Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study

Razieh Nokhbeh Zaeem
Kai Chih Chang*
Teng-Chieh Huang*
David Liau*
Wenting Song*
Aditya Tyagi*
University of Texas at Austin
Austin, Texas, USA
{nokhbeh,kaichih1013,tengchieh,davidliau,wentingsong,adityatyagi6498}@utexas.edu

Manah M. Khalil
Michael R. Lamison
Siddharth Pandey
Verizon
Dallas, Texas, USA
{manah.khalil,michael.lamison,siddharth.pandey}@verizon.com

K. Suzanne Barber
University of Texas at Austin
Austin, Texas, USA
sbarber@identity.utexas.edu

ABSTRACT

Identity is at the heart of digital transformation. Successful digital transformation requires confidence in and protection of digital identities. On the Internet, however, there is no unique and standard identity layer. Consequently, a variety of digital identities have emerged over years, leading to privacy risks, security vulnerabilities, risks for identity owners, and liability for identity issuers and those relying on digital identities to grant access to goods and services. Self-Sovereign Identity (SSI) and similar forms of identity management on the blockchain distributed ledger are novel technologies that recognize the need to keep user identity privately stored in user-owned devices, securely verified by identity issuers, and only revealed to verifiers as needed. There is limited academic literature defining the prerequisite SSI functional and non-functional requirements and comparing SSI technologies. Often those SSI technologies reviewed in the literature lack behind current advances. We present the first work that compiles a comprehensive list of functional and non-functional requirements of SSI and compares an extensive number of existing SSI/blockchain-based identity management solutions with respect to these requirements. Our work sheds light on the state-of-the-art SSI development and paves the way for future, more informed analysis and development of novel identity management and SSI solutions.

CCS CONCEPTS

• **Computer systems organization** → **Peer-to-peer architectures**; • **General and reference** → *Surveys and overviews*; • **Security and privacy** → **Access control**; **Authentication**; **Authorization**; **Privacy protections**.

KEYWORDS

self-sovereign identity, blockchain, privacy

ACM Reference Format:
Razieh Nokhbeh Zaeem, Kai Chih Chang, Teng-Chieh Huang, David Liau, Wenting Song, Aditya Tyagi, Manah M. Khalil, Michael R. Lamison, Siddharth Pandey, and K. Suzanne Barber. 2021. Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study. In *IEEE/WIC/ACM International Conference on Web Intelligence (WI-IAT '21), December 14–17, 2021, ESSENDON, VIC, Australia.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3486622.3493917

1 INTRODUCTION

Many activities–be it performed in the physical world or on the Internet–require a form of identity proofing, the act of verifying an individual is who they claim to be. Traditional identity proofing methods usually involve standard documents issued by authorities (e.g., passports issued by government agencies). On the Internet, no unique and standard identity layer exists. As a result, a haphazard structure has evolved over time, which includes standalone passwords, Single Sign On (SSO), Federated Identity Management (by third parties such as Google and Facebook), etc.

Self-Sovereign Identity (SSI) is a recent approach to digital identity. SSI recognizes that a user's identity should be owned and controlled by the user. Many SSI solutions are developed on top of the distributed ledger technology (blockchain), but non-blockchain variants exist as well.

1.1 Blockchain

The term blockchain is rooted in the seminal Bitcoin white-paper [27] that introduced a novel crypto-currency (i.e., electronic cash) technology. This technology allows online transactions to take place without the need to go through a trusted financial third party. Digital signatures and a peer-to-peer network form the backbone of the blockchain technology. The two parties of the transaction communicate through digital signatures (i.e., public and private keys). The peer-to-peer network timestamps transactions by hashing them into a chain of blocks, forming a record of transactions. The longest chain of blocks serves as a tamper-proof ledger of all witnessed transactions. This ledger (also known as blockchain) cannot be altered without the consensus of the network majority.

*These authors contributed equally to this research.

WI-IAT '21, December 14–17, 2021, ESSENDON, VIC, Australia

ACM ISBN 978-1-4503-9115-3/21/12…$15.00
https://doi.org/10.1145/3486622.3493917

1.2 Blockchain-Based Identity Management

The blockchain technology has found many applications [6, 12, 17, 21, 33], including identity management (IdM), patient IdM [16] and the Internet of Things IdM [4, 14, 41]. An IdM is the framework that identifies, authenticates, and authorizes users to access resources. Blockchain-based IdM solutions [28, 31, 37, 42] adopt blockchain for identity management. As previously suggested in related work [7], building an IdM on top of blockchain offers advantages like decentralization, immutability, transparency, and security.

In any IdM, when the user (identity owner/holder) needs to make a *claim* (i.e., assert something about one's identity, such as identity as a citizen of a country) to an identity verifier (e.g., a police officer), he/she provides an *identity proof* (i.e., some form of document that provides evidence for the claim, like a passport). Such identity proofs should be *attested* (i.e., validated) by the relevant identity authority (e.g., the agency that issued the passport, also known as the issuer).

Blockchain-based identity solutions encrypt a user's identity, hash it, and add its attestations to the blockchain ledger. These attestations are later used in order to prove the user's identity. Two major flavors of blockchain-based IdM solutions exist [7] and we study both:

- Decentralized Identity (e.g., ShoCard, Authenteq, and IDchainZ): This identity solution is similar to conventional digital identity management solutions where credentials from a trusted service are used. The only difference is the storage of validated attestations on a distributed ledger for later validation by a third party.
- Self-sovereign identity (e.g., Civic, Sovrin, uPort, and Onename.io): The user owns and controls their identity without heavily relying on central authorities. In essence, self-sovereign identity is very similar to how non-digital identity documents work today. Every user keeps their own identity documents in their device. The user creates a public/private key pair and contacts identity authorities to associate and attest their public key with an identity proof—saving the association between the public key and this identity in a distributed manner (e.g., in the blockchain). When the user makes a claim, he/she signs the claim with the private key of the attested public key. The verifier fetches the public key from the blockchain and accepts only the claims signed with the corresponding private key.

