IdM) is also known as identity and access management (IAM) in the literature. Broadly speaking, IdM refers to a framework of policies and technologies for ensuring that only authorized individuals can access the associated resources in an organization [8, 9]. IdM is a relatively mature topic, given the large number of standards and frameworks [10], such as the Security Assertion Markup Language (SAML) [11], the Web Services Federation (WS-Fed) [12], the Identity Federation Framework (ID-FF) [13], and the Identity Web Services Framework (ID-WSF) [14]. Examples of IdM criteria include the CoSign Protocol [15], the Open Authentication (OAuth) citehardt2012oauth, and the OpenID Connect (OIDC) [16].

However, as our society becomes more interconnected and digitalized, with a significant increase in the number and types of systems and identities that need to be managed, there is also a need to revisit our conventional IdM paradigms. For example, as discussed earlier, there have been attempts to leverage the characteristics of blockchain (e.g. decentralization, openness, trustworthiness, and security) in the next generation IdM design [17, 18, 19, 20, 21].

2.1.1. Building blocks

For simplicity, let's consider the scenario where a user requests for proof of identity from an identity provider, and the identity provider responds to the token. In this simplistic setting, there is exchange of information between both entities (e.g. real individual or some entities). If the identity providers are separate entities, then this becomes a three-party identity management model of comprising users, identity providers and identity dependents. In such a model, since the identity provider is a separate entity, the identity resource used for authentication only stores in the identity provider, and the identity dependent can only verify the authentication of the user's identity by querying the identity provider. In addition to providing user identities, identity providers should also have identity management, identity reset, identity revoke, and other related functions.

- **User.** Users are the primary enablers of the system, enjoying the various services offered by the service provider and identity provider. Not all users have the same privilege.
- **Identity provider.** Identity provider, the core of the system, is tasked with providing users with identity services (e.g. registration, authentication and management). This entity also provides user authentication.
- **Service provider.** Service provider is an important part of the system, and is mainly responsible for providing services for users (once they are successfully authenticated).

The flow-chart of the system is presented in Fig. 1, and explained below:

- In order to enjoy the desired service, a user must submit a request for an identity from the identity manager. The identity manager then generates

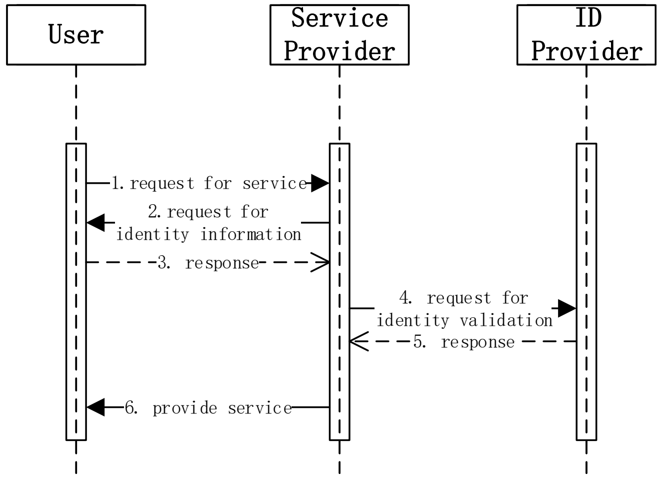

Figure 1: A typical operation of an identity management system

a unique identity based on the information provided by the user and replies to the user.

- The user requests a specific service from the service provider, and the service provider requests for identity information from the user. The user receives the request and replies with the corresponding data.

- The service provider requests the identity provider to verify the validity of user's identity. The identity provider returns the authentication results, and the service provider provides the service based on the received validation results.

2.1.2. Architecture

There are many different identity management systems and architectures in the literature [22, 23, 24, 25, 26], which can be broadly categorized into independent identity management architecture (IMA), federated identity management architecture, and centralized identity management architecture.

- **Independent IMA.** In this architecture, each service provider has its own user identity data. In other words, the identities of different service providers are not interoperable. Although the structure is simple, it is not scalable as the number of service providers increases (e.g. implications for storage requirements at the service providers). Also, it is not practical for the users to remember their identity information for every single service provider, without reusing or recycling their user credentials.

- **Centralized IMA.** The centralized IMA has only one identifier and identity provider in the trusted domain. This means that all service providers in the same trusted domain will share the users' identity. Hence, the identifier should be carefully selected, and the unique identity in the trusted domain is a typical choice.

- **Federated IMA.** The federated IMA establishes a trusted domain and comprises multiple identity providers in the federation. A trusted domain consists of multiple service providers within the federation that recognizes users' identity from other service providers. For example, a U.S.-based academic can choose to sign in to *Research.gov* using either their National Science Foundation (NSF) identity information or their organization credentials.

A comparative summary of the three IMAs is presented in Table 1, where IIMA denotes independent IMA, FIMA denotes federated IMA, and CIMA denotes centralized IMA.

2.1.3. Laws of Identity

We will now revisit the Cameron's law of identity [27], which is used in the later part of this paper.

- **User Control and Consent.** Technical identity systems must only reveal information identifying a user with the user's consent[27].

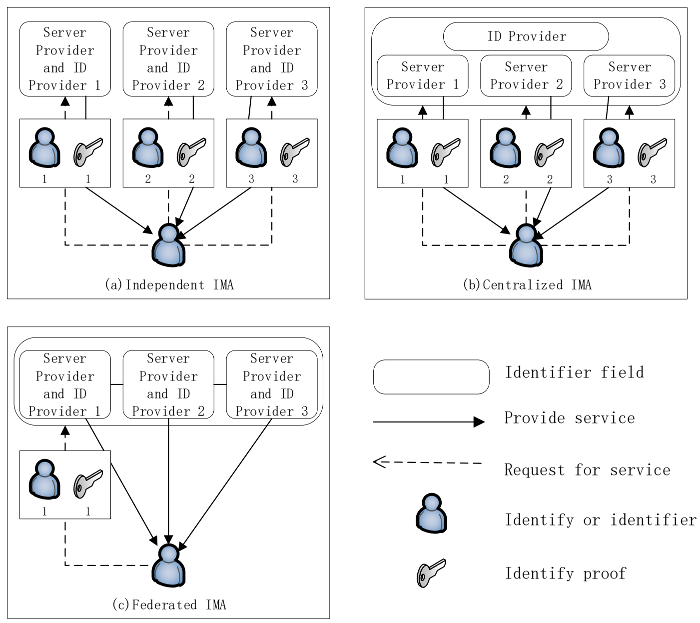

Figure 2: Identity Management Architecture: An Overview

Table 1: Independent, federated, and centralized identity management architectures: A comparative summary

Standard	System Architecture		
	IIMA	CIMA	FIMA
Complexity	Low	Medium	High
Implementation	Simple	Medium	Hard
Scalability	High	Medium	Low
Users' requirements	Significant (e.g. storage)	Light	Medium
SSO	Not supported	Supported	Supported

- **Minimal Disclosure for a Constrained Use.** The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution[27].

