THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 21, Number 1/2020, pp. 45–52

IDENTITY MANAGEMENT ON BLOCKCHAIN – PRIVACY AND SECURITY ASPECTS

Andreea-Elena PANAIT[1], Ruxandra F. OLIMID[1,2,3], Alin STEFANESCU[1,2]

[1] University of Bucharest, Department of Computer Science, Romania
[2] The Research Institute of the University of Bucharest (ICUB), Romania
[3] NTNU – Norwegian University of Science and Technology, Department of Information Security and Communication Technology, Trondheim, Norway
Corresponding author: Andreea-Elena PANAIT, E-mail: andreea-elena.panait@drd.unibuc.ro

Abstract. In the last years, identity management solutions on blockchain were proposed as a possible solution to digital identity management problems. However, they are still at an early stage, and further research needs to be done to conclude whether identity systems could benefit from the use of blockchain or not. Motivated by this, we investigate blockchain-based identity management solutions to give the reader an overview of the current status and provide a better understanding of the pros and cons of using such solutions. We analyze ten of the most known implementations, with a focus on privacy and security aspects. Finally, we identify existing challenges and give new research directions.

***Key words**:* digital identity, identity management, blockchain, self-sovereign identity.

1. INTRODUCTION

1.1. Motivation and contribution

Identity management became one of the major problems in today's world. Because of the continuous technological development, specifically the development of 5G and the Internet of Things (IoT), the number of entities in the digital world had significantly increased. In consequence, it is a high demand to digitally identify not only individuals, but also organizations, services, applications, and devices in an efficient and interoperable (or ideally, universal) way. In this context, the privacy and security aspects are important. Identity management solutions based on blockchain technology were proposed as a possible solution to solve these needs but are still at an early stage. While some tend to erroneously consider blockchain a general solution, there have been a lot of discussions lately about whether identity systems could benefit from blockchain or not. Motivated by this, we investigate identity management solutions on blockchain.

The goal of the paper is to provide an overview of the current status in the field and a better understanding of the pros and cons of using such solutions. We analyze ten of the most known implementations, with a focus on privacy and security aspects. The paper discusses the limitations and weaknesses of blockchain-based identity management and identifies challenges and new research directions.

The paper is organized as follows. The next subsection introduces the related work. Section 2 gives the necessary background in digital identity and blockchain. Section 3 presents identity management on the blockchain with a focus on particularities, classification, and investigation of existing implementations. Section 4 discusses the necessities and challenges of blockchain-based identity management, highlighting open research questions. Section 5 concludes the paper.

1.2. Related work

Recently, a great amount of work has been done for designing identity management on blockchain and closely related fields, such as public-key infrastructure [1, 2]. Mühle et al. give an overview of self-sovereign identity, with a focus on general architecture, authentication solutions to link a user to his digital identifier, and verifiable claims [3]. Dunphy et al. discuss the role of the distributed ledger technology in the context of digital identity, identify challenges, and propose future research directions [4]. Bokkem et al. [5] explore the self-sovereign solutions available and discuss their implementations with respect to the principles previously described by C. Allen [6]. Dunphy and Petitcolas offer a view on the distributed ledger technology-based identity management and evaluate three system proposals (*uPort*, *ShoCard,* and *Sovrin*) [7]. Roos explains the design of some of the most promising identity management solutions that use blockchain and evaluates whether the solutions fulfill their goals or not [8]. Many other solutions have been published in the last years. Some will be discussed in more detail in Subsection 3.2.

2. BACKGROUND

2.1. Digital identity

A *digital identity* is a representation of an actual entity (e.g., a person, a device, an organization) in the digital world. It is not exhaustive, and it can vary depending on the specific domain it is used for. The *attributes* of a digital identity are e.g., physical characteristics of a person, address, e-mail, phone number [9]. Similar to attributes of an actual identity, some of them might change over time. From a technical point of view, credentials (username and password), security tokens, or transaction history can also be used for identification. On the other hand, individuals can also be uniquely identified by single-use identifiers or pseudonymous especially created for different purposes or specific intervals of time [10, 11].