Blockchain-based IdM improves identity management in several ways. Digital signatures, one of the major components of the blockchain technology, provide authenticity of the identity proof and attestation. The peer-to-peer network, the other major component of blockchain, eliminates the need for a central repository of users' identity. Hence, blockchain can make IdM solutions decentralized, tamper-resistant, and enhance security and privacy.

1.3 Our Contribution

The commercial implementation of blockchain-based IdM largely precedes the academic work. In addition, the comparative analysis of blockchain-based IdM has not received the attention it deserves. Many surveys and competitive analysis papers review only the most popular blockchain-based IdM solutions. Furthermore, almost all lack functional and non-functional requirements analysis, and, as a result, present a rather shallow comparison. In this paper we make the following contributions:

- With a comprehensive study of both commercial and academic work on SSI and blockchain-based IdM, we are the first to enlist 22 non-functional requirements of SSI solutions.
- We further add seven groups of functional requirements, with a total of 20 use cases.
- We cover 31 blockchain based IdM solutions and compare them with respect to our extensive list of functional and non-functional requirements as well as various emerging SSI standards.

We structure the rest of this paper as follows. Section 2 reviews the related academic work on SSI and blockchain-based IdM and highlights the gap wee seek to fill. Section 3 lists the functional and non-functional requirements we identify in SSI. Section 4 particularly covers the use cases for functional requirements. Section 5 surveys and compares existing SSI solutions with respect to functional and non-functional requirements. Section 6 briefly summarizes relevant emerging standards, and Section 7 concludes the paper.

2 RELATED WORK

While SSI based on blockchain has been studied in the academic literature [7, 11, 25, 30, 42] and there are proposed academic solutions for it [13, 24, 29], commercial implementation of blockchain-based IdM largely precedes the academic work (e.g., Evernym [10] was started in 2012, ShoCard [2] in 2015, and uPort [34], Sovrin [32], and Civic [1] in 2016).

The comparative analysis of blockchain-based IdM has been relatively limited in the literature. For example, many researchers [5, 7–9, 15, 23, 26, 36] looked at only the four popular solutions (Sovrin, uPort, Civic, and ShoCard). As another example, Kondova and Erbguth [20] recently surveyed some of the most popular solutions for SSI on blockchain: Hyperledger Indy public permissioned blockchain as well as uPort and Jolocom on the Ethereum public permissionless blockchain. Dunphy and Petitcolas [7] used the "laws of identity" framework (including user control and consent, minimal disclosure, justifiable parties, directed identity, design for a pluralism of operators, human integration, and consistent experience across contexts) to evaluate three blockchain-based IdM solutions (uPort, ShoCard, and Sovrin).

Some of the more comprehensive comparative studies of SSI on the blockchain look at numerous existing solutions, but nonetheless remain descriptive and lack depth. Baars [3] compared ten SSI solutions (including (1) Onename.io, (2) Qiy, (3) iDIN, (4) eHerkenning, (5) IRMA, (6) PKIoverheid, (7) Jumio, (8) Tradle, (9) Idensys, and (10) uPort) based on their type of access (centralized vs. decentralized), storage type, technology, and development status. Lim et al. [22] compared 15 existing solutions ((1) Sovrin, (2) MyData, (3) Waypoint, (4) Bloom, (5) BlockStack, (6) ShoCard, (7) uPort, (8) I/O Digital, (9) BlockAuth, (10) UniquID, (11) Jolocom, (12) Cambridge Blockchain, (13) KYC.LEGAL, (14) CertCoin, and (15) Authenteq) based on their underlying blockchain, network type (permissioned or permissionless) and development status. Similarly Jacobovitz [18] surveyed 30 IdM solutions without going into details of functional or non-functional requirements of such solutions. Kaneriya and colleagues [19] have investigated six SSI solutions (namely (1) Sovrin,

Table 1: The list of SSI NFR and their definitions.

NFR	Definition
1. Provability	The ability for the identity owner to prove their identity
2. Interoperability	Accessibility to all kinds of public and private services, working across programming languages, blockchains, vendors, platforms, networks, legal jurisdictions, geos, cryptographies, and hardware, as well as across time
3. Portability	Ability to take one's digital identifier credentials anywhere
4. Pseudonymity	Ability to interact without disclosing one's real identity
5. Recovery	Ability to retrieve keys and credentials easily and safely
6. Scalability	Feasibility for adoption and replication
7. Security	Protecting data, including keys & credentials
8. Usability	Human-meaningful and good user experience
9. Protection	Information is kept secure
10. Persistence	Identity is available until removed by holder
11. Minimization	Sending the least amount of data required
12. Existence	User can see the data until asked to be removed
13. Control	User must be in control of who can see/access their data
14. Consent	Every access requires holder consent
15. Transparency	Holder has a clear idea of who has their data
16. Access	User can access their data whenever they want
17. Convenience	The ease of access to user data for them
18. Inclusion	Supports various groups of users (race, nationality, etc.)
19. Trust	User trusts the platform
20. Biometrics support	Whether users can authenticate with their biometrics
21. Support for IoT	Support for device IdM in the Internet of Things
22. Cost	The monetary charge for identity owners, issuers, verifiers

(2) uPort, (3) EverID, (4) LifeID, (5) Sora, and (6) SelfKey) but their comparison remains highly descriptive too, with the limited observation of some non-functional features such as portability, minimization, and robustness. **While the above studies looked at up to 30 solutions, none compared based on a comprehensive list of functional or non-functional properties of SSI.**

Our previous work [28] investigated different personal data options given to users for authentication on current blockchain-based IdM solutions. Based on our Identity Ecosystem model [38–40], we evaluated these options and their risk and liability of exposure.

