Self-Sovereign Identity Systems

Abylay Satybaldy, Mariusz Nowostawski, Jørgen Ellingsen

Self-Sovereign Identity Systems

Evaluation framework

Abylay Satybaldy, Mariusz Nowostawski, and Jørgen Ellingsen

Computer Science Department, NTNU, Gjøvik, Norway
{abylay.satybaldy, mariusz.nowostawski}@ntnu.no

Abstract. Digital identity systems have been around for almost as long as computers and have evolved with the increased usage of online services. Digital identities have traditionally been used as a way of authenticating to the computer systems at work, or a personal online service, such as an email. Today, our physical existence has a digital counterpart that became an integral part of everyday life. Self-Sovereign Identity (SSI) is the next step in the evolution of the digital identity management systems. The blockchain technology and distributed ledgers have provided necessary building blocks and facilities, that bring us closer to the realisation of an ideal Self-Sovereign Identity. But what exactly is an ideal Self-Sovereign Identity? What are the characteristics? Trade-offs? Here, we propose the framework and methodology that can be used to evaluate, describe, and compare SSI systems. Based on our comparison criteria and the evaluation framework, we present a systematic analytical study of existing SSI systems: uPort, Sovrin, ShoCard, Civic, and Blockstack.

Keywords: Identity management systems · Digital signatures · Peer-to-peer computing · Cryptographic protocols · Computer security.

1 Introduction

Our world becomes increasingly digital and our lives heavily rely on digital systems. Data and information is valuable for governments and industry alike. Digital industry leaders have built their business on targeted marketing and big data for years and the public slowly realises the scope of the impact it has on the social structures, as well as on individuals. The legal systems in different countries take closer look into digital identities and the consequences of people not owing their own information. In Europe, the General Data Protection Regulation (GDPR) and other similar initiatives are put in place to ensure that governments and industry is managing personal information correctly and that the individuals' data is not misused.

As more and more businesses and governmental entities understand the value of data, personally-identifiable information, and digital identities there emerge new challenges related to information security and individual freedoms. There are inherent trade-offs that need to be addressed and explored. On the one hand,

we give up information about us to online services at a rapid rate, for the industry to store, analyse and process it all in new and creative ways. Sometimes to gain financial value, as with targeted marketing and content. Sometimes to achieve political leverage. On the other hand, governments want us to reveal the data and not use privacy-preserving techniques as they can be misused for criminal or terrorism purposes. The data sharing creates opportunities for businesses to reach their target audience with high accuracy. It also offers value to users, through sharing interesting content around topics that they care about.

As a society, we are trading privacy for convenience and the negative effects have just started to shw up. In 2018 the scandal surrounding Facebook and Cambridge Analytica has been revealed and demonstrated how much value and impact social data has. Cambridge Analytica is suspected to have been able to influence the United States 2016 presidential election and the Brexit vote on the British referendum to leave the European Union [7, 8].

While information sharing on social media is a choice, society today expects us to have an online presence and identity. We need to have an account on Google or Apple to use our smart phones and an e-mail address to register additional online accounts for various services. We need identity to access our bank account, to purchase travel tickets and to board an airplane. It is nearly impossible to function without having some form of online identity.

The concept of Self-Sovereign Identity (SSI) is that each user fully controls their own information. Users can add, remove and share attributes at their own discretion. They can share their email to a service provider and then subsequently revoke the rights to use this email. Federated identities made some of these options available by allowing users to register with one provider, and then use that identity to access other services that accepted the same standard. One of the major problems of this approach is that the federated provider(s) users choose to register with has all the user information and control over it. Under self-sovereign identity model, identities must not be held by a singular third-party entity.

When Bitcoin first launched in 2009 it introduced the notion of a decentralised ledger [23]. The blockchain technology and decentralised consensus mechanisms offer technological solution to the 3^{rd} party trust problem. Despite the fact that the majority of industry and academic efforts focus on currencies and transferring ownership of value, there is a growing interest in the use of blockchain and related decentralised technologies for managing identity.

While distributed ledgers have taken identity systems a step closer to an ideal Self-Sovereign Identity, they continue to struggle with some fundamental challenges. Most of the proposed and implemented identity systems are built on the infrastructure of digital currencies, and interactions with the network require some monetary value to be transferred. Those that are not, are partly centralized to manage consensus in the network. An ideal Self-Sovereign Identity System should be free and decentralized and the solutions proposed and implemented today have made compromises [4].

