Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

Jørgen Ellingsen

Self-Sovereign Identity Systems

Opportunities and challenges

Master's thesis in Information Security
Supervisor: Assoc. Prof. Mariusz Nowostawski
June 2019

NTNU
Kunnskap for en bedre verden

Jørgen Ellingsen

Self-Sovereign Identity Systems

Opportunities and challenges

Master's thesis in Information Security
Supervisor: Assoc. Prof. Mariusz Nowostawski
June 2019

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Preface

This is a Master Thesis in Information Security at NTNU following the Technology Track. The research was carried out in 2018 and spring of 2019. The idea for this research was introduced by my Supervisor Assoc. Prof. Mariusz Nowostawski and resonated with my thoughts on a worrying trend for privacy and individual online freedom.

01-06-2019

Acknowledgment

I would like to thank my supervisor, Assoc. Prof. Mariusz Nowostawski, for his enthusiasm and guidance on this thesis. I would also like to thank my fellow classmates for their feedback and advice.

J.E.

Abstract

Digital identity systems has been around for almost as long as the computer 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 email. Today, our entire lives have a digital counterpart that become an integral part of everyday life. Self-Sovereign Identity (SSI) is the next step in the evolution of digital identity management systems and distributed ledgers have provided necessary building blocks for Self-Sovereign Identity Systems. But what exactly is an Ideal Self-Sovereign Identity? In this research we propose a definition and set of principles to characterizes the nature of successful SSI systems. Based on our criteria and principles we present a systematic analytical study of the current SSI landscape, represented by uPort, Sovrin, ShoCard, and Civic. A system for truly self-sovereign online identities are not yet archived in the current state of the field. It is our conclusion that it is paramount that a non-profit organization or academia take the reins on this effort and deliver a standardized way of managing online identities.

Contents

List of Figures

List of Tables

1 Introduction

The Internet and the digital revolution is drastically changing the world we live in. We have access to information and services from the other side of the world instantly from a device in our pocket. We can communicate with our friends and family easier than ever and engage in discussion with strangers on any topic we want. It allows us to spread ideas and collaborate and it has excelled our progress and innovation. The internet increasingly form how we live our modern life and where we socialize, learn, and express ourselves.

In this increasingly digital world, information is valuable for governments and industry alike. Digital industry leaders has built their business on targeted marketing and big data for years, and the public is slowly realizing the scope of their digital identity and the consequences of not owing their own information. The General Data Protection Regulation (GDPR) is taking a large step to ensure that governments and industry is managing personal information correctly, and that the individual is in control of their own information.

As more and more businesses and governmental entities understand the value of information, we're faced with a new challenge in information security and individual freedom. We give up information about ourselves to online services at a rapid rate, and the industry is analyzing and storing this data for targeted marketing and content. This is creating great opportunities for businesses to reach their target audience with high accuracy, and the user are experiencing interesting content around topics that they care about.

At the face of it, it looks like a win-win - but we're trading privacy for convenience and the negative effects have just started to show themselves. In 2018 the scandal surrounding Facebook and Cambridge Analytica was front-page news and showed how much value big data can have. Cambridge Analytica is suspected to have been able to influence the United States 2016 presidential election and the vote on the British referendum to leave the European Union [3, 4].

While information sharing on Social Media is a choice, our 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.

Traditional Identity Management and Identity systems are not fit for this new era. Identity information is scattered among a large number of providers, but has been increasingly centralized by some of the larger corporations like Apple, Google and Facebook. While managing identities, they have learned that knowing the audience is a key enabler for targeted marketing - the more they know about the audience, the more efficient marketing they can deliver to their advertisers. It's no longer just the information you willingly enter, its your browsing habits, online purchases, clicks, likes, and all other aspects of your online presence. In addition, we all now carry highly connected phones with large computational power in our pockets, giving information about our real world

habits as well.

When Bitcoin first launched in 2009 they introduced the first Blockchain. This was the closest thing to a decentralized ledger ever seen, and the technology has been pushed forward by innovation for over a decade. In the later years, systems for managing identity on blockchain applications have been proposed, developed, and implemented in various ways, but the majority of industry and academic focus have been on currencies and transferring ownership of value.

An ideal Self-Sovereign Identity System is free and decentralized focusing on individual control and privacy. Most of the proposed and implemented identity systems today are built on the infrastructure of digital currencies. While distributed ledgers have taken identity systems a huge leap closer to an ideal Self-Sovereign Identity, our hypothesis is that the solutions proposed and implemented today have made compromises.

2 Background

Digital identity systems has been around for almost as long as the computer, and have evolved with the increased usage of online services. Digital identities have traditionally been a way of authenticating to the computer system at your work, or possibly a personal online email. Today, our entire lives have a digital counterpart or replacement in an online service. Our professional lives are kept in detailed record on LinkedIn; our work experience, recommendations and professional connections. Facebook have our personal lives; we keep in contact with distant friends, plan and accept invitations to events and have a digital photo album. We manage our banking online, and our phones know us almost better than we know ourselves. Yet, our digital identities are managed and controlled by large corporations.