3 SSI REQUIREMENTS

To perform a deep and detailed comparative analysis of SSI solutions rooted in blockchain, we first distill a list of functional and non-functional requirements of such solutions from the literature. Then we enlist a comprehensive set of existing solutions and compare them based on these functional and non-functional requirements.

Table 1 lists the **Non-Functional Requirements (NFR)** of SSI [7, 30]. The first eight rows (Provability, Interoperability, Portability, Pseudonymity, Recovery, Scalability, Security, and Usability) are the most prominent NFR of SSI, widely used in the academic literature and also in the commercial and open-source solutions and standards.

The **Functional Requirements (FR)** of SSI are extensive. We identified 20 use cases. We grouped these use cases into seven high-level functionalities as required by emerging standards and/or commonly supported by existing solutions. The Operational Reference Model (ORM) captures the high-level functionality across the scenarios. The ORM groups of FR are as follows:

(1) Issuer Discovery
(2) Connection Creation
(3) Credential Creation
(4) Verification with Credentials
(5) Backup/Recovery
(6) Derive/Share Credentials
(7) Sunset/Delete/Revoke Credentials

4 SSI USE-CASES FOR FR

We chose two canonical and reusable use cases of SSI out of all the use cases. We elaborate on these two building block use cases which represent key and foundational capabilities across multiple use cases. At the end of this section, we briefly name the other SSI use cases, but we do not include their sequence diagrams for the sake of brevity.

4.1 Discover, Connect, Create Credential

Figure 1 shows the temporal sequence diagram for the use case "Discover, Connect, Create Credential". Holder-Wallet is the SSI wallet on the identity holder's device. Mediator-Cloud is an agent acting on behalf of the identity owner in the cloud (as a part of the provided SSI solution). In this use case, a connection is initiated by the identity holder, but one might imagine a use case wherein the issuer can publish connection invitations.

4.2 Online Identity Verification

Figure 2 depicts the temporal sequence diagram for the use case "Online Identity Verification Initiated by the Identity Holder". The identity holder uses credentials to make an identity claim to a verifier. We assumed a connection between holder and verifier for simplicity. The steps to create this connection is identical to those used in use case above. The identity holder may divide identity attributes into three groups in this proof: (1) value revealed, (2) value not revealed, and (3) value not required, to reveal a minimal amount of data. Finally, note that how issuer does not play any role in this sequence diagram.

4.3 Other Use Cases

We group the rest of our use cases according to the ORM, but skip their details for brevity.

(1) Issuer Discovery
(2) Connection Creation
(3) Credential Creation
  (a) Credentials proposed by verifier
  (b) Hierarchical identity (e.g., nationality, state, etc.)
(4) Verification with Credentials
  (a) Verification of business good
  (b) Online identity verification initiated by the verifier
  (c) Optimized selection of identities
  (d) "Identity payments" via contact-less technologies
  (e) IoT devices verify on behalf of users
  (f) Issuing tickets to each person only once
(5) Backup/Recovery
  (a) Recover from permanently lost wallet, also if the user wants to change devices
  (b) Recover from temporarily lost wallet
(6) Derive/Share Credentials
  (a) Cross platform user driven sharing of personal data
  (b) Derive new credentials from existing credentials
  (c) Third party app authenticates through wallet
(7) Sunset/Delete/Revoke Credentials