2 Self-Sovereign Identity

Even though, the Self-Sovereign Identity as a term is now well-established, both in academia and in the industry, there is no agreed consensus upon the actual formal definition. Using Peter de Marneffe's principles for Self-Sovereignty [18] and Martin H. Weik's definition of Identity [30], we can describe Self-Sovereign Identity in its simplest form as *a digital representation of the individuals characteristics, description and identifiers where no government, or organization, can violate our right to chose our level privacy or celebrity with our identity attributes.*

Kim Cameron wrote *The Laws of Identity* in 2005 while working as Identity and Access Architect at Microsoft Corporation [9]. *The Laws of Identity* [9] precedes the first distributed ledger [22] and the first mention of the concept Self-Sovereign Identity [4]. While unaware of the technological advance of distributed ledgers in the years to come, Kim Cameron elaborate on Microsoft Passport and how privacy concerns and reliability on a single organization in part lead to the failure of it's mission to become the identity system for the internet. He defines the need for user control, minimal disclosure, and a portable and inter-operable system.

While *The Laws of Identity* is a good foundation for *identity*, one of the first references to identity sovereignty occurred in February 2012 by Moxie Marlinspike in his post about *Sovereign Source Authority* [17]. Subsequently, in 2016 Christopher Allen introduces the term Self-Sovereign Identity and defines it using 10 principles [4]. He expands on *the Laws of Identity* by defining how the identity should exist, why the system and its algorithms must be transparent, and how it must be persistent while still being portable and inter-operable.

Abraham in a whitepaper on Self-Sovereign Identity [1] details the requirements of a Self-Sovereign Identity Concept. The definitions of Abraham align well with Christopher Allen, although Christopher Allens principles are noticeably more comprehensive. Abraham expands on the definition of control and adds *"all access of identity data of a user should be logged for later verification"*. This is trade-off between security and privacy, and should at least be optional for the user.

The concept of Self-Sovereign Identity (SSI) could become the next stage in the evolution in identity management. SSI can be defined as a permanent identity owned and controlled by the person or entity to whom it belongs to without the need to rely on any external administrative authority and without the possibility that this identity can be taken away. That requires not just the inter-operability of a users identity across multiple locations, with the users consent, but also, true user control of that digital identity, and full user autonomy. To accomplish this, a self-sovereign identity must be transportable; it cannot be locked down to one site, provider or locale. This can be enabled by an ecosystem that facilitates the acquisition and recording of attributes, and the propagation of trust among entities leveraging such identities.

3 Evaluation Framework

There is no definitive criteria of how to evaluate SSI systems, but the framework proposed by Allen represents a comprehensive spectrum of SSI requirements, encompassing security, data integrity and privacy. In addition to Allen's work, we have used Cameron's *"The Laws of Identity"* [9] - another well-established evaluation framework for digital identity systems. We decided to add the *"Usability"* law to our evaluation model as the role of user experience is essential in building successful digital identity system. We used these guiding principles as a reference to evaluate the current state of Self-Sovereignty in the published and proposed Self-Sovereign Identity Systems.

The requirements are as follows:

1. *User control and consent*
   Users must control their identities. Users should always be able to refer to it, update it and access their own data. All the claims and personal identity information must be easily retrieved by user when needed. Sharing of personal data must only occur with the consent of the identity owner.
2. *Privacy and protection*
   The rights of users must be protected on the protocol level. The users must be able to choose their privacy model. In order to support users' privacy, disclosure of claims must be minimized. When personal data is disclosed, that disclosure should involve the minimum amount of information necessary to accomplish the task at hand. Given the long-living ambition of SSI implementations, long-term (e.g., post-quantum, information theoretical, etc.) security guarantees must be taken into account.
3. *No trust in central authority*
   Identities must not be held by a single third-party entity, even if it is a trusted entity that is expected to work in the best interest of the user. The necessary guarantees and checks must be part of the protocol layer.
4. *Portability and persistence*
   Identities must be long-lived and preferably last for as long as the identity owner wishes; a user must have a *right to be forgotten*, which means, ability to remove some of the operational data from the SSI system. Personal information and services about identity must be transportable. Transportable identities ensure that the user remains in control of his identity and can also improve an identity's persistence over time. Identity owners should be able to recover their private keys and credentials in case of loss or theft of their primary access device.
5. *Transparency*
   Systems and protocols must be transparent. The systems used to administer and operate a network of identities must be open, both in how they function and in how they are managed and how they are updated. The algorithms should be free, well-known and architecture independent;
6. *Interoperability*
   Identities should be as widely usable as possible. The SSI system should enable global identities which could cross international boundaries and various

system implementations. Transportable identity is sometimes mentioned as a requirement to be fulfilled.