- **Justifiable Parties.** Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship[27].

- **Directed Identity.** A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles[27]. Facilitating electronic discovery (e.g. in a civil litigation) and forensic investigations (e.g. in a criminal investigation) [28], while preventing unnecessary release of correlation handles.

- **Pluralism of Operators and Technologies.** A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers[27].

- **Human Integration.** The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks[27].

- **Consistent Experience Across Contexts.** The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies[27].

The Cameron's law of identity plays an important role in the implementation of IdM systems, as its seven laws regulate the behavior of IdM systems. Specifically, the "User Control and Consent" law guarantees the user's control to his/her identity information, the "Minimal Disclosure for a Constrained Use" law guarantees the use of identity information on demand, the "Justifiable

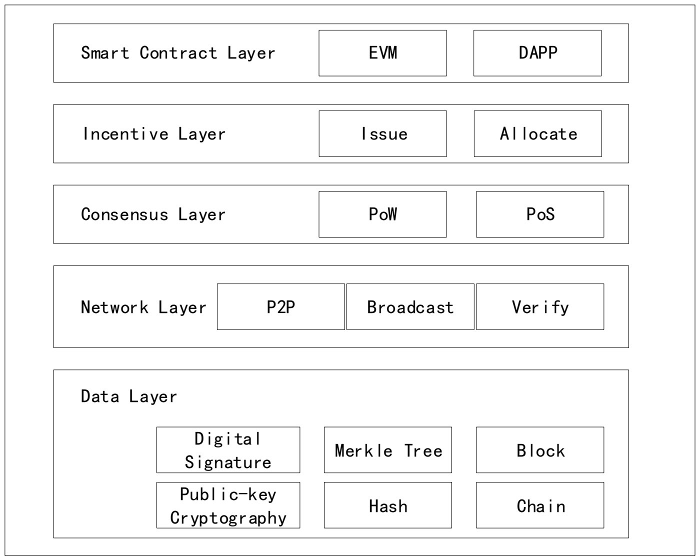

Figure 3: Structure of Ethereum

Parties" law guarantees that the third parties would not access more identity information than needed, the "Directed Identity" law guarantees that the user can connect and access the desired service(s), the "Pluralism of Operators and Technologies" law provides convenience for both developer and cooperator and guarantees the system's scalability, the "Human Integration" law provides some prestore hints like guide and emergency manual for all users, and the "Consistent Experience Across Contexts" law guarantees a certain quality of experience for the users.

2.2. Blockchain

2.2.1. Architecture

Ethereum, the first platform to run Turing complete smart contract, is currently one of the most preferred platforms for blockchain applications. Therefore, we will use Ethereum as an example to explain the blockchain architecture. An overview of Ethereum's structure is presented in Fig. 3.

The data layer is the foundation of all functions, including data storage and security assurance. The data storage is realized through the blocks and the chain. The storage is based on the Merkle tree to ensure data persistence. Security guarantee relies on the data layer's hash function, digital signature and other cryptography technology, which collectively guarantee the security of the account and the transaction. The underlying signature and hash adopt the Elliptic Curve Digital Signature Algorithm (ECDSA) signature algorithm and SHA3 hash algorithm [29, 30].

The network layer is a layer implemented using peer-to-peer (P2P) technology. In a P2P network, there is no centralized server, and each user is a node with server functionality. This layer embodies decentralization and network robustness.

The consensus layer is responsible for network nodes agreeing on transactions and data, and includes two consensus mechanisms. At the beginning, there are few ethers (ETHs), and the proof of work (PoW) consensus mechanism is adopted to encourage the rapid exploration of ETHs. When the number of ETHs is sufficiently large, the proof of stake (PoS) mechanism will be adopted. Such an approach can effectively avoid the partial distribution of a single node.

The incentive layer is responsible for the issuance and distribution of ETHs. ETHs can be used to pay for fuel to run smart contracts, etc, and are produced by mining, with a bonus of some ETHs per block. In the smart contract layer, the running smart contract must have a corresponding virtual machine, for example, ethereum has ethereum virtual machine (EVM) to support the underlying smart contract. At the same time, the decentralized application (DAPP) has an interactive interface, which facilitates the use of smart contracts by users[30, 31].

2.2.2. Merkle Tree

The Merkle tree acts as a representative role in the blockchain, and contains all transactions in a block. Such a container leaves all transaction details in the body, and the relatively light block header can only hold a Merkle root of these transactions and other configured attributes. Fig. 4 presents an overview of the

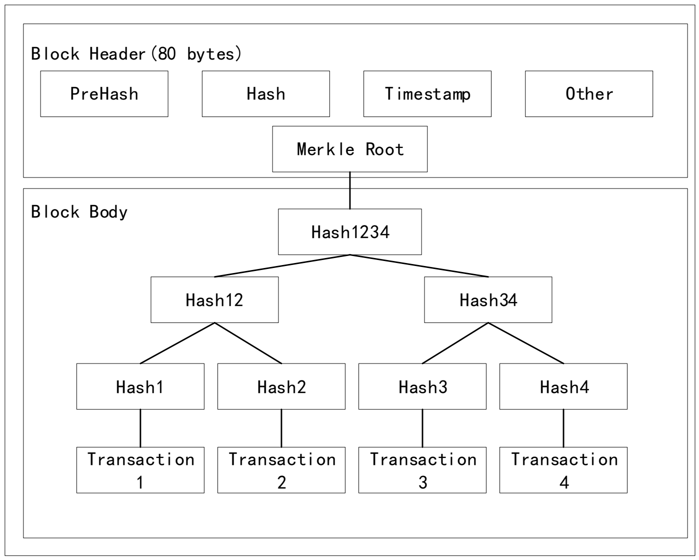

Figure 4: An overview of the Merkle tree in a block

Merkle tree [32, 33].

The Merkle tree includes a root node, a group of internal nodes, and a group of leaf nodes. Each leaf node represents the hash of a corresponding transaction in this block. The value in a internal node is produced by computing the hash of two child nodes, and if there is only one child, its hash will be copied. In this way, root node represents all transactions. The hash of root node will be the identifier of this block, which will participate in either PoW or PoS.