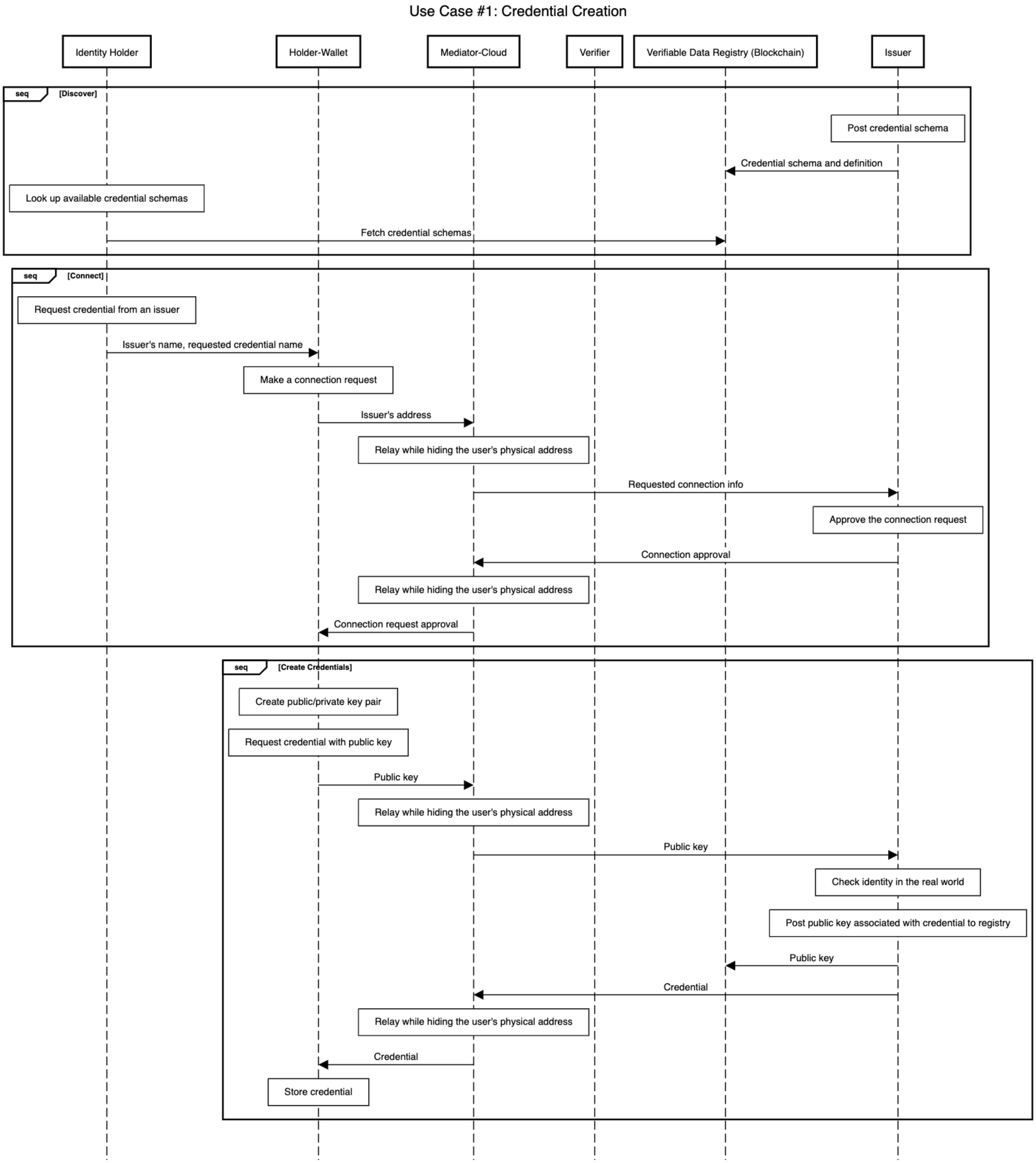
Use Case #1: Credential Creation
Identity Holder
Holder-Wallet
Mediator-Cloud
Verifier
Verifiable Data Registry (Blockchain)
Issuer
seq
[Discover]
Post credential schema
Credential schema and definition
Look up available credential schemas
Fetch credential schemas
seq
[Connect]
Request credential from an issuer
Issuer's name, requested credential name
Make a connection request
Issuer's address
Relay while hiding the user's physical address
Requested connection info
Approve the connection request
Connection approval
Relay while hiding the user's physical address
Connection request approval
seq
[Create Credentials]
Create public/private key pair
Request credential with public key
Public key
Relay while hiding the user's physical address
Public key
Check identity in the real world
Post public key associated with credential to registry
Public key
Credential
Relay while hiding the user's physical address
Credential
Store credential

Figure 1: Use Case in Temporal Sequence Diagram: Discover, Connect, Create Credential Initiated by Identity Holder.