A *digital identity management model* can be traditionally interpreted as a three-party model that consists of an *end-user* (that possesses a digital identity and wants to perform an action), *an identity provider* (that enrolls new users, manages digital entities and performs authentication), and *a service provider* (or *relying party* – that provides services to the end-user, and relies on the identity provider to verify the identity of the end-user) [4, 12].

In the literature, there are four major identity management models: (1) *the isolated identity model*, (2) *the centralized identity model*, (3) *the federated identity model*, and (4) *the user-centric identity model*. In the isolated identity model, the service provider is also managing user identity, meaning that the end-user has one digital identity for each service provider [12, 13]. In the centralized identity model, the identity provider manages and centralizes digital identities, and the users are authenticated before connecting to the service provider; this means that the user can reuse the same credentials for multiple service providers by e.g., Single Sign-On (SSO) [12, 13]. In the federated identity model, the user can use the same credentials for authenticating and accessing service providers that together with the identity provider form a federation; contrary to the centralized identity model, it makes use of pseudonyms (distinct pseudonyms are used for different service providers) [12, 14]. In the user-centric identity model, the user has control of his attributes, and he can define his policies for sharing his identity with the service providers. However, despite the users' capabilities in selecting and change contractual terms, it still relies on identity providers [12, 15]. A quite recent model, called the *Self-Sovereign Identity (SSI) model,* eliminates the need for an external identity provider. The end-user gains full control of its identity, being his own identity provider. This eliminates the need for an external authority and, as a consequence, it decreases the danger of identity theft [7, 15]. We will refer more to the SSI model in Subsection 3.1.

2.2. Blockchain

A blockchain is a specific implementation of *Distributed Ledger Technology* (DLT) with cryptographic enhancements [7]. It is *distributed*, in the sense that it is spread between multiple nodes, each node stores a copy of the blockchain and *decentralized* by design in the sense that there is not a single point of decision, but the decision is a result of a *consensus* of the nodes. There are different types of consensus protocols (e.g., Proof of Work (PoW), Proof of Stake (PoS)) but their goal is always the same: to decide how the nodes agree on blocks that are validated and added to the blockchain. Blockchains can be classified into *permissionless* – any entity can become a node and participate in the blockchain consensus (e.g., add transactions) – and *permissioned* – restricted nodes only are allowed to participate in the consensus protocol.

Asymmetric cryptography is intensively used in blockchains. Usually, the public key corresponds to the public address of the user in the blockchain. The user signs a transaction under his private key such that everyone can verify its authenticity in the blockchain (as corresponding to his address). The private key is thus used to authorize actions on the user account, this being a simple method of authentication.

3. IDENTITY MANAGEMENT ON BLOCKCHAIN

3.1. Specific characteristics and classification of identity management on blockchain

A blockchain-based identity management solution should allow selective storing of identities in the blockchain. Identities need to be *attested* by authorities or other entities in the blockchain. This usually works as follows. An entity claims an identity by a *verifiable claim*, that is attested after the verification of some *attributes* that differentiate the user (e.g., phone number, e-mail, governmental identity documents (IDs), biometrics). Within identity management on the blockchain, it is a clear difference between the *digital identifier* (a value that uniquely identifies the entity) and the *attributes* that are associated with it [7]. Because the non-authorized or uncontrolled disclosure of attributes results in security and privacy leaks, the storage of attributes (if the case) needs to be treated accordingly to well-defined principles.

In [4,7], the authors classify DLT-based identity management solutions into two categories: *Self-Sovereign Identity* and *Decentralized Trusted Identity*. Both can be built on top of either permissionless or permissioned blockchains, with direct implications on the properties of the identity management solution.

Self-Sovereign Identity (SSI) is owned, controlled, and managed by the user, with no need to rely on a third party [3,7]. The users generate their digital identities and add them to the blockchain, tied with a public key, which permits anyone to challenge and verify the authenticity of the user [7]. Any authentication procedure can be tied to the identity on the blockchain, but the usage of public-private key pairs is the most common method. The users are then issuing *claims* of identities that need to be attested by other users to endorse their identity, called *claim-verifiers*, as they verify and validate the other users' claims. The verifiable claims are managed outside the blockchain, to preserve privacy, as sometimes the issuer needs to make the private information to be public for the verifier to prove their link to the digital identity. Thus, a trustful relationship between the issuer and the verifier must be established before a verification, off-chain [3].