7. *Scalability*
   As the user demands are increasing all the time, the identity systems must be highly scalable. SSI system should be able to maintain its effectiveness throughout even if there are additions or expansions in aspects such as resources or the number of end users without disrupting its functionality.
8. *Usability*
   The user experience must be consistent with user needs and expectations. Identity owners must be able to count on a consistent user experience across various technology platforms and services.

4 State-of-the-art developments in practice

There is a number of start-ups and companies that directly tackle the problem of digital identity management. Examples include Sovrin, uPort, OLYMPUS [24], SelfKey [14], Blockstack, Civic, ShoCard, lifeID [15] and MultiChain [20]. Many of those systems utilize blockchain technology to solve current identity management challenges.

In this review, we evaluate five representative proposals: Sovrin, uPort, ShoCard, Civic and Blockstack. We selected these systems because they provide technical documentation, reports and white papers with the most technical details of their designs, have sizable online communities, and serve similar purpose to the broader landscape of self-sovereign identity management schemes.

4.1 Sovrin

The Sovrin Foundation have set out on a mission to standardize and create an infrastructure for Self-Sovereign identities, using blockchain as storage for Distributed Identities. In theory, anyone can issue or verify an identity [27]. The Sovrin blockchain has been designed only for identity, and is takes the digital trust away from centralized Certificate Authorities (CAs) to a web of trust model. The Sovrin SSI model is not dependent on any particular distributed ledger, but can work with any blockchain that meets the required properties. With Sovrin, trust is established using verifiable claims. As stated by [21] a verifiable claim is a claim shared by any person, organization, or thing that can be instantly verified by the receiving party. Verifiable claims, along with all private data, are stored off-ledger by each self-sovereign identity owner, wherever the owner decides. Sovrin utilizes a permissioned blockchain using nodes called *Stewards* to achieve global consensus. The *Stewards* are approved by the Sovrin Foundation, a non-profit foundation with a board of twelve trustees plus a Technical Governance Board. The open source code base was transferred to the Linux Foundation to become the Hyperledger Indy project [13], and was officially launched with the first 10 *Stewards* in 2017 [28].

Analysis. The main goal of Sovrin is to provide users with full control over all aspects of their digital identity. Each user can choose which attribute credentials are revealed and who can access them (1).

The selective disclosure uses an advanced privacy-enhancing technique known as a zero-knowledge proof (ZKP). Moreover, Sovrin provides pairwise-pseudonymous *Decentralized Identifiers* (DIDs) [25] and public keys for every relationship to protect the privacy of users without sacrificing functionality. By design, each DID is linked to pseudonymous network address provided by private agent, thus, user can securely exchange verifiable claims and any other data with another user over an encrypted private channel. These private agents can operate in the cloud layer or on edge devices (mobile phones, laptops, tablets, etc.). If encrypted data was stored on a public blockchain, the encryption could have been broken in the future (for instance, with quantum computing). Therefore, no private data is stored on the Sovrin ledger which makes the system satisfy the security aspects (2).

Although there is no central authority in the Sovrin Network, users must rely on agencies and on the Stewards. The trust and transparency are addressed through the web of trust and the reputation and non-collusion of the Stewards. Private data is stored on the users device or a chosen agent and does not exist in any service providers system or database (3).

Sovrin expects to create a market for agencies who act on behalf of users and support portability of personal data. Identity owners can recover their private keys and credentials in case of loss as Sovrin provides a decentralized means of revocation using cryptographic accumulators. Data should use system-independent semantic graph formats such as JSON-LD to ensure portability across providers (4).

The Sovrin protocol is based entirely on open standards and software developed with open source licences. The infrastructure support and core software is built on top of the Hyperledger Indy Project [13]. The Sovrin Network is governed by nonprofit Sovrin Trust Framework composed of stewards (volunteer experts) in digital identity, privacy, and policy from around the world (5).