The Merkle tree makes it possible to relieve nodes from the significant storage burden, and new nodes may be a light node to participate in this blockchain. Without transaction details, the space occupied by blockchain data is significantly reduced. Although the heavy node (that holds all blockchain data including transaction details) will still exist, such nodes are minorities.

2.2.3. Smart Contract

A smart contract is a computer protocol designed to digitally facilitate, validate, or enforce the negotiation or performance of a contract. Smart contracts

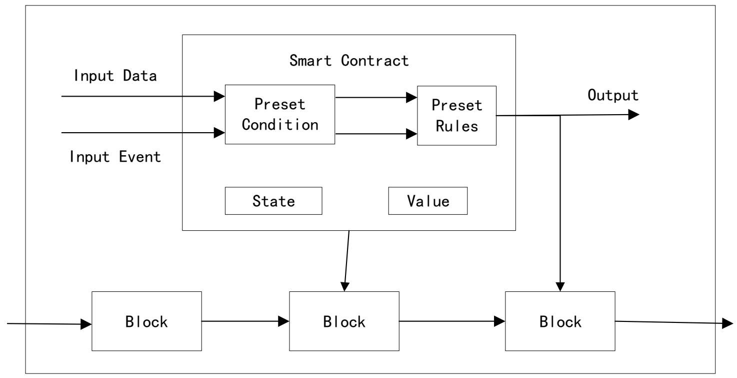

Figure 5: An overview of a smart contract

allow the execution of contract code without third parties – see also Fig. 5.

Smart contract inherits three features of blockchain, namely: tamper-proof, permanent operation and data transparency. The data in blockchain are permanent. Therefore, the deployed smart contract cannot be modified (i.e. contract execution cannot be modified) [34, 35].

The blockchain has a large number of nodes, and some nodes keep a complete data copy. Theoretically, as long as there are nodes, the contract will not stop. The data are transparent, with code and data available to any party at any time. In a public blockchain, data and data processing of smart contracts are publicly available.

Smart contracts are codes deployed on a blockchain which need to be executed on the node's EVM. The EVM is just like the Java virtual machine (JVM), which is a Java runtime environment. EVM interprets smart contracts as running bytecode, which is encapsulated so that the internals of virtual machine are not affected by external networks or other processes. In other words, the smart contract can only make limited invocations to the virtual machine's interface. Smart contracts run on the Ethereum. After obtaining the contract code, each Ethereum node can be carried in the local EVM and get their results. Then, the result will be compared with other nodes, and the result is written to the blockchain after confirmation.

There are a number of challenges underpinning an IdM system, and here we will only focus on the following. First, the level of trust requirement varies between different real application scenarios. Hence, the practical requirements in the design of IdM systems should be taken into consideration.

- **Access and resource.** The system should predefine several levels of access, say for different roles or for different resources. For example, an IdM system in an education institution, the system may include identities such as faculty members (tenured and non-tenured track), administrative staff (i.e. non-faculty members), and students. In such a system, the faculty members have certain roles and accesses (e.g. read/edit access to assignments, examinations and course materials), and similarly a student has different roles and accesses (e.g. to upload the assignment and view the marked assignments and grades). An administrator should also have different accesses, for example, to help students enroll in certain courses or remove a hold on the student's record, after the approval from the relevant faculty member has been obtained.

- **Trust.** There are two key trusted elements, namely: the user trusts the identity provider, and the service provider trusts the identity provider. For example, a corrupted identity provider can potentially access the service, using the user's identity without his/her consent. Such unauthorized access may not be known to the users. Therefore, a developer should consider mitigating such a scenario in the design of the system. The service provider should also ensure that the identity provider will notify them when a new provider is added to the trusted domain. This will allow the service provider to obtain the relevant user attributes from the identity provider, in order to determine whether a user can enjoy its service. With a new identity provider subitem joining the trusted domain, the true decider of access is the identity provider, rather than the service provider. In other words, the trusted relation in system will be at risk. For each trusted relation, there is always a situation that a trusted part can potentially violate the security policy of the other part.

The above discussion reinforces the importance of clearly understanding and stating the types of resources, their access requirements, the trust levels, etc.

3. Blockchain-based Identity Management Systems

In this section, we will review three existing blockchain-based IdM systems.

- **Sovrin.** Sovrin [36] is designed to use digital credentials in the offline world. Sovrin has a self-sovereign identity that does not depend on any centralized authority and cannot be eliminated. Characteristics of Sovrin include governance, scalability and accessibility. More importantly, Sovrin is a worldwide public chain based on Hyperledger that enables design privacy, such as identifying private customers under pseudonyms. It adopts zero-knowledge proof encryption to selectively ensure privacy.

- **uPort.** uPort [37] is a system of self-sovereign identity. It depends on Ethereum, so the essence of the uPort identity is the Ethereum account address on which users interact, and the identity is permanent. uPort table is the smart contract for all uPort identities and is the basis for authentication and offline data access sharing. From the user's perspective, uPort optimizes Ethereum-based applications, so that users interact with real people instead of dealing with hexadecimal addresses.

- **ShoCard.** ShoCard [38] is a blockchain-based IdM system, where users can keep and protect their own digital identities. User's identity information will always be used together with the user's key to ensure privacy. This elimiates the need for a third-party database. ShoCard keeps the authentication code of user data on the blockchain, which can guarantee the legitimacy of personal identity and facilitate third-party verification. ShoCard also issues SFN coins for payments.

Table 2: How do sovrin, uport, shocard relate to Cameron's Laws of Identity [17]?

Law	Item		
	Sovrin	uPort	ShoCard
1.User Control and Consent	Users can choose ID to use and attributes to reveal. Potential to use web of trust to prevent users from deception	Creation and disclosure of uPortIDs are fully controlled by users, and users can prove their ownership. Potential for leakage of attributes in registry.	Users control creation and disclosure of ShoCardIDs. Only party invited by ShoCardIDs' owner can access the attributes, and all attributes will be validated by ShoCard servers.
2.Minimal Disclosure for a Constrained Use	Anonymous credentials based on zero-knowledge proofs guarantee the principle of "least amount of identifying information" disclosure.	There is no need to disclose personal attributes when attaining an uPort identifier.	The trusted identity document is used to bootstrap ShoCardIDs.
3.Justifiable Parties	Only authorized parties and agencies can access the attributes.	Everyone can access the attributes in the registry. Potential for encrypted data to be leaked.	Only party invited by ShoCardIDs' owner can access the attributes, and the ShoCard servers can also access the attributes without invitation.
4.Directed Identity	Supports omnidirectional identifiers.	Supports unidirectional sharing of identifiers between parties.	Supports unidirectional sharing of identifiers between parties.
5.Pluralism of Operators and Technologies	Builds a platform for intermediaries between users and its network, and interface for other identity system is also supported.	Allows for customization of types, although using a specific data format will be preferred.	Parties can parse existing trusted credentials after integrations with ShoCard centralized servers.
6.Human Integration	Not clear about the usability and user understanding of privacy in Sovrin	Mobile application is provided but usability and user understanding of privacy are not clear.	Mobile application is provided but usability and user understanding of privacy are not clear.
7.Consistent Experience Across Contexts	Hard to say, as it depends whether Sovrin will choose multiple platforms or not.	Users interact with mobile application and QR code scanning is accessible.	Users interact with mobile application and QR code scanning is accessible.