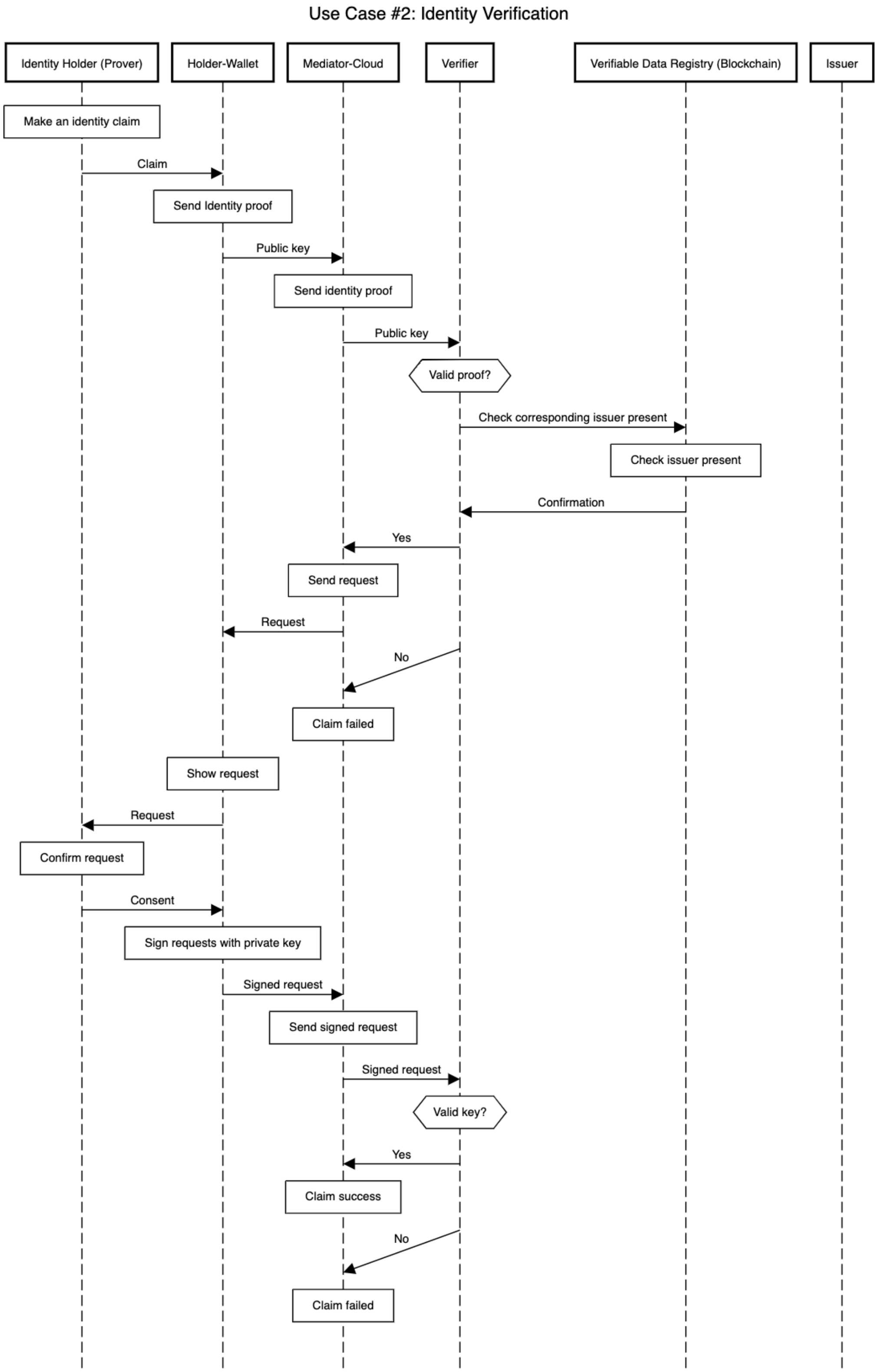

Figure 2: Use Case in Temporal Sequence Diagram: Online Identity Verification Initiated by the Identity Holder.

Table 2: The comparison of SSI solutions based on NFR. Horizontal lines added to improve table readability.

	Provability	Interoperability	Portability	Pseudonymity	Recovery	Scalability	Security	Usability	Protection	Persistence	Minimization	Existence	Control	Consent	Transparency	Access	Convenience	Inclusion	Trust	Biometrics support	Support of IoT	Cost
AusPost DigitalID (https://www.digitalid.com)	✓	✓	✓	?	?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	Free to download
BLOCK ID (https://www.1kosmos.com)	✓	✓	✓	*P*	?	✓	✓	✓	✓	✓	*P*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Paid
Blockcerts (https://www.blockcerts.org)	?	✓	*P*	?	?	✓	?	*P*	✓	✓	✓	✓	✓	✓	✓	✓	*P*	✓	*P*	*P*	*P*	Free to download
Blockstack (https://decentralized-id.com/blockchain/blockstack)	*P*	×	×	*P*	?	✓	*P*	*P*	✓	✓	*P*	✓	✓	?	?	✓	×	✓	*P*	*P*	?	Free: Github is open
Cambridge blockchain (https://www.blockchains.com)	?	✓	✓	✓	?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	?	?	Paid
Connect.me (https://connect.me)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	Free to download from app store
Corda R3 (https://www.r3.com)	*n/a*	✓	?	✓	?	✓	✓	✓	*P*	✓	✓	✓	✓	✓	?	✓	*P*	✓	✓	?	?	Paid
Ethereum (https://ethereum.org)	?	✓	✓	✓	*P*	✓	✓	✓	✓	?	?	✓	✓	?	✓	✓	✓	?	✓	×	✓	Free
EverID (https://everidapp.com)	✓	✓	✓	✓	?	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	?	✓	✓	?	?
Evernym (https://www.evernym.com)	?	✓	✓	✓	?	✓	✓	✓	✓	?	?	?	?	?	?	?	?	?	?	✓	✓	$0, $1000, $2500/month
FIDO (https://fidoalliance.org)	?	✓	✓	✓	✓	✓	✓	✓	✓	?	?	✓	✓	?	✓	?	✓	?	✓	✓	✓	Free
Forticode Cipherise (https://www.forticode.com)	?	✓	✓	✓	✓	✓	✓	✓	✓	?	?	✓	✓	?	✓	?	✓	?	✓	×	×	Free
Hyperledger Indy (https://www.hyperledger.org)	?	✓	✓	✓	✓	✓	✓	✓	✓	?	?	✓	✓	?	✓	?	✓	?	✓	×	✓	Free
IDchainz (https://www.chainzy.com)	✓	✓	✓	✓	?	✓	✓	*P*	✓	✓	×	✓	✓	✓	✓	✓	✓	?	✓	?	*P*	Free
Identity.com (https://www.identity.com)	✓	✓	✓	✓	?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	×	Paid by requester per transaction
IRMA (https://irma.app)	✓	✓	✓	✓	×	×	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	?	*P*	×	×	Free: users/requesters; charges issuers
Jolocom (https://jolocom.io)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	?	✓	Free
KayTrust by Everis (https://www.kaytrust.id)	✓	✓	✓	✓	✓	*P*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	✓	Free for users; charges organizations
KYC Chain/SelfKey (https://kyc-chain.com)	✓	✓	✓	✓	✓	*P*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	×	Charge for using some of the services
LifeID (https://lifeid.io)	✓	✓	✓	✓	✓	✓	✓	*P*	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	✓	Free
OSMA (https://github.com/mattrglobal/osma)	×	✓	✓	×	?	×	*P*	*P*	✓	✓	✓	✓	✓	✓	✓	✓	*P*	*n/a*	*n/a*	×	✓	Free
PDS (https://openpds.media.mit.edu)	✓	✓	✓	✓	*n/a*	✓	✓	✓	✓	*P*	✓	*P*	✓	*P*	*P*	✓	✓	*n/a*	*n/a*	?	✓	?
Peer Mountain (https://peermountain.com)	*P*	✓	✓	✓	*n/a*	✓	✓	✓	✓	?	✓	*n/a*	✓	✓	*P*	✓	✓	✓	✓	?	✓	Free for individuals
reclaimID (https://www.gnunet.org/en/reclaim)	?	✓	✓	✓	?	✓	✓	✓	✓	?	✓	✓	✓	?	✓	✓	✓	?	✓	✓	✓	?
Rem by World Data (https://apps.apple.com/us/app/id1452647818)	?	✓	✓	✓	?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	?	?	✓	Paid
SelfKey (https://selfkey.org)	✓	✓	✓	✓	?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	?	✓	✓	Paid
Shocard (https://www.shocard.com)	✓	✓	✓	✓	*n/a*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	Paid
Sora (https://soraid.com)	✓	✓	✓	✓	?	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	?	?	×	✓	Free for school
Sovrin (https://sovrin.org)	×	✓	×	*P*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	*P*	?
Trinsic (Based on Aries) (https://trinsic.id)	×	✓	×	*P*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	Free
uPort (https://www.uport.me)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	*P*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Paid