The Sovrin Network consists of stewards from all over the world. The first 24 stewards span 11 countries and include different financial institutions, startups, non-governmental organizations and personal data authorities. As the SSI identity ecosystem expands, new agencies, and new stewards, will join. The Sovrin Foundation expects to collaborate and support interfaces with other existing digital identity systems (6).

To achieve high scalability, the Sovrin Network uses two rings of nodes: a ring of validator nodes to accept write transactions, and a much larger ring of observer nodes running read-only copies of the blockchain to process read requests (7).

User integration is not well-defined. It is unclear how it will happen and it remains an open question. The smart cryptographic tools deployed by the identity system should be transformed and delivered to end-users in a user-friendly way. Sovrin is still in the early development phase, and the user experience

should be thoroughly addressed by developers and services joining the identity ecosystem (8).

4.2 uPort

uPort is an open identity system that allows users to register their own identity on Ethereum, send and request credentials, sign transactions, and securely manage keys and data. The uPort mobile app generates a key pair and deploys three smart contracts for each identity. A *Proxy Contract* is deployed as the user's unique identifier, a *Controller Contract* to provide identity access, and a *Recovery Quorum Contract* to help with recovery of a user's identity should they lose access to it [29]. For key recovery, identity owners must nominate trustees, who can activate a vote to create a new public key via the *Controller Contract*; once a quorum is reached, the controller replaces the lost public key with a new nominated key by invoking a dedicated function of the proxy. The uPort Registry cryptographically links profile data or attributes to a uPort identifier and stores the data as a plain JSON structure [16].

Analysis. uPort provides a framework for identity owners to gather attribute credentials from an ecosystem of identity providers and does not perform any identity proofing. User controls creation of uPortIDs and can share personal information with 3rd parties at their own discretion. The personal information is stored on-device and off-chain with IPFS and is always accessible by the user. uPort provides more control and responsibility over uPortIDs to the hands of its users (1).

For low-value accounts uPort identifiers can be created without disclosure of personal data. Moreover, the lack of inherent link between uPortIDs makes the identity system robust. The JSON profile of user in the registry is visible to public, which could leak information about specific attributes and compromise privacy of users (2).

Users can prove ownership of uPortID without relying on a central authority and the authentication of a user can be done on mobile device. As only identity owner alone has write access, a user can selectively discard their negative attributes such as a criminal conviction, a low credit score, and others that the user does not want to be associated with her or his account. Moreover, uPort has some centralized elements, such as the messaging server to transfer attributes, a push notification center and an application manager. Those can potentially represent a source of censorship or enforcement in the system (3).

uPort provides users with Self-Sovereign Wallet to manage keys, credentials and identity data. The private key is stored on the users mobile device. Support of key recovery protocol helps users to maintain a persistent digital identity even after the loss or theft of mobile device. The key recovery protocol is based on the act of nominated trustees who can raise a vote to set a new public key via the controller smart contract (4).

uPort is an open identity system built on public, permissionless blockchain, Ethereum, and consists of open-source protocols and developer tools (5).

uPort provides tools for building user-centric Ethereum apps. Developers can freely create uPort compatible applications. Moreover, the platform supports simple authentication, single-sign-on, and easy integration for Dapps or other applications. uPort joined the Decentralized Identity Foundation [12], and aims to develop a standard for everyone (6).

uPort is building identity infrastructure on top of the Ethereum, the public blockchain has significant scalability problems. By having identity rooted on-chain uPort gets benefits of the verification and security of the Ethereum. The majority of interactions in uPort including the transactions and the data storage happen off chain which make the system more scalable. However, with the increase of user base and the expansion of system enabling faster and cheaper transactions could become a major hurdle for uPort (7).

Identity owner can access the service by the mobile application which provides a consistent user experience. Also, QR code-scanning feature makes it easy to initiate interactions with a relying party. However, users could find uPort's key recovery protocol and personal data storage schemes too cumbersome or difficult to understand (8).

4.3 ShoCard

ShoCard is a digital identity and authentication platform built on the public Bitcoin blockchain. User's identity information is stored in the form of signed cryptographic hashes in the blockchain. The blockchain is used to validate that information and confirm third parties that have certified the identity of the user. There is no store or central location that holds user's private information and pieces of a user's identification do not need to be spread in other services in order to authenticate or prove ownership of an account. On the blockchain, the user initiates an identity verification handshake with the third party. The information is fully encrypted and placed in a secure data envelope that only the recipient can decrypt. Once both identities are confirmed the transaction can proceed. The system can write five million user records on a publicly verifiable blockchain in 30 minutes. ShoCard was founded in 2015 [11, 26].