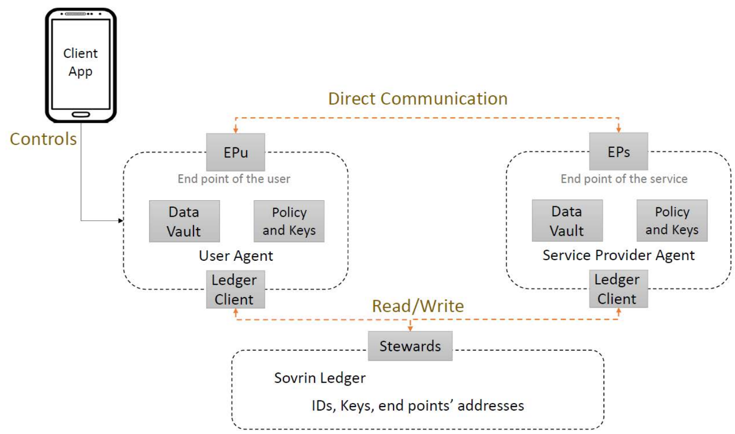

Figure 6: Sovrin architecture [39]

We will now use Cameron's law of identity [27] to help us compare Sovrin, uPort, and ShoCard – see Table 2. The structures of Sovrin, uPort, and ShoCard are respectively shown in Fig 6, Fig 7 and Fig 8.

There are clearly many other blockchain-based IdM systems, including those proposed in the literature.

In the remaining of this section, we will review the existing literature.

3.1. Authentication

The distributed nature of blockchain-based IdM systems shifts the paradigm of having a central storage location to peer node storage, as previously discussed. There are many other defining features and requirements of blockchain-based IdM systems, including those surveyed by Nabi et al. [40]. For example, in addition to distributed storage, blockchain-based IdM systems also support improved efficiency and enhanced security [41]. There have also been attempts to introduce blockchain-based IdM systems to include Internet of Things (IoT) device and edge computing [44, 42]. Mell et al. [45] presented a federated IdM system, where smart contract is used to enable authentication on the blockchain. In their system, there is no credential service provider. The Horcrux protocol [46] is designed to facilitate user-controlled biometric authentication.

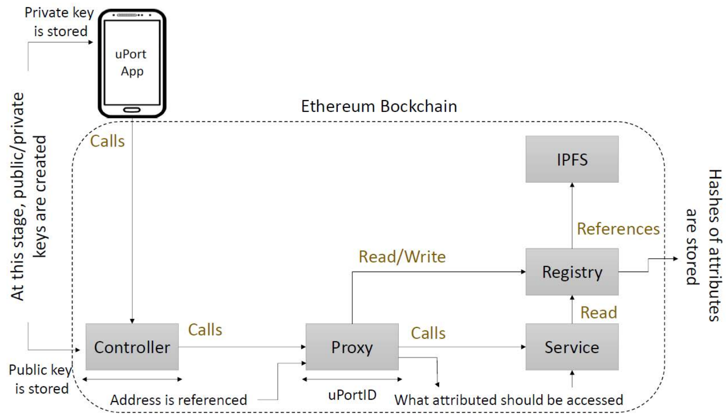

Figure 7: uPort architecture [39]

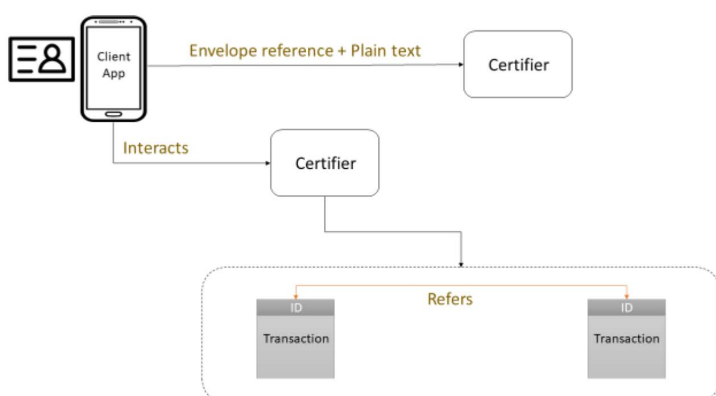

Figure 8: ShoCard architecture [39]

Table 3: Comparative summary of existing blockchain-based works

	Works
Authentication	Nabi et al. [40], Mikula et al. [41], Pularikkal et al. [42], Lin et al. [43], Ren et al. [44], Mell et al. [45], Othman et al. [46], Ebrahimi [47], HYUN et al. [48], Madisetti et al. [49], Zheng Zhao et al. [50], Arshad Jamal et al. [51], Oluyemi Amujo et al. [52], Pengfei Fan et al. [53], Saravanan Raju et al. [54], Tom Hamer et al. [55]
Privacy	Santos et al. [56], Faber et al. [57], Borse et al. [58], Kassem et al. [39], Nágy et al. [59], Liang et al. [60], Gao et al. [61], Wack et al. [62], Madisetti et al. [63], CHARI et al. [64, 65], Saravanan Raju et al. [54], Yue Zheng et al. [66], Martin Schanzenbach et al. [67], Jeonghyuk Lee et al. [68]
Trust	Baars et al. [69], Manohar et al. [9], Grüner et al. [70], Takemiya et al. [71], Jim St. et al. [72],