Decentralized Trusted Identity (DTI) assumes a service that proves the user's identity and records his digital identity on the blockchain. Proving the user's identity relies on a general trusted method or (inter)national IDs such as passports and requires the presence of an external authority [7]. Similar to SSI, additional identification attributes can be further tied to the digital identity. The existence of a trusted authority centralizes (to some extent) the users' enrollment in the blockchain: the service that performs the identity verification is usually proprietary and might sometimes be seen as a single point of trust.

3.2. Existing implementations

We describe several blockchain-based identity management implementations, with focus on privacy and security aspects. Table 1 gives an overview of these implementations.

Table 1

Classification of implementations based on blockchain

Implementation	Type (SSI/DTI)	Open-Source	Blockchain Type (Permissionless / Permissioned)	Blockchain Implementation
Namecoin [16]	SSI	yes	permissionless	Bitcoin fork
Blockstack [18]	SSI	yes	permissionless	Blockstack (Bitcoin)
uPort [21]	SSI	yes	permissionless	Ethereum
Sovrin [22]	SSI	yes	permissioned	Sovrin Network
EverID [23]	SSI	no	permissioned	Ethereum private
SelfKey [24]	SSI	yes (beta)	permissionless	Ethereum
ShoCard [25]	DTI	no	Permissionless / permissioned	(Bitcoin)
Sora [26]	SSI	(under development)	permissioned	Hyperledger Iroha
lifeID [27]	SSI	yes	permissionless	(Ethereum)
IDchainZ [28]	DTI	(prototype)	-	ChainZy Smart Ledger

Namecoin [16] was the first step towards blockchain usage for identity management systems. It was thought as a naming system that binds human-readable names with IP addresses, in the sense of a Domain Naming System (DNS) [16]. Currently, Namecoin is an experimental open-source technology that aims to provide the user with several features: the possibility of attaching attributes (e.g., Pretty Good Privacy (PGP) keys, e-mails) to a digital identity, decentralized Transport Layer Security (TLS) certificate validation, and website access using the .bit top-level domain that uses Bitcoin to decentralize website addresses [16]. Concerning identities, Namecoin allows fetching data associated with an identity in JavaScript Object Notation (JSON) format [17]. This raises some privacy concerns, as anyone can access the data. Namecoin was proved vulnerable to the 51% attacks [18], and more recently, it has been shown that an adversary can take ownership of any .bit domain [19].

Blockstack [18,20] is an open-source solution that extends Namecoin. Motivated by the possibility of a 51% attack against Namecoin, Blockstack brings a novel contribution: it allows migration to another blockchain in case of a major attack. This is possible by defining several layers, with the currently used blockchain being the first layer that runs under a virtual chain logical layer that allows high flexibility [18]. Unlike Namecoin, it uses encryption to protect users' data, giving more control to the user by using public cryptography (i.e., the user uses his private key for decrypting and signing the data).

uPort [21] is an open-source identity management system that claims to provide the users with a self-sovereign identity registered on the Ethereum blockchain using a mobile application. The uPort identifier is, in fact, an address on the Ethereum blockchain, while the user public key resolution and the management of the identifiers are done by using a smart contract (currently called EthereumDIDRegistry). The user can control the changes of his data by signing with the corresponding private address. Any entity can query the EthereumDIDRegistry and therefore, even if the data itself might be encrypted, the attributes structure and other metadata can leak sensitive information [7]. Moreover, this means the user has no full control over his attributes' disclosure to others, which makes uPort susceptible to not being a complete SSI solution [8]. uPort provides recovery mechanisms for the private key, which is stored on the user's mobile: either recovering the identity by using the seed words (from which the private key is derived) or by using a group of trustees previously chosen. The first method implies advanced user management skills, while the second one might be open to attacks such as coalitions of malicious trustees (the IDs of the trustees might be linked to the victim), or to direct replacement of trustees [7,8]. The users can temporarily delegate his identity to other users and they can perform actions on behalf of the owner. There is a chance that the uPort identity management system has unusable accounts due to private key loss [8]. uPort also lacks portability in the sense that only internal identities can attest claims of other uPort identities [5].