Analysis. ShoCard allows users and entities to establish their identities with one another in a secure, verified way. Storage of personal information and sharing with 3rd parties is controlled by the end user (1).

The data is not available in any readable form to any third party or ShoCard without the user sharing information first. ShoCard only uses the blockchain to verify and does not store any personal data on it. ShoCardIDs are bootstrapped with an existing trusted identity document (for example, passport or drivers license). This may make ShoCard less attractive for low-value online accounts (2).

Although there is no central database of logins to become a target for hacking, ShoCard central servers act as an intermediary between users and relying parties. Attribute validation protocol relies on ShoCard servers that write the encrypted, signed credentials onto the blockchain (3).

ShoCard is partly centralized and it creates uncertainty about the longitudinal existence of a ShoCardID. If the ShoCard servers eventually stop working, identity owners would be unable to use their digital identities and credentials. Users are also not supported with cryptographic key management (4).

ShoCard identities are stored in the Bitcoin blockchain which is inherently public and transparent. Users keep their private keys safe on their own smartphones or computers, and they have a public key that can be used by services to verify their ID using ShoCard (5).

Companies can incorporate the ShoCard technology into their existing app or website through a software development kit. ShoCard facilitates for a multitude of different authentication and verification purposes, including KYC, authentication, auditable authorization, and attestation of credentials. Moreover, ShoCard provides enterprise-level identity authentication through mobile device (6).

Shocard relies on public blockchain, but the architecture of ShoCard is designed to be highly-scalable. The system can write five million user records on a publicly verifiable blockchain in 30 minutes. Moreover, ShoCard is designed to be blockchain-independent to position themselves to take advantage of future advances in technology (7).

The authentication process is simple to follow. It begins when a user downloads the app to create their ShoCard ID. They take a picture of a valid, government-issued piece of identification from which ShoCard extracts the personal information. The user confirms the data, self-certifies, and either creates a passcode or opts for their phones fingerprint scan (8).

4.4 Civic

Civic is another system that creates an ecosystem for identity verification services based on a blockchain. Key pairs are generated by a third party wallet, and the identity information is stored on the user's device [31]. Civic and the blockchain only receives hashes of the data, and stores these as a ERC20 tokens on the Ethereum network. Civics network accommodates three different but interdependent entities: users, validators, and service providers. The users are anyone who wishes to use the protocol to register an identity. Validators are responsible for verifying an identity's authenticity on the blockchain's distributed ledger. They can then sell this information to service providers who need to verify their customer's identities, exchanging the data for a Civic token (CVC). CVC will be used as a form of settlement between participants to an identity-related transaction within the ecosystem [10, 19]. Civic is built on the Ethereum blockchain and uses smart contracts to oversee data attestation and payout for this work.

Analysis. Civic's identity platform uses a verified identity for multi-factor authentication on web and mobile apps without the need for usernames or passwords. Users are in control of their secured data and they only have to provide the information they are comfortable sharing (1).

Identity data is encrypted and stored only in the Civic app on user mobile devices. With third-party authenticated identity data, Civic cannot be compelled by a foreign government or criminal organization to invalidate identity data. Personal identity information that was attested are stored in the form of verified hash into a Merkle tree and recorded in the blockchain. The portions of the Merkle tree can selectively be revealed which enhances user control by allowing the identity owner to selectively reveal pieces of personal information in various circumstances (2).

The Civic ecosystem will incentivize participation by trusted identity verification providers known as *Validators* who run the nodes on the public blockchain and sign transactions. Civic reshapes the role of centralization and embraces an open ecosystem of validators. Thus, proposed identity system does not have a single point of failure, but it is not fully decentralized and has similar consensus mechanism as Sovrin (3).

Moreover, identity data is revocable by the authenticating authority. For example, if a user changes their last name, then the former/invalid last name data is revoked on the blockchain by the authenticating authority. Thus, to maintain a persistent digital identity, Civic users should rely on authentication authorities (4).

Civic uses the public blockchain and has no proprietary software or infrastructure which makes the system more transparent (5).

One of the advantages of Civic identity ecosystem is a healthy partner network which includes financial institutions, government entities, and utility companies. Civic wants to create identity verification market where banks, utility companies, local, state, and federal agencies, etc. will be able to verify the attributes of the identity of an individual or business on a blockchain and through the use of smart contracts, validators will be able to price their identity verification and offer them to other participants (6).