Table 4: Features in existing schemes and patents: A comparative summary

works	SC	Scalability	ZKP	Time
Grüner et al. [70]		√		2018
Abraham et al. [73]		√		2018
Othman et al. [46]		√		2018
Soltani et al. [74]		√		2018
Lesavre et al. [20]	√		√	2019
Borse et al. [58]	√		√	2019
Kassem et al. [39]	√			2019
Stokkink et al.[75]			√	2018
Mell et al. [45]	√			2019
Ren et al. [44]	√			2019
Lin et al. [43]	√	√		2018
CHARI et al. [49]	√		√	2018
Mikula et al. [41]	√			2018
Westerkamp et al. [76]	√			2019
Faber et al. [57]	√			2019
Kikitamara et al. [77]	√	√		2017
Baars et al. [69]	√			2016
Santos et al. [56]	√			2018
Liang et al. [60]		√		2017
Takemiya et al. [71]		√		2018
Zheng Zhao et al. [50]	√	√		—-
Jim St. et al. [72]		√		2020
Arshad Jamal et al. [51]		√		2019
Yue Zheng et al. [66]		√		2019
Oluyemi Amujo et al. [52]	√	√		2019
Pengfei Fan et al. [53]	√			2019
Saravanan Raju et al. [54]	√			2017
Tom Hamer et al. [55]		√		2019
Martin Schanzenbach et al. [67]		√	√	2018
Jeonghyuk Lee et al. [68]			√	2019

In settings where users are anonymous, IdM systems need to be able to adequately authenticate and authorize these unknown identities [78]. For example, Zhao et al. [50] proposed a self-sovereign IdM system and a reputation model, both for attribute reputation. Other approaches include those of Jamal et al. [51] and Amujo et al. [52]. The latter system is designed to mitigate Sybil attacks and facilitate identity attribute disclosure. In a separate work, Fan et al. [53] introduced an identity security authentication system based on blockchain. The system is designed to achieve fault-tolerance and significantly increase the hardness of compromising half of the nodes in the network.

Hamer et al. [55] combined both cancelable biometrics protocol and W3C verifiable claims in their proposed scheme, which is designed to achieve self-sovereign identity. In addition to non-linkable identification and privacy preservation, double enrollment is disallowed in this system. Raju et al. [54] considered both anonymity and attribute in their proposed blockchain-based privacy-enhancing system, which also supports end-to-end management.

Pass-closed undirected graph validation can also be used in IdM systems to facilitate authorization, as demonstrated in the encrypted member authentication scheme of [43]. In the scheme, it comprises a new transitively closed undirected graph validation mechanism that only requires the appearance of node signatures (e.g. certificates used to identity nodes). The trapdoor hash function makes it sufficiently lightweight for the signer to effectively update the certificate, as there is no need to re-sign the node. The scheme also allows the dynamic adding and removing of nodes and edges.

There are also a number of patents on blockchain-based IdM systems for authentication [48, 49]. For example, Ebrahimi [47] designed a service using blockchain to provide certifying transactions between devices. This scheme allows devices to transfer related public key and signature. In this way, the device could receive data from others.

Table 5: Examples of privacy-preserving schemes

works	privacy criteria	remote admin	anonymity	data minimization	user empowering
Grüner et al. [70]		√			√
Abraham et al. [73]				√	√
Othman et al. [46]	√	√			√
Soltani et al. [74]			√	√	√
Lesavre et al. [20]	√		√		√
Borse et al. [58]			√		√
Kassem et al. [39]	√				√
Stokkink et al.[75]	√			√	√
Mell et al. [45]			√		√
Ren et al. [44]		√			
Lin et al. [43]	√		√		√
CHARI et al. [49]	√	√			
Mikula et al. [41]			√		
Westerkamp et al. [76]		√	√		√
Faber et al. [57]		√	√		
Kikitamara et al. [77]	√	√	√	√	√
Baars et al. [69]			√	√	√
Santos et al. [56]	√	√	√	√	
Liang et al. [60]		√	√		
Takemiya et al. [71]		√			√
Zheng Zhao et al. [50]			√	√	√
Jim St. et al. [72]					√
Arshad Jamal et al. [51]					√
Yue Zheng et al. [66]	√		√		√
Oluyemi Amujo et al. [52]		√	√		√
Pengfei Fan et al. [53]		√	√		
Saravanan Raju et al. [54]	√		√		
Tom Hamer et al. [55]	√	√	√		√
Martin Schanzenbach et al. [67]		√			√
Jeonghyuk Lee et al. [68]			√	√	√

3.2. Privacy

There have been a number of privacy-preserving schemes proposed in the literature, such as those presented in Table 5. For example, Faber et al. [57] proposed a blockchain-based personal data and identity management system, which is designed to facilitate transfer of control over personal data to edge users. The emphasis is on providing transparency and control over the use of personal data.

To achieve self-sovereign identity, zero-knowledge proof is be a viable approach, such as the approach presented by Borse et al. [58]. The scheme of Borse et al. [58] allows one to achieve selective anonymity for the user's properties on the blockchain. The IdM system is a scheme with zero-knowledge proof of membership combined with the Pedersen commitment, and the zero-knowledge proof is used to keep details secret from the public ledger. Thus, this creates a secure self-sovereign identity system. In a separate work, Chari et al.[65] designed the ownership of assets based on collaborative strenthened by commitment and zero-knowledge proofs. Other approaches include those of Kassem et al. [39], who proposed a smart contract-based identity management system. The latter is designed to overcome the limitations of existing decentralized system and mitigate security threats by leveraging Blockchain's decentralized nature. In another separate work, a user-centric health data sharing solution was presented in [60]. The solution also includes a proof of integrity to guarantee data integrity.

Anonymity and unlinkability are two other significant design considerations, as demonstrated in the schemes of Zheng et al. [66] and Jeonghyuk Lee et al. [68]. There have also been efforts to design approaches based on attribute-based encryption (ABE). For example, Schanzenbach et al. [67] presented an architecture, which allows a user to reclaim digital identities in a sharing identity attribute approach. The user is able to selectively authorize and the attributes are encrypted using ABE. They also proposed a system with type-1 pairings in ABE. Besides, a number of researchers have leveraged biometrics to design blockchain-based IdM systems. For example, Gao et al. [61] proposed an IdM framework, which integrates biometric authentication and trusted computing. Other hybrid approaches include those of [59].

In addition to academic articles, there have been a number of patent applications filed [63, 64] . For example, Wack et al. [62] designed a method to provide a cryptographic platform for information exchange. A comparative summary is presented in Table 5.

3.3. Trust

Trust is important in the design of IdM systems. Existing literature has focused on trust, consensus, etc. For example, Baars et al. [69] created a new DIMS design solution based on blockchain. In this scheme, each person needs to implement and customize modular building blocks based on their own trust needs. Tables 6 and 7 summarize some of these existing approaches.

4. Discussion

While identity management has been extensively studied and adopted in practice, a number of limitations and challenges remain [79]. While blockchain may be able to mitigate some of these limitations, there are a number of issues and implications remaining.