Sovrin [22] is an open-source, public service designed for identity management on the blockchain. The use of a permissioned blockchain makes Sovrin take advantage of increased efficiency in reaching consensus, improved transaction rate and be less susceptible to 51% attacks [7]. To preserve minimization of data exposure, Sovrin makes use of Zero-Knowledge Proofs (ZKP) for all verifiable identity claims stating that it is possible to share selective attributes connected to the identity credentials without disclosing the credentials. Moreover, Sovrin tries to reduce the correlation between data and identifiers by separating them, which makes a linkage to an identity difficult without additional information stored separately [22]. Similar to uPort, it provides a mobile application and accepts key recovery by using trustees [7, 22].

EverID [23] is an identity management system that runs on a private Ethereum instance hosted on EverID operated hardware. It is part of a larger solution, called Everest [23]. It uses proprietary datagrams to store users' identity information that is further cryptographically secured in some storage arrays. It is not clear if the algorithms use proprietary cryptographical mechanisms as well, hence the product breaks the well-known *Kerckhoffs principle*. The user's data is protected by several mechanisms such as public-private key pair, biometric means (face and fingerprint recognition), password and Personal Identification Number (PIN) [23]. Usage of so many authentication means should be properly tested, both from a security and a usability perspective. As a feature, in EverID, the digital identity can be stored in the cloud and therefore its persistence is not linked to a physical device. On the weaknesses side, for claim verifications, the user has to disclose full data, which overcomes the principle of minimal exposure of data [5].

SelfKey [24] is an open-source identity management system that runs on Ethereum public blockchain. For individual users, the data is stored on the user's device and is managed by the owner. Only if approved by the owner, other entities can access specific data. In the 2017 whitepaper, SelfKey planned to use uPort for recoverability of lost private keys. If so, then all vulnerabilities of uPort remain valid in the context of SelfKey too. Although in literature SelfKey is supposed to have implemented ZKP to minimize the exposure of data [5], we found no official evidence of that. The SelfKey whitepaper only mentions ZKP as a future possibility.

ShoCard [25] is an identity management platform that can use any permissioned or permissionless blockchain. As an advantage over solutions such as Blockstack, ShoCard supports not only migration but also multiple types of blockchain at the same time [8] even though ShoCard operating on the blockchain might expect long processing times [7]. On the other hand, ShoCard is not open source and it is centralized, meaning that all records written on the blockchain pass via a ShoCard server. The ShoCard server does not break confidentiality directly, as the messages are encrypted under a public key (in a *secure envelope*) but restricts decentralization and maintains the availability of the solution for the lifetime of the ShoCard company only [7]. For self-certification, the user needs a mobile device that collects the name and value of his identity. The identity might be a phone number, an e-mail address, a scan of a valid document (e.g., passport, driving license), or biometric data (e.g., iris-scan, facial image, voice). To protect leakage, the names and values are locally stored apart, and the solution only publishes the salted hash on the blockchain, signed under the user's public key [25].

Sora [26] is an identity solution based on the Iroha permissioned blockchain. Both Sora and Iroha are currently under development. The Sora mobile application allows a user to generate a pair of cryptographic keys and store a salted hash of his private data on the blockchain. The solution basically follows the model of a general SSI solution. To prevent a key loss, the public-private keys pair is stored on a central server in an encrypted form [26]. Encryption is performed under a key derived from an 8-digits password, which must satisfy some security requirements. We note two shortcomings here. Firstly, the storage of the keys is centralized, therefore the solution cannot aim for full decentralization. Secondly, the security of the solution resides in the security of the master password, which is prone to human selection and hence might be vulnerable to known attacks, like for example, dictionary attacks.

lifeID [27] is an open-source identity management solution designed to work on any permissionless blockchain capable of using smart contracts (e.g., Ethereum). It allows the implementation of ZKP to minimize sensitive data exposure. lifeID presents three key recovery procedures: self-backup, trusted organization backup, and backup using a trusted group of individuals. lifeID makes no use of passwords but uses biometric authentication instead. Hence, it requires a mobile with biometric capabilities. The current status of the project is not clear, as the official website posted no updates since 2018.