Although Civic is built on the Ethereum blockchain, the system retains its effective performance as it has a central role in their ecosystem and uses validators that verify identity information (7).

Users can download mobile app to gain access to Civic's identity platform. Moreover, Civic is planning to launch the *Civic Wallet*. By coupling identity with other features, this wallet will allow users to transact using traditional and cryptocurrencies more securely and easily than with other wallets. However, the project's development is in early stages and wider user adoption has not yet been achieved (8).

4.5 Blockstack

Blockstack is a decentralized computing network and app ecosystem that puts users in control of their identity and data. Instead of relying on servers operated by applications, users are able to provide their computation and storage resources. The Stacks blockchain provides the global consensus and coordination layer for the network and implements the native token of the Blockstack network called the Stacks token. A Blockstack ID is a decentralized

identity which provides a user with a single identity to log into decentralized applications (DApps). Blockstack PBC, a Public Benefit Corp, along with open-source contributors develop the core protocols and developer libraries for Blockstack [2, 3, 6].

Analysis. Applications built on Blockstack enable users to own and control their data directly. Blockstack applications store data with the user (using their private data lockers) and don't need to store any user data or access credentials at the server side (1).

Sharing of content is achieved through a secure and encrypted medium. However, the set of profiles is globally visible and discoverable via the blockchain, which could leak information about specific attributes and compromise privacy of users (2).

Blockstack protocol removes central points of control and failure. Compared to traditional internet applications, the business logic and data processing runs on the client, instead of on centralized servers hosted by application providers (3).

A decentralized storage system, called Gaia [5], enables user-controlled private data lockers. Data on Gaia is encrypted and signed by user-controlled cryptographic keys. Users can host these data lockers on a cloud-provider or other data storage options like private hosting. Importantly, the user controls which provider to use. However, Blockstack does not have the key recovery protocol and users cannot reset their keys in case of loss or theft (4).

Blockstack's first-generation blockchain (Stacks) operates logically on top of the Bitcoin network. The Blockstack open-source repositories contain developer libraries for a number of different platforms. The open-source community behind the project maintains tutorials, API documentation, and system design documents which are available on Github (5).

Blockstack is modular, and developers can easily customize it and integrate alternative technologies. Blockstack takes a full-stack approach and provides default options for all the layers required to develop decentralized applications. As of early 2019, there are more than 100 applications built on Blockstack (6).

To achieve scalability, Blockstack minimizes application logic and data at blockchain layer. The use of off-chain name registrars enables over a hundred users to register in a single blockchain transaction, which could support hundreds of thousands of user registrations per day. The decentralized storage system also scales well because it does not index individual user files or file-chunks but indexes pointers to users storage backends (7).

Blockstack provides users with a universal username that works across all applications without the need for any passwords. However, the Blockstack ecosystem is still in its early days and currently provides only the desktop version of *Blockstack Browser* that allows users to create and manage Blockstack IDs and explore decentralized apps (8).

Table 1. A summary of analysis based on SSI principles

SSI requirements	Sovrin	uPort	ShoCard	Civic	Blockstack
1. User control and consent	✔	✔	✔	✔	✔
2. Privacy and protection	✔	✖	✖	✔	✖
3. No trust in a central authority	✔	✔	✖	✔	✔
4. Portability and persistence	✔	✔	✖	✖	✖
5. Transparency	✔	✔	✔	✔	✔
6. Interoperability	✔	✔	✔	✔	✔
7. Scalability	✔	✖	✔	✔	✔
8. Usability	✖	✔	✔	✔	✖

* A table cell with ✔ indicates that we found evidence that a system complied with a specific requirement, and a cell with ✖ indicates that a system does not fully comply with a specific requirement.

5 Discussion

The definition presented in Section 2 represents requirements for an idealised Self-Sovereign Identity System. Distributed Ledger Technology has provided us with tools to decentralize applications that previously required a trusted third-party. Those new solutions and technologies present an opportunity to rethink how we manage identities and personal information digitally.

The academic landscape on the topic is sparse. Most of the information is published in whitepapers and through industry implementations. A true Self-Sovereign Identity system might have an unappealing non-profit requirement that limit the business validity of SSI as a Service, or SSI for profit.