4.1. Identity-related challenges

There is potential risk that identity information kept at the user's side may be subject to risk and exploitation. Examples include the following:

- **Identity "wallet" leakage.** If the identity "wallet" is successfully compromised, then information could be leaked or useful information about the user could be obtained. Consequently, such leaked information can be used to facilitate other nefarious activities.

- **Identity changes.** In reality, the user's identity is not permanent and can be changed. Traditional, centralized identity providers can revoke or renew identity status in a timely manner, for example during promotions, or

Table 6: Examples of trust-based systems

Solution	Items			
	Development	Description	Weakness	Strength
Borse et al. [58]	simulation	a system for self-sovereign identity combining Pedersen's commitment to Interval membership's zero-knowledge protocol to provide privacy for certain attributes of a user's identity	economic cost for large-scale implementation	commitment and zero-knowledge protocol, the selective anonymity of the user's properties on the blockchain
Faber et al. [57]	scheme	The Blockchain-based Personal Data and Identity Management System(BPDIMS) is a human-centered and GDPR based personal data and identity management system	No a detailed specification that describes various interactions between different stakeholders of the system in an unambiguous manner	provide transparency and control over the use of users' personal data
Kikitamara et al. [77]	scheme	a system for self-sovereign identity using hybrid digital identity	the possibility for those sectors with great scale need to be discussed, limitations and uncertainties in advanced authentication mechanism	mixture of federated and user-centric identities, extensibility, Hybrid IT and interoperability
Ren et al. [44]	simulation	an identity management portfolio access control mechanism based on blockchain and edge computing with self-sovereign	no key agreement protocol, performance need to be optimized	bind the generated implicit certificate to identity, secure communication in the edge of the resource-constrained devices
Mell et al. [45]	scheme	a Federated identity management system to enable users to perform RP authentication and property transfer directly without the involvement of third parties	narrow available range(suitable for a large organization)	authentication is only through RP communication by user without third parties, no need to maintain a public key infrastructure
Lin et al. [43]	simulation	encrypted member authentication scheme to support blockchain-based identity management system	requestors may be utilized to trick other users by receiving several certificates of one node	more effective in the ability to dynamically add or remove nodes and edges, demonstrate the security of proposed TCUGA in the standard model and evaluate its performance to demonstrate its feasibility against BIMS

Table 7: Examples of trust-based systems (Cont'd)

Solution	Items			
	Development	Description	Weakness	Strength
Baars et al. [69]	product	a new DIMS design solution based on blockchain after investigating and combining the principle of self-sovereign identity with the design motivation of IRMA project	legislation questions arose when discussing especially the exchange of more sensitive data attributes, scalability problem	decentralized exchange, centralized issuance, no storage of sensitive information on blockchain, no address reuse, identity verification of acquirers
Kassem et al. [39]	simulation	a smart contract-based identity management system called DNSIdM that enables users to maintain their identities associated with certain attributes, accomplishing the self-sovereign concept	the facilitators and barriers for blockchain-based identity management services in developing compliance with digital standards need to be identified	overcome the limitations and weaknesses of identity attributes: persistence, request, and verification, amicable overhead and security
Mikula et al. [41]	simulation	a system for identity and access management using blockchain technology to support authentication and authorization of entities in a digital system	poor scalability, performance doesn't meet requirement	A simulation based on Hyperledger Fabric was made, achieved in a decentralized, efficient, and secure manner
Nágy et al. [59]	scheme	a hybrid solution to deal with issues caused by trusted centralize organizations. The solution is a blockchain gateway solution, which supports legal compliance and traditional Identity Management features that require strong authentication, and it is a general blockchain Identity Framework too	the incentive misalignment between Subject, Authentication agent, and Authorization agent caused by conflicting interests and responsibilities	a secure and privacy friendly middle ground between the blockchain and the mundane world using a hybrid solution
Santos et al. [56]	simulation	a Blockchain system based on Hyperledger Fabric is suitable for managing patients identity in Healthcare	malicious parties may use potential flaws to threat security of the Healthcare industry	data transparency , immutability of data and decentralization.

driver license suspension. However, in blockchain-based identity system, due to the persistence of blockchain and the SSI, any modification of user identity information requires user participation. Hence, identity change can be challenging to carry out.

4.2. Cost Implications

There are also cost implications associated with blockchain-based solutions.

- **Infrastructure.** SSI is relatively new and may not be easily supported by existing IdM systems and their supporting infrastructure. Hence, there will be cost implications associated with infrastructure upgrades. For example, user passwords will need to be replaced by certificates and the authentication mechanism dependencies within the service provider will need to be improved. Clearly, upgrading of equipment and procedures is only part of the cost. Other costs include staff training and equipment maintenance. To minimize the costs, infrastructure upgrades can be gradual.

- **Key management.** In bitcoin-based system, losing the private key will result in the lost of the associated asset (e.g. bitcoins). Unlike a password-based system, there is no mechanism to reset the forgotten password. Hence, one viable approach is to integrate such a reset feature or outsource key management to a third-party. However, private key delegation management contradicts the concept of SSI. To support SSI, there are significant maintenance cost implications. We can also use multi-party key management, such as that of [80].

5. Conclusion

In this paper, we provided an in-depth review of blockchain-based identity management systems.

As part of the review, we identified a number of challenges, such as those related to block data storage. For example, the user's storage requirement will increase with the increase of number of users and the subscribed services. Hence, *how do we design a scalable mechanism that also takes into consideration the differing storage capability of different users?* Another challenge is associated with the de-authorization classification in blockchain. Some nodes can participate in book-keeping while others can only view the block data. This can potentially result in the boundary division of the chain, due to the existence of node identity.

Blockchain-based IdM systems overcome a number of limitations inherent of conventional IdM systems. Such blockchain-based systems might be described as an identity revolution. For example, the user becomes the owner of the identity, and it does not require users to sacrifice safety for convenience. In addition, one potential future extension is to adopt some unique factor in reality as a mainly evidence for account reset.

Acknowledgements

We thank the anonymous reviewers for their invaluable feedback. The work was supported by the National Natural Science Foundation of China (Nos. 61932016, 61972294) and the Opening Project of Guangxi Key Laboratory of Trusted Software (No. kx202001). Prof. Obaidat is supported by the Chinese Ministry of Education Distinguished Possessor Grant (No. MS2017BJKJ003). K.-K. R. Choo was supported in part by the Cloud Technology Endowed Professorship and National Science Foundation CREST (No. HRD-1736209).

References

References

[1] S. El Haddouti, M. D. E.-C. El Kettani, Analysis of identity management systems using blockchain technology, in: 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), IEEE, 2019, pp. 1–7.

[2] M. Kuperberg, Blockchain-based identity management: A survey from the enterprise and ecosystem perspective, IEEE Transactions on Engineering Management (2019).