IDchainZ [28] is a proof of concept DTI, built on top of the ChainZy Smart Ledger. The system has two distinct mutual distributed ledgers – one for holding the individually encrypted documents and the other a transaction ledger that holds the keys of the documents [28]. There is not enough public information available on the website to conduct an in-depth security evaluation of the proposal. We found no specification about the used type of blockchain (permissioned or permissionless) either.

4. DISCUSSION

Blockchain-based identity management solutions were proposed as a candidate solution to the identity management problem. The main property a blockchain should have by definition – *decentralization* – could increase freedom of choice and independence of big companies and organizations. It could become a strong alternative to the existing identification and authentication systems widely used (e.g., via Google or Facebook) [18]. Moreover, SSI solutions give, in theory, full control to the user with respect to his data, decreasing the danger of identity theft. However, important questions persist: *Does identity management on blockchain bring real benefits?*, *Are the benefits brought by identity management on blockchain strong enough to overcome the complexity they introduce?* and, the most important one, *Is blockchain a real solution to identity management problems?* Although there is no straight positive answer to the questions above, blockchain-based identity management solutions have been implemented, and people started to use them at personal, organizational and governmental levels. An example is the pilot implementation of *uPort* to manage the digital identity of the citizens of the Swiss city Zug [29].

Currently, blockchain-based identity management solutions are still emerging, and more research must be performed to gain a better knowledge of their functionalities. Table 2 summarizes some important aspects of the implementations described in Section 3.2, with respect to what the solutions claim to offer. We further indicate more directions that must be considered for in-depth analysis and future research.

Table 2

Claimed properties of the analyzed blockchain implementations

Implementation	ID Secure Verification	Long-term Validity	ID Management (recovery of identity / private key)	ID Self-management (e.g., set attributes, delegation)
Namecoin [16]	no	no	no	set attributes
Blockstack [18]	yes	yes	12-word recovery phrase	no
uPort [21]	yes	yes	12-word recovery phrase, group of trustees	set attributes, delegation
Sovrin [22]	yes	yes	"social recovery" (trustees having shards of data)	no
EverID [23]	yes	yes	mnemonic phrase, biometrics, PIN, password	set attributes
SelfKey [24]	yes	yes	no, but planned	no, partially planned (delegation)
ShoCard [25]	yes	yes	three-factor recovery process (from phone number, e-mail, phrase, ID, scanned document)	set attributes
Sora [26]	yes	yes	not provided	set attributes
lifeID [27]	yes	yes	12/24-word recovery phrase, group of trustees, trusted organization	set attributes
IDchainZ [28]	not provided	yes	not provided	not provided

Specific aspects of blockchain-based identity management that should be considered can be either particular to identity management or inherited from the underlying blockchain technology.

In the first category, we mention the verification of the real identity. It remains open how this can be performed securely in totally decentralized environments (because of e.g., 51% attack, malicious trustees, or fake identities created by combinations of different attributes of real entities [30]). Moreover, decentralization itself can be an issue. Not all implementations are fully decentralized (e.g., ShoCard – see Subsection 3.2), and even if they are, then there is a great need for trust [7]: trust between the claimers and the verifiers, trust in the majority of participants, etc. Even more, the decentralization of the underlying blockchains is also debatable [31]. Furthermore, attention must be paid to possible faults. Key recovery mechanisms should be available in case of lost private keys, to prevent identity loss, but they must be implemented with care. Solutions such as recovery via trustees may be exposed to vulnerabilities (e.g., uPort, Sovrin - see Subsection 3.2), and private key recovery from passwords (e.g., Sora – see Subsection 3.2) is strongly not recommended. Many solutions are built for mobile environments, and some store the private key directly on the smartphone [3]. This transforms the smartphone in a single point of vulnerability from a user perspective. Finding appropriate key recovery solutions is a research topic.

By definition, blockchain should be immutable (i.e., published information is unchangeable), long-preserving (i.e., information remains in the blockchain for at least the life-time of the blockchain) and, for permissionless blockchains, data is public. While this transparency can be good in some contexts, it can harm privacy. Attributes should not be published in the blockchain, at least not in cleartext. Moreover, even if data is encrypted, metadata might leak sensitive information (e.g., uPort – see Subsection 3.2). Pattern analysis of on-chain data and exchanged messages is a general risk with respect to information disclosure [11].