(a) Setting expiration dates for identity credentials
(b) Revoke credentials from third party app
(c) Temporarily deactivate an identity
(d) Delete credentials by identity owner
(e) Revoke identity proof by issuer

5 COMPARATIVE STUDY OF SSI SOLUTIONS

This section covers our comparative analysis of existing and emerging SSI solutions against two sets of requirements: non-functional and functional, as outlined in Section 3.

5.1 Comparative Study with Respect to NFR

In Table 2, each row represents one existing or emerging SSI solution. The solutions are alphabetically ordered. Columns represent NFR as listed in Table 1. The first eight columns are the most prominent NFR of SSI. For each SSI solution, the coverage of a given NFR is studied and coded as follows:

- ✓, meaning the solution supports the NFR
- ×, meaning that it does not support the NFR
- *P*, meaning that it partially supports the NFR
- *n/a*, not applicable
- ?, unable to find the answer

One distinction that we should make here is the difference between actual SSI products (e.g., Trinsic based on Aries) versus SSI backends (e.g., Aries). Many newer products are built upon predecessors and backends. Some are built on a different layer and some just add more functionalities. We include a full list for completeness.

5.2 Comparative Study with Respect to FR

Table 3 compares the same solutions with respect to the seven high level ORM functional requirements.

5.3 Discussion

Based on functional and non-functional requirement comparison of the existing SSI solutions, we answer the following questions.

5.3.1 What are the best existing/emerging SSI solutions and why are they superior? SSI solutions can be divided into two categories, that is, blockchain solutions and non-blockchain variants. Blockchain solutions include uPort, IDchainZ, EverID, Sovrin, etc. Non-Blockchain variants are those such as PDS, IRMA, reclaimID, etc. The tables show that, in general, the blockchain-based solutions fulfill more properties than the non-blockchain ones.

Sovrin is one of the best existing SSI solutions. Sovrin has a complete ecosystem built around it, with some important concepts implemented in the Hyperledger project. Different from Hyperledger, Sovrin has the ecosystem well set up for SSI.

Furthermore, Connect.me is one of the best SSI solution available for individuals. The application is very easy to use as well as covers all the bases of FR and NFR. From users' perspective, Connect.me is intuitive and easy to use. It is built based on a huge, developed SSI ecosystem. Connect.me is a digital wallet built by Evernym which is in turn built on Sovrin networks, which is in turn based on Hyperledger Indy. Therefore, the reason that Connect.me supports so many FR and NFR is that it utilizes many layers of preceding products and functionalities, making it more omnipotent.

Table 3: The comparison of SSI solutions based on FR.

	Issuer Discovery	Connection Creation	Credential Creation	Verification w. Credentials	Backup/Recovery	Derive/Share Credentials	Sunset Credentials
AusPost DigitalID	✓	✓	✓	✓	?	✓	*P*
BLOCK ID	✓	✓	✓	✓	?	✓	*P*
Blockcerts	✓	✓	✓	✓	?	✓	?
Blockstack	*P*	✓	*P*	*P*	?	×	✓
Cambridge blockchain	✓	✓	✓	✓	?	?	✓
Connect.me	✓	✓	✓	✓	✓	✓	✓
Corda R3	✓	✓	✓	✓	?	✓	?
Ethereum	✓	✓	?	?	?	?	?
EverID	✓	✓	✓	✓	?	✓	?
Evernym	✓	✓	✓	✓	?	?	✓
FIDO	✓	✓	✓	✓	✓	✓	?
Forticode Cipherise	✓	✓	✓	✓	?	?	✓
Hyperledger Indy	✓	✓	✓	✓	✓	✓	✓
IDchainz	?	✓	✓	✓	?	?	?
Identity.com	✓	✓	✓	✓	?	×	✓
IRMA	✓	✓	✓	✓	×	?	*P*
Jolocom	✓	✓	✓	✓	✓	✓	✓
KayTrust by Everis	✓	✓	✓	✓	✓	×	×
KYC Chain/SelfKey	?	✓	✓	✓	✓	?	×
LifeID	✓	✓	✓	✓	✓	✓	✓
OSMA	✓	✓	✓	✓	✓	✓	✓
PDS	?	?	?	?	×	?	?
Peer Mountain	✓	✓	✓	✓	✓	✓	✓
reclaimID	✓	✓	✓	✓	✓	✓	✓
Rem by World Data	?	✓	✓	✓	?	✓	?
SelfKey	✓	✓	✓	✓	?	✓	?
Shocard	✓	✓	✓	✓	✓	✓	?
Sora	✓	✓	✓	✓	×	?	?
Sovrin	✓	✓	✓	✓	✓	*P*	*P*
Trinsic (Based on Aries)	✓	✓	✓	✓	✓	*P*	*P*
uPort	✓	✓	✓	✓	✓	*P*	*P*

We observe that Jolocom fits all the SSI bases as well. Jolocom has its own Software Development Kit which can be used to easily integrate with an organization's authentication process for secure access as a company needs.