All the compared Self-Sovereign Identity Systems in Section 4 provide the *identity owner* with full control over their identity and the ability to selectively disclose claims and attributes. They all also embrace the need for trust and transparency by providing source code available for review.

The evaluation in Section 4 and its accompanying Table 1 provide an overview of the current state of the Self-Sovereign Identity landscape. This comparison reveals four major shortcomings that are present in all of the discussed systems.

Centralization. The systems are all based on blockchains and inherit the security of the network making it resistant to third party influence. However, a system is not decentralized just by incorporating partial data storage in a blockchain. The collusion of a large mining pools in Bitcoin network and of validators in permissioned blockchains could potentially introduce censorship problems when maintaining an identity ecosystem. In order to create a truly decentralized system every aspect of the system must be outside any one organizations control. This would reduce the economic viability for organizations to pursue Self-sovereign Identity as a Service and the incentive to do research and development to create the underlying system.

Identity revocation. Identity revocation represents one of the most challenging issues within SSI systems as there is no central server which can easily

revoke users associated cryptographic keys. The systems presented here do not store the anonymous credentials and secret keys. The systems rely on a user to keep the data in a secure storage in his smartphone or PC. On-device storage increases security by being inaccessible for adversaries even in its encrypted state. However, this new approach that relies on nontechnical users to keep credentials safe comes with undeniable risks. The current on-device solution that is used in some of these systems are not persistent through failure or loss of device. For example, Blockstack and ShoCard do not support any end user key management. While Sovrin and uPort have proposed the promising concept of key recovery, their work are still in progress. Creating a secure, cost-efficient and usable management of identities is not a simple task. Self-sovereign identity requires innovative, effective and well-analyzed solutions to support it.

Human integration. Self-sovereign identity systems should be designed to solve the challenges faced by end users. So far, we have seen that the evaluated implementations mainly focus on the underlying technology, not the user interaction. Usable interface and key management and privacy implications for users are not addressed yet in sufficient depth. The future SSI schemes with a novel technological underpinning but developed with impractical end user interaction are unlikely to create widespread uptake.

Economic Barriers. Traditional decentralized blockchains like Bitcoin and Ethereum require miners to reach consensus in the network. These hashing-operations are keeping the network safe by so called *proof of work* mechanism. This relies on having large computational power that any one adversary never will be able to outperform the legitimate network nodes. This computational race is power and hardware expensive and as long as this is the fundamental technology behind a Self-Sovereign Identity System there must be cost associated with usage. One alternative would be to shift the cost over to the service providers, but its hard to find other than economic incentives for them to participate in the system. Running a permissioned ledger like *Sovrin* does create a solution for the cost challenge but is at the same time it shifts the system towards a more centralized model.

6 Conclusion

In this article we have studied and provided our vision of the concept of Self-Sovereign Identity. We have analyzed the current state-of-the-art and investigated existing working implementations: Sovrin, uPort, ShoCard, Civic, and Blockstack. We investigated how these early experiments with SSI address the identity management challenges and how they map to the ideal, proposed SSI model. The current strengths and limitations of SSI systems were discussed by applying a new evaluation framework. The framework has been based on the literature and it represents a synthesised model based on frameworks proposed earlier by other authors. We can see that identity platforms presented in this paper have different level of decentralization and incorporate blockchain to achieve

their goals – in an attempt at creating a true self-sovereign identity management system.

Technology innovations in the area of cryptographic protocols, blockchain and distributed ledger as well as decentralised consensus systems might provide us with the practical building blocks to implement and realise an SSI. The distributed and decentralised ledger creates a jurisdictional space that makes it harder to be manipulated by powerful actors and could provide necessary censorship resistance. A system for truly self-sovereign identities has not yet been achieved in the current state of the field, however the discussed systems represent various attempts that address the core challenges. The recommendation based on the research in this paper would be to re-evaluate how we formally approach the issue. Corporations and for-profit organizations might never benefit economically from a true self-sovereign identity system, and therefore, it is paramount that a non-profit organizations and academia take the lead in the effort and innovate new ways of managing digital identities.