In the second category, we note that in many situations the underlying blockchain immutability does not hold, e.g., in case of 51% attacks on Proof of Work (PoW). A financial incentive can be enough to mount such an attack, if the rewards are high [4]. According to [32], investment in computational mining power to equal the total mining power in Bitcoin is 400 million dollars, while the financial gain over the network can be estimated to much more. High electricity consumption [4] and performance should also be considered when thinking about blockchains as an underlying technology. Possible solutions to problems regarding the underlying blockchain are migration (e.g., Blockstack – see Subsection 3.2) or multiple-blockchain usage (e.g., ShoCard – see Subsection 3.2). However, there are problems that appear from the blockchain definition itself and cannot be easily overcome. An example is the infinite ledger problem: the length of the blockchain is endlessly increasing, which introduces difficulties for storage, at least for new full nodes (e.g., the download time for Bitcoin is currently up to three days) [18]. It remains open how would identity management solve this concerning scalability in time and users.

Cryptographical aspects have a direct impact on the privacy and security of identity management on the blockchain. Usage of proprietary, not public solutions, that break Kerckhoffs principle (e.g., EverID – see Subsection 3.2) and passwords (e.g., Sora – see Subsection 3.2) that might be vulnerable to well-known dictionary attacks are examples of bad practice. Moreover, if attributes or other sensitive data are published in the blockchain, future advances of cryptanalysis might damage privacy. Hash functions and public-key encryption that used to protect data are currently computationally infeasible, but in time they might get broken. Additionally, most of the existing public-key solutions are known to be vulnerable to quantum attacks, so in the future, quantum-resistant primitives must be accommodated in the blockchain-based identity management solutions. How can this be done and to what extent it will influence their efficiency and functionality is a research direction. Similarly, the usage of ZKP for proving identity claims might be a good option from a cryptographic point of view, but the tradeoffs in complexity need to be analyzed in more depth. Last but not least, effective key management also remains a challenge in from cryptographic terms perspective too [7].

Usability aspects are important for a successful identity management system. However, research in usability and user experience seems to be in an incipient stage. Studies should determine if the users are willing to use those solutions in the long term. Moreover, it is an open question whether the end-users are able to securely manage their identifiers and credentials by themselves or not. They could (partially) delegate control for certain periods of time or rely on services such as recovery mechanisms in case of loss [11]. uPort mentions that there is a list of requirements to onboard new users in decentralized applications and admits that it is not a trivial task [33] and EverID introduces many means of authentication (password, PIN, biometric recognition), making the solution non-user-friendly (see EverID – Subsection 3.2). One inconvenience of PKI is its complexity, but blockchain-based solutions are also complex, so they might not be a good replacement from this perspective.

5. CONCLUSIONS

This paper presents identity management on the blockchain and discusses the most known current implementations. We show that they still have shortcomings, so further analysis must be conducted to overcome the existing challenges and the (sometimes) unsolid widespread adoption of blockchain technology. The possible benefits of blockchain-based identity management in relation to the complexity of usage, implementation, and maintenance must be carefully taken into consideration for future research.

ACKNOWLEDGEMENTS

This work was partially supported by a grant of Romanian Ministry of Research and Innovation CCCDI-UEFISCDI project no. 17PCCDI/2018.

REFERENCES[1]

1. L. AXON, *Privacy-awareness in blockchain-based PKI*, Oxford University Research Archive, Oxford, UK, 2015.
2. M. AL-BASSAM, *SCPKI: A Smart Contract-based PKI and identity system*, Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, UAE, pp. 35-40, 2017.
3. A. MÜHLE, A. GRÜNER, T. GAYVORONSKAYA, C. MEINEL, *A survey on essential components of a self-sovereign identity*, Computer Science Review, **30**, pp. 80-86, 2018.
4. P. DUNPHY, L. GARRATT, F. PETITCOLAS, *Decentralizing digital identity: Open challenges for distributed ledgers*, 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, pp. 75-78, 2018.
5. D. VAN BOKKEM, R. HAGEMAN, G. KONING, L. NGUYEN, N. ZARIN, *Self-sovereign identity solutions: The necessity of blockchain technology*, arXiv, p. 1904.12816, 2019.
6. C. ALLEN, *The path to self-sovereign identity*, available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html, 2016.
7. P. DUNPHY, F. A. P. PETITCOLAS, *A first look at identity management schemes on the blockchain*, IEEE Security & Privacy, **16**, *4*, pp. 20-29, 2018.