As evident by previous work [5, 7, 8, 15, 23, 26, 36] uPort and ShoCard are very good and popular SSI solutions as well. We would add LifeID for its support of FR and NFR.

5.3.2 What are the worst existing/emerging SSI solutions and why are they inferior? We observe that PDS is one of the worst SSI solutions since it does not offer full integration of the various NFRs and FRs considered. Recovery and Trust are the two important NFRs that PDS does not support.

Blockstack lacks or only partially fulfills the pseudonymity and security requirements, which are crucial for SSI.

5.3.3 What is the minimal support of functional and non-functional requirements that is common across the board? The Blockchain technology already encompasses some of the FR and NFR properties. First, data on the blockchain is not deleted, only appended. This provides a blockchain-based SSI solution the persistence property. In addition, the consensus algorithm that forms the basis of a blockchain gives the transparency property since it provides a global truth that is known to at least 51% of the network.

An SSI solution inevitably should have the existence property. Moreover, both blockchain and non-blockchain based solutions claim that users have full control over their own identity.

FR that are common across the board are: Issuer Discovery, Connection Creation, Credential Creation, and Verification with Credential. NFR that are common across the board are: Access, Control, Transparency, Protection, Interoperability, and Security.

It was particularly difficult to find information on the NFR "recovery", despite the fact that securing and recovering an account in SSI solutions is extremely vital since the IDs are now all accessible from a single wallet. With the same sentiment, "backup credentials" was not a very well-known FR among the solutions studied.

5.3.4 What are some gaps in the existing and emerging SSI solutions that we can identify? Both blockchain-based and other Self-Sovereign Identity solutions show to fulfill most of the evaluation criteria. Blockchain-based solutions definitely meet more requirements, on average, than the others. IRMA shows that it is possible to create an SSI solution without the blockchain technology. To conclude, blockchain technology is a good foundation to build a Self-Sovereign Identity solution, but it is not a necessity [35].

6 EMERGING STANDARDS

Finally, we review some standards related to SSI. Several Non-Profit Organizations are currently advocating for SSI standards as follows. We summarize their reported non-functional requirements.

- Rebooting Web of Trust, RWoT. NFRs include Usability, Deployability, Security, and Unlinkablity.
- W3C Credential Community Group, W3C CCG. NFRs are provability, Discoverabiltiy, Simplicity, and Extendability.
- Decentralized Identity Foundation, DIF. NFRs include Security, Privacy, Decentralization, Transport-agnostic, Routablity, Extensibility, and Efficiency.
- Internet Identity Workshop, IIW. NFRs include Existence, Independence, Self-Determination, Portability, Privacy, Security, Agency, Compensation, Traceability, and Retractability.

7 CONCLUSIONS

We presented the first survey of requirements critical to Self-Sovereign Identity (SSI) and its promise to secure digital identities, reduce risks in digital transactions for all parties and enhance online privacy and trust. The survey defines 22 non-functional requirements and seven groups of functional requirements of SSI and offers a competitive analysis of 31 existing SSI solutions with respect to these requirements. Our competitive analysis upholds the common consensus about the best SSI solutions: Sovrin, Connect.me, uPort, and ShoCard cover most of the requirements. We also add Jolocom and LifeID to this list. Furthermore, our work confirms that existing blockchain-based SSI solutions surpass non-blockchain counterparts. We observed that backup and recovery are the least supported non-functional requirements across all commercial SSI solutions. Our comparative study provides a summary of where SSI solutions stand today and underscores the gaps in the current state of the art, empowering developers and researchers in building better identity management solutions that protect user privacy, manage risk, and enhance trust and security.

ACKNOWLEDGMENTS

The University of Texas Center for Identity wishes to thank Verizon for its collaboration, leadership, and sponsorship in this transformative research. This research is funded in part by Verizon, Inc.

REFERENCES

[1] [n.d.]. Civic Decentralized Reusable KYC Services - Blockchain-Powered. https://www.civic.com/solutions/kyc-services/. (Accessed on 04/11/2019).

[2] [n.d.]. ShoCard Identity Management Use Cases | ShoCard. https://shocard.com/identity-management-use-cases/. (Accessed on 04/11/2019).

[3] DS Baars. 2016. *Towards self-sovereign identity using blockchain technology.* Master's thesis. University of Twente.

[4] Paulo C Bartolomeu, Emanuel Vieira, Seyed M Hosseini, and Joaquim Ferreira. 2019. Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 1173–1180.

[5] Jorge Bernal Bernabe, Jose Luis Canovas, Jose L Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. 2019. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access* 7 (2019), 164908–164940.

[6] Christian Cachin and Marko Vukolić. 2017. Blockchain consensus protocols in the wild. *arXiv preprint arXiv:1707.01873* (2017).

[7] Paul Dunphy and Fabien AP Petitcolas. 2018. A first look at identity management schemes on the blockchain. *IEEE Security & Privacy* 16, 4 (2018), 20–29.

[8] Samia El Haddouti and M Dafir Ech-Cherif El Kettani. 2019. Analysis of identity management systems using blockchain technology. In *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*. IEEE, 1–7.

[9] Jørgen Ellingsen. 2019. *Self-Sovereign Identity Systems: Opportunities and challenges.* Master's thesis. NTNU.