[3] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, K.-K. R. Choo, Best: Blockchain-based secure energy trading in sdn-enabled intelligent transportation system, Computers and Security 85 (2019) 288 – 299.

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

[5] A. Jindal, G. S. Aujla, N. Kumar, Survivor: A blockchain based edge-as-a-service framework for secure energy trading in sdn-enabled vehicle-to-grid environment, Computer Networks 153 (2019) 36 – 48.

[6] M. Schäffner, Analysis and evaluation of blockchain-based self-sovereign identity systems.

[7] X. Zhu, Y. Badr, A survey on blockchain-based identity management systems for the internet of things, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1568–1573.

[8] F. Stroud, What is identity and access management (iam)? webopedia definition, `https://www.webopedia.com/TERM/I/iam-identity-and-access-management.html`, retrieved 27 February 2019.

[9] A. Manohar, J. Briggs, Identity management in the age of blockchain 3.0 (2018).

[10] X. ShangGuan, Research on the international identity management and privacy standards, information technology and standardization (1) (2012) 29–34.

[11] J. Hughes, S. Cantor, J. Hodges, F. Hirsch, P. Mishra, R. Philpott, E. Maler, Profiles for the oasis security assertion markup language (saml) v2. 0, OASIS standard (2005).

[12] M. Goodner, A. Nadalin, Web services federation language (ws-federation) version 1.2, OASIS Web Services Federation (WSFED) TC (2009).

[13] S. Cantor, J. Hodges, J. Kemp, P. Thompson, Liberty id-ff architecture overview, Wason, Thomas (Herausgeber): Liberty Alliance Project Version 1 (2003).

[14] C. P. Cahill, G. Whitehead, H. J. Yang, Liberty id-wsf provisioning service specification (2007).

[15] Cosign: Secure, intra-institutional web authenticationhttp://weblogin.org/.

[16] Openid connect — openidhttps://openid.net/connect/.

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

[18] R. Zambrano, A. Young, S. Velhurst, Connecting refugees to aid through blockchain-enabled id management: World food programme's building blocks (2018).

[19] S. Wadhwa, Decentralized digital identity management using blockchain and its implication on public sector, Ph.D. thesis, Dublin Business School (2019).

[20] L. Lesavre, P. Varin, P. Mell, M. Davidson, J. Shook, A taxonomic approach to understanding emerging blockchain identity management sys-

tems (draft), Tech. rep., National Institute of Standards and Technology (2019).

[21] A. Grüner, A. Mühle, C. Meinel, On the relevance of blockchain in identity management, arXiv preprint arXiv:1807.08136 (2018).

[22] B. Mohamad, H. A. Bakar, A. R. Ismail, H. Halim, R. Bidin, Corporate identity management (cim) in malaysian higher education sector: Developing a conceptual model, International Review of Management and Marketing 6 (7S) (2016) 175–180.

[23] M. Rowden, Identity: Transforming performance through integrated identity management (2017).

[24] J. D. Caldwell, Emotional labor and identity management among hiv counselors and testers (2016).

[25] L. V. Martinez, S. Ting-Toomey, T. Dorjee, Identity management and relational culture in interfaith marital communication in a united states context: A qualitative study, Journal of Intercultural Communication Research 45 (6) (2016) 1–23.

[26] U. Pavalanathan, C. M. De, Identity management and mental health discourse in social media (2015).

[27] K. Cameron, The laws of identity, Microsoft Corp 12 (2005) 8–11.

[28] B. Manral, G. Somani, K. R. Choo, M. Conti, M. S. Gaur, A systematic survey on cloud forensics challenges, solutions, and future directions, ACM Comput. Surv. 52 (6) (2020) 124:1–124:38.

[29] Q. Feng, D. He, S. Zeadally, M. K. Khan, N. Kumar, A survey on privacy protection in blockchain system, Journal of Network and Computer Applications 126 (2019) 45–58.

[30] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, A. Y. Zomaya, Blockchain for smart communities: Applications, challenges and

opportunities, Journal of Network and Computer Applications 144 (2019) 13 – 48.

[31] I. Mistry, S. Tanwar, S. Tyagi, N. Kumar, Blockchain for 5g-enabled iot for industrial automation: A systematic review, solutions, and challenges, Mechanical Systems and Signal Processing 135 (2020) 106382.

[32] C. Lin, D. He, X. Huang, K. K. R. Choo, A. V. Vasilakos, Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, Journal of network and computer applications 116 (1) (2018) 42–52.

[33] J. Wang, L. Wu, K.-K. R. Choo, D. He, Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure, IEEE Transactions on Industrial Informatics 16 (3) (2020) 1984–1992.

[34] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, K.-K. R. Choo, Homechain: A blockchain-based secure mutual authentication system for smart homes, IEEE Internet of Things Journal 7 (2) (2020) 818–829.

[35] Y. Zhang, D. He, K.-K. R. Choo, Bads: Blockchain-based architecture for data sharing with abs and cp-abe in iot, Wireless Communications and Mobile Computing 2018 (2018) 1–9.

[36] A. Tobin, D. Reed, The inevitable rise of self-sovereign identity, The Sovrin Foundation 29 (2016).

[37] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, M. Sena, Uport: A platform for self-sovereign identity, URL: https://whitepaper. uport. me/uPort_ whitepaper_DRAFT20170221. pdf (2017).

[38] Shocard: The premier blockchain-based mobile identity platform`https://shocard.com.html`.

[39] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, K. Dahal, Dns-idm: A blockchain identity management system to secure personal data sharing in a network, Applied Sciences 9 (15) (2019) 2953.

[40] A. G. Nabi, Comparative study on identity management methods using blockchain, University of Zurich, Department of Informatics (IFI). https://files. ifi. uzh. ch/CSG/staff/Rafati/ID% 20Management% 20using% 20BC-Atif-VA. pdf (2017).

[41] T. Mikula, R. H. Jacobsen, Identity and access management with blockchain in electronic healthcare records, in: 2018 21st Euromicro Conference on Digital System Design (DSD), IEEE, 2018, pp. 699–706.

[42] B. Pularikkal, S. Patil, S. Anantha, S. Chakraborty, Blockchain based wi-fi onboarding simplification, identity management and device profiling for iot devices in enterprise networks (2018).

[43] C. Lin, D. He, X. Huang, M. K. Khan, K.-K. R. Choo, A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems, IEEE Access 6 (2018) 28203–28212.

[44] Y. Ren, F. Zhu, J. Qi, J. Wang, A. K. Sangaiah, Identity management and access control based on blockchain under edge computing for the industrial internet of things, Applied Sciences 9 (10) (2019) 2058.