[1] Note: all the links were last accessed in February 2020

8. J. ROOS, H. NIEDERMAYER, *Identity management on the blockchain*, Seminars FI / IITM SS 18, Network Architectures and Services, 2018.
9. U. DER, S. JÄHNICHEN, J. SÜRMELI, *Self-sovereign identity − Opportunities and challenges for the digital revolution*, arXiv, p. 1712.01767, 2017, available online: https://arxiv.org/pdf/1712.01767.pdf.
10. G. GOODELL, T. ASTE, *A decentralised digital identity architecture*, Frontiers in Blockchain, 2019, doi: 10.3389/fbloc.2019.00017, available at SSRN: https://ssrn.com/abstract=3342238.
11. L. LESAVRE, P. VARIN, P. MELL, M. DAVIDSON, J. SHOOK, *A taxonomic approach to understanding emerging blockchain identity management systems*, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2019, available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01142020.pdf.
12. L. MARYLINE, J. DENOUEL, C. LEVALLOIS-BARTH, P. WAELBROECK, *Digital identity*, Chapter 1 in: "Digital identity management", Elsevier, 2015, pp. 1-45.
13. A. JØSANG, S. POPE, *User centric identity management*, AusCERT Asia Pacific Information Technology Security Conference, p. 77, 2005.
14. D.W. CHADWICK, *Federated identity management*, in: "Foundations of security analysis and design V", Springer, 2009, pp. 96-120.
15. A. TOBIN, D. REED, *The inevitable rise of self-sovereign identity*, The Sovrin Foundation, 2016, available online: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.
16. Namecoin, available online: https://namecoin.org.
17. Namecoin ID: *Manage your online identity*, available at: https://github.com/namecoin/wiki/blob/master/Namespace:Identity.mediawiki.
18. M. ALI, R. SHEA, J. NELSON, M.J. FREEDMAN, *Blockstack: A global naming and storage system secured by blockchains*, 2016 USENIX Annual Technical Conference (USENIX ATC 16), pp. 181-194, 2016.
19. D. GILSON, *Developers attempt to resurrect Namecoin after fundamental flaw discovered*, available online: https://www.coindesk.com/namecoin-flaw-patch-needed.
20. Blockstack, available online: https://blockstack.org.
21. uPort, available online: https://www.uport.me.
22. SOVRIN FOUNDATION, *A protocol and token for self-sovereign identity and decentralized trust*, 2018, available online: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf.
23. B. REID, B. WITTEMAN, *EverID whitepaper*, available online: https://everest.org.
24. THE SELFKEY FOUNDATION, *Selfkey*, 2017, available online: https://selfkey.org/wp-content/uploads/2017/11/selfkey-whitepaper-en.pdf.
25. A. EBRAHIMI, *ShoCard whitepaper – Identity management verified using the blockchain*, 2019, available online: https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf.
26. M. TAKEMIYA, B. VANIEIEV, *Sora identity: Secure, digital identity on the blockchain*, 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), IEEE, 2018.
27. lifeID, *An open-source, blockchain-based platform for self-sovereign identity*, available online: https://lifeid.io/whitepaper.pdf.
28. ChainZy, *IDChainZ*, available online: https://www.chainzy.com/products/idchainz.
29. *Zug Stadt*, available online: https://www.stadtzug.ch/digitaleid.
30. IDENTITY THEFT AMERICA, *The changing face of identity theft*, available online: https://www.ftc.gov/sites/default/files/documents/public_comments/credit-report-freezes-534030-00033/534030-00033.pdf.
31. A.E. GENCER, S. BASU, I. EYAL, R. VAN RENESSE, E.G. SIRER, *Decentralization in Bitcoin and Ethereum networks*, in: "International Conference on Financial Cryptography and Data Security", pp. 439-457, Springer, 2018.
32. G. GREENSPAN, *The blockchain immutability myth*, available online: https://www.coindesk.com/blockchain-immutability-myth.
33. uPort, *Helping you build user centric apps on blockchains*, available online: https://developer.uport.me/overview/index.

Received June 27, 2019