References

1. Abraham, A.: Self-sovereign identity, available at https://www.egiz.gv.at/files/download/Self-Sovereign-Identity-Whitepaper.pdf, Visited 1 March 2018
2. Ali, M., Nelson, J., Shea, R., Freedman, M.J.: Blockstack: A global naming and storage system secured by blockchains. In: 2016 {USENIX} Annual Technical Conference ({USENIX} {ATC} 16). pp. 181–194 (2016)
3. Ali, M., Shea, R., Nelson, J., Freedman, M.J.: Blockstack: A new internet for decentralized applications. Technical Whitepaper Version **1** (2017)
4. Allen, C.: The path to self-sovereign identity. URL:http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (2016)
5. Blockstack: A decentralized storage architecture, available at https://docs.blockstack.org/storage/overview.html, Visited 10 December 2019
6. Blockstack: Blockstack technical whitepaper v 2.0. https://blockstack.org/whitepaper.pdf (May 2019), (Accessed on 21/10/2019)
7. Cadwalladr, C.: The great british brexit robbery: how our democracy was hijacked. The Guardian **7** (2017)
8. Cadwalladr, C., Graham-Harrison, E.: The cambridge analytica files. The Guardian **21**, 6–7 (2018)
9. Cameron, K.: The laws of identity. Microsoft Corp **5**, 8–11 (2005)
10. Capilnean, T.: Evolving trust with applied game theory: Recent white paper update describes trust creation through smart contracts. URL:https://www.civic.com/blog/evolving-trust-with-applied-game-theory-recent-white-paper-update-describes-trust-creation-through-smart-contracts/ (2018)
11. Dunphy, P., Petitcolas, F.A.: A first look at identity management schemes on the blockchain. IEEE Security & Privacy **16**(4), 20–29 (2018)
12. Foundation, D.I.: Decentralized identity foundation, available at https://identity.foundation, Visited 10 December 2019

13. Foundation, L.: Hyperledger indy project, available at https://www.hyperledger.org/projects/hyperledger-indy, Visited 10 December 2019
14. Foundation, T.S.: Selfkey technical whitepaper. https://selfkey.org/wp-content/uploads/2019/03/selfkey-whitepaper-en.pdf (September 2017), (Accessed on 21/10/2019)
15. lifeID: An open-source, blockchain-based platform for self-sovereign identity. https://lifeid.io/whitepaper.pdf (September 2017), (Accessed on 21/10/2019)
16. Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., Sena, M.: Uport: A platform for self-sovereign identity. URL: https://whitepaper. uport. me/uPort_ whitepaper_DRAFT20170221. pdf (2017)
17. Marlinspike, M.: Sovereign source authority (2012), available at http://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html, Visited 23 May 2019
18. de Marneffe, P.: Vice laws and self-sovereignty. Criminal Law and Philosophy **7**(1), 29–41 (Jan 2013). https://doi.org/10.1007/s11572-012-9157-x, https://doi.org/10.1007/s11572-012-9157-x
19. Mountain, P.: Working together for better self-sovereign identity: Civic, selfkey, and peer mountain. URL:https://medium.com/peermountain/working-together-for-better-self-sovereign-identity-civic-selfkey-and-peer-mountain-282bca9a8e4a (2018)
20. MultiChain: Multichain: Open source blockchain platform. https://www.multichain.com (October 2019), (Accessed on 21/10/2019)
21. Nabi, A.G.: Comparative Study on Identity Management Methods Using Blockchain. Master's thesis, University of Zurich (2017)
22. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org (2017), https://bitcoin.org/bitcoin.pdf, available at https://bitcoin.org/bitcoin.pdf, Visited 19 November 2017
23. Nakamoto, S., et al.: Bitcoin: A peer-to-peer electronic cash system. Working Paper (2008), https://bitcoin.org/bitcoin.pdf
24. OLYMPUS, I.: Oblivious identity management for private and user-friendly services. https://olympus-project.eu (October 2019), (Accessed on 21/10/2019)
25. Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M.: Decentralized identifiers (dids). W3C, Credentials Community Group (2017)
26. ShoCard: Identity for a mobile world. URL:https://shocard.com (2019)
27. Sovrin: Control your digital identity. URL:https://sovrin.org (2019)
28. Tobin, A., Reed, D.: The inevitable rise of self-sovereign identity. The Sovrin Foundation **29** (2016)
29. uPort: Open identity system for the decentralized web. URL:https://www.uport.me (2019)
30. Weik, M.H.: Computer Science and Communications Dictionary. Springer US, Boston, MA (2001). https://doi.org/10.1007/1-4020-0613-6_8580, https://doi.org/10.1007/1-4020-0613-6_8580
31. Wiki, B.: Civic. URL:https://en.bitcoinwiki.org/wiki/Civic (2019)