[45] P. Mell, J. Dray, J. Shook, Smart contract federated identity management without third party authentication services, arXiv preprint arXiv:1906.11057 (2019).

[46] A. Othman, J. Callahan, The horcrux protocol: a method for decentralized biometric-based self-sovereign identity, in: 2018 International Joint Conference on Neural Networks (IJCNN), IEEE, 2018, pp. 1–7.

[47] A. Ebrahimi, Identity management service using a blockchain providing certifying transactions between devices, uS Patent 9,722,790 (Aug. 1 2017).

[48] N. S. Hyun, H. S. Chae, S. H. Kim, K. J. Kim, M. S. Yang, Y. M. Seo, Blockchain-based digital identity management method, uS Patent App. 15/913,456 (Oct. 11 2018).

[49] V. K. Madisetti, A. Bahga, Method and system for blockchain-based combined identity, ownership, integrity and custody management, uS Patent App. 16/118,599 (Dec. 27 2018).

[50] Z. Zhao, Y. Liu, A blockchain based identity management system considering reputation, URL: http://faculty.neu.edu.cn/swc/liuyuan/paper/iccse1.pdf.

[51] A. Jamal, R. A. A. Helmi, A. S. N. Syahirah, M.-A. Fatima, Blockchain-based identity verification system, in: 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), IEEE, 2019, pp. 253–257.

[52] O. Amujo, C. U. Ebelogu, E. O. Agu, M. Hammawa, Development of a national identity management system using blockchain technology (2019).

[53] P. Fan, Y. Liu, J. Zhu, X. Fan, L. Wen, Identity management security authentication based on blockchain technologies, URL: http://ijns.femto.com.tw/contents/ijns-v21-n6/ijns-2019-v21-n6-p912-917.pdf (2019).

[54] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, J. S. Deogun, Identity management using blockchain for cognitive cellular networks, in: 2017 IEEE International Conference on Communications (ICC), IEEE, 2017, pp. 1–6.

[55] T. Hamer, K. Taylor, K. S. Ng, A. Tiu, Private digital identity on blockchain (2019).

[56] J. P. N. d. Santos, Identity management in healthcare using blockchain technology, Master's thesis, Universidade de Évora (2018).

[57] B. Faber, G. C. Michelet, N. Weidmann, R. R. Mukkamala, R. Vatrapu, Bpdims: A blockchain-based personal data and identity management system, in: Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019.

[58] Y. Borse, A. Chawathe, D. Patole, P. Ahirao, Anonymity: A secure identity management using smart contracts, Available at SSRN 3352370 (2019).

[59] K. Nyante, Secure identity management on the blockchain, Master's thesis, University of Twente (2018).

[60] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, in: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2017, pp. 1–5.

[61] Z. Gao, L. Xu, G. Turner, B. Patel, N. Diallo, L. Chen, W. Shi, Blockchain-based identity management with mobile device, in: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, ACM, 2018, pp. 66–70.

[62] C. J. Wack, E. M. Scheidt, Identity management distributed ledger and blockchain, uS Patent App. 15/703,433 (Sep. 20 2018).

[63] V. K. Madisetti, A. Bahga, Method and system for identity and access management for blockchain interoperability, uS Patent App. 15/830,099 (Oct. 4 2018).

[64] S. Chari, H. Gunasinghe, A. Kundu, K. K. Singh, D. Su, Protection of confidentiality, privacy and financial fairness in a blockchain based decentralized identity management system, uS Patent App. 15/839,117 (Jun. 13 2019).

[65] S. Chari, H. Gunasinghe, H. M. Krawczyk, A. Kundu, K. K. Singh, D. Su, Protection of confidentiality, privacy and ownership assurance in

a blockchain based decentralized identity management system, uS Patent App. 15/824,405 (May 30 2019).

[66] Y. Zheng, Y. Li, Z. Wang, C. Deng, Y. Luo, Y. Li, J. Ding, Blockchain-based privacy protection unified identity authentication, in: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), IEEE, 2019, pp. 42–49.

[67] M. Schanzenbach, G. Bramm, J. Schütte, reclaimid: Secure, self-sovereign identities using name systems and attribute-based encryption, in: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 946–957.

[68] J. Leea, J. Hwangc, J. Choib, H. Oha, J. Kimb, Sims: Self-sovereign identity management system with preserving privacy in blockchain, URL: https://eprint.iacr.org/2019/1241.pdf (2019).

[69] D. Baars, Towards self-sovereign identity using blockchain technology, Master's thesis, University of Twente (2016).

[70] A. Grüner, A. Mühle, T. Gayvoronskaya, C. Meinel, A quantifiable trust model for blockchain-based identity management, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1475–1482.

[71] M. Takemiya, B. Vanieiev, Sora identity: Secure, digital identity on the blockchain, in: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Vol. 2, IEEE, 2018, pp. 582–587.

[72] J. StClair, A. Ingraham, D. King, M. B. Marchant, F. C. McCraw, D. Met-

calf, J. Squeo, Blockchain, interoperability, and self-sovereign identity: Trust me, it's my data, Blockchain in Healthcare Today (2020).

[73] A. Abraham, K. Theuermann, E. Kirchengast, Qualified eid derivation into a distributed ledger based idm system, in: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 1406–1412.

[74] R. Soltani, U. T. Nguyen, A. An, A new approach to client onboarding using self-sovereign identity and distributed ledger, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1129–1136.

[75] Q. Stokkink, J. Pouwelse, Deployment of a blockchain-based self-sovereign identity, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1336–1342.

[76] M. Westerkamp, S. Göndör, A. Küpper, Tawki: Towards self-sovereign social communication, in: Proc. IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). IEEE, 2019.

[77] S. Kikitamara, M. van Eekelen, D. I. J.-P. Doomernik, Digital identity management on blockchain for open model energy system, Unpublished Masters thesis–Information Science (2017).

[78] V. Benjumea, S. G. Choi, J. Lopez, M. Yung, Anonymity 2.0–x. 509 extensions supporting privacy-friendly authentication, in: International Conference on Cryptology and Network Security, Springer, 2007, pp. 265–281.

[79] R. Dhamija, L. Dusseault, The seven flaws of identity management: Usability and security challenges, IEEE Security & Privacy 6 (2) (2008) 24–29.

[80] Q. Feng, D. He, Z. Liu, D. Wang, K.-K. R. Choo, Multi-party signing protocol for the identity-based signature scheme in ieee p1363 standard, IET Information Security 1 (99) (2020) 1–10, dOI: 10.1049/iet-ifs.2019.0559.