[10] Evernym. [n.d.]. Evernym. https://www.evernym.com

[11] Md Sadek Ferdous, Farida Chowdhury, and Madini O Alassafi. 2019. In search of self-sovereign identity leveraging blockchain technology. *IEEE Access* 7 (2019), 103059–103079.

[12] T. M. Fernández-Caramés and P. Fraga-Lamas. 2018. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* 6 (2018), 32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685

[13] Zhimin Gao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, and Weidong Shi. 2018. Blockchain-based identity management with mobile device. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. 66–70.

[14] Samson Kahsay Gebresilassie, Joseph Rafferty, Philip Morrow, Liming Luke Chen, Mamun Abu-Tair, and Zhan Cui. 2020. Distributed, Secure, Self-Sovereign Identity for IoT Devices. In *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*. IEEE, 1–6.

[15] Andreas Grüner, Alexander Mühle, Tatiana Gayvoronskaya, and Christoph Meinel. 2019. A comparative analysis of trust requirements in decentralized identity management. In *International Conference on Advanced Information Networking and Applications*. Springer, 200–213.

[16] Bahar Houtan, Abdelhakim Senhaji Hafid, and Dimitrios Makrakis. 2020. A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access* 8 (2020), 90478–90494.

[17] Marco Iansiti and Karim R Lakhani. 2017. The truth about blockchain. *Harvard Business Review* 95, 1 (2017), 118–127.

[18] Ori Jacobovitz. 2016. Blockchain for identity management. *The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva* (2016).

[19] Jayana Kaneriya and Hiren Patel. 2020. A Comparative Survey on Blockchain Based Self Sovereign Identity System. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*. IEEE, 1150–1155.

[20] Galia Kondova and Jörn Erbguth. 2020. Self-sovereign identity on public blockchains and the GDPR. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*. 342–345.

[21] Karim R Lakhani and M Iansiti. 2017. The truth about blockchain. *Harvard Business Review* 95 (2017), 118–127.

[22] Shu Yun Lim, Pascal Tankam Fotsing, Abdullah Almasri, Omar Musa, Miss Laiha Mat Kiah, Tan Fong Ang, and Reza Ismail. 2018. Blockchain technology the identity management and authentication service disruptor: a survey. *Int. J. Adv. Sci. Eng. Inf. Technol* 8, 4-2 (2018), 1735–1745.

[23] Yang Liu, Debiao He, Mohammad S Obaidat, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, et al. 2020. Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications* (2020), 102731.

[24] Kumaresan Mudliar, Harshal Parekh, and Prasenjit Bhavathankar. 2018. A comprehensive integration of national identity with blockchain technology. In *2018 International Conference on Communication information and Computing Technology (ICCICT)*. IEEE, 1–6.

[25] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. 2018. A survey on essential components of a self-sovereign identity. *Computer Science Review* 30 (2018), 80–86.

[26] Atif Ghulam Nabi. 2017. Comparative study on identity management methods using blockchain. *University of Zurich* 118 (2017).

[27] Satoshi Nakamoto. 2019. *Bitcoin: A peer-to-peer electronic cash system (2008).* Technical Report. Manubot.

[28] Rima Rana, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2019. An Assessment of Blockchain Identity Solutions: Minimizing Risk and Liability of Authentication. In *2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*. 26–33.

[29] Reza Soltani, Uyen Trang Nguyen, and Aijun An. 2018. 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, 1129–1136.

[30] Quinten Stokkink and Johan Pouwelse. 2018. 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, 1336–1342.

[31] Makoto Takemiya and Bohdan Vanieiev. 2018. Sora identity: Secure, digital identity on the blockchain. In *2018 ieee 42nd annual computer software and applications conference (compsac)*, Vol. 2. IEEE, 582–587.

[32] Andrew Tobin and Drummond Reed. 2016. The inevitable rise of self-sovereign identity. *The Sovrin Foundation* 29 (2016).

[33] Sarah Underwood. 2016. Blockchain beyond bitcoin. *Commun. ACM* 59, 11 (2016), 15–17.

[34] uPort. [n.d.]. uPort. https://www.uport.me

[35] Dirk van Bokkem, Rico Hageman, Gijs Koning, Luat Nguyen, and Naqib Zarin. 2019. Self-sovereign identity solutions: The necessity of blockchain technology. *arXiv preprint arXiv:1904.12816* (2019).

[36] Fennie Wang and Primavera De Filippi. 2020. Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain* 2 (2020), 28.

[37] Razieh Nokhbeh Zaeem and K Suzanne Barber. 2020. How Much Identity Management with Blockchain Would Have Saved Us? A Longitudinal Study of Identity Theft. In *International Conference on Business Information Systems*. Springer, 158–168.

[38] Razieh Nokhbeh Zaeem, Suratna Budalakoti, K Suzanne Barber, Muhibur Rasheed, and Chandrajit Bajaj. 2016. Predicting and explaining identity risk, exposure and cost using the ecosystem of identity attributes. In *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*. IEEE, 1–8.

[39] Razieh Nokhbeh Zaeem, Monisha Manoharan, Yongpeng Yang, and K Suzanne Barber. 2017. Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security* 65 (2017), 50–63.

[40] Jim Zaiss, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2019. Identity Threat Assessment and Prediction. *Journal of Consumer Affairs* 53, 1 (2019), 58–70.

[41] Xiaoyang Zhu and Youakim Badr. 2018. Identity management systems for the internet of things: a survey towards blockchain solutions. *Sensors* 18, 12 (2018), 4215.

[42] Guy Zyskind, Oz Nathan, et al. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*. IEEE, 180–184.