The introduction of distributed ledgers have a theoretical power to change that, and several companies and foundations have launched identity systems based on blockchain but this has yet to achieved large market adoption.

2.1 Identity, identifiers and authenticators

This research will use [5] definition of Identity as "*The set of known values or attributes that characterizes, identifies, or describes an entity*". An identity in the real world will consist of attributes such as a name, address, birth date, social security number, and driver's license. Some of these attributes can be used as an identifier - it allows us to refer to that identity. Among a group of friends, the first name might be sufficient to refer to an individual, while in the workplace it might be necessary to use the full name. Governmental institutions require something truly unique, like the social security number. An authenticator is an attribute that can be used to determine the legitimacy of someone's claim to that identity, and are often issued by a relevant authority [6].

A digital identity is the corresponding concept in the digital world. The *identity* and the *digital identity* are increasingly linked together, and this is giving rise to important privacy concerns. In Christopher Allen's *Existence* principle, as cited in Section 2.5.2, he points out that the "I" is in the heart of identity as the continuation of "oneself" and that it cannot exist only in digital form [7].

2.2 Identity Management

Identity management is creation, maintenance, and termination of a digital identity in systems and services, and an *Identity Management System* is the processes and tools used for Identity Management. Identity management has traditionally been a component of system security environments to control access and permission, but have in more recent years also included attributes connected to the real world identity.

2.2.1 Traditional Identity Management Systems

The most common user management in online services today is still the traditional localized register of users where the user sign up with their information directly on the website or service. This poses several challenges for both the user and the service provider. For the user, this often forces them to either use the same password on several services, or manage a increasingly large number of passwords. The number of online services an average person uses today, having different passwords for each is a daunting task, often eliminating this option. If the user uses the same password everywhere, chances are one of those services uses bad practices and the password is leaked and the adversary can access all the users accounts using the same password. Additionally, the individual spreads information over an increasingly large number of service providers, and as companies are acquired, merged or involved in cooperation, this information is aggregated and can in combination reveal aspects of your life and identity that was not foreseen. For the service provider, the users are trusting them with personal information that they have to manage and protect responsibly.

The second most used method is federated identities, where the user trusts one identity provider and registers with them. The user can then log in to several services using the same account. Most known applications of this is seen on websites that has the option "Sign in with Facebook/Google". This also poses some challenges; the user relies on one provider to store and protect their data, and also facilitating for tracking and big data gathering as that provider will get information on what services the user is accessing when.

OAuth

The OAuth 1.0 Protocol was proposed in April 2010 by Eran Hammer-Lahav, the second version of the protocol, OAuth 2.0, was proposed in 2012 [8] by Dick Hardt. The protocol provides a standard for accessing server resources on behalf of a resource owner and provide access to server resources without sharing credentials [9]. The traditional client-server model authorizes a user based on their credentials, and allow them access to a server resource. While this was sufficient for the early internet, the increasing use of distributed services and cloud computing require third-party applications to access server resources. A long-lasting access token is generated such that the third-party application can access the resources on the server on behalf of the client, without the client sharing their credentials with the third-party application. OAuth does not have a concept of Identity, and does not provide much value in terms of Identity Management other than being a tool for access management to private resources from an already established identity.

OpenID

The OpenID protocol was developed in 2005 by Brad Fitzpatrick, and it allows users to create an account with a OpenID Provider and then use this account to authenticate with a third-party, known as a Relying Party, without creating new account with new credentials. This works well if the OpenID provider is a trustworthy actor and persist over time, but the user cannot know this in advance. The OpenID Protocol is distinct from the OAuth Protocol as it does have a concept of identity, and provide identity authentication, while OAuth is strictly managing access control of resources.

SAML

The Security Assertion Markup Language is an XML-based framework for sharing identity and security information across security domains. It was primarily developed for web browser single sign-on, but is also designed to be modular and extensible to facilitate usage in other contexts.

Web-of-trust

The web of trust is a public-key authentication system originally built on Pretty Good Privacy (PGP). PGP was primarily developed by Philip R. Zimmerman in the early 90s, where each individual can be a end-user and a certification authority at the same time. This was the tools needed for users to certify other users and create their own web-of-trust [10]. A user can build confidence in their identity by having other users sign their public key [11]. In an identity management system where we distinguish between Users, Identity Providers and Service Providers, we can build on this idea to form a basis of trust around each identity.

We can look at a scenario where a User has their identity verified and signed by visiting the governmental department issuing passports for their citizens. If the user wants proof that they also have a drivers license, and the issuing body (DMV, Statens Vegvesen, e.g.) trusts the department issuing passports, they can sign a proof of license ownership and send it to the user. This opens up for possibilities where the User can visit a small number of Identity Providers and establish a base identity, and then build upon that over the internet.

2.3 Distributed Ledgers

Distributed Ledger Technology (DLT) is a collective term for a immutable ledger that is replicated and synchronized over a large number of nodes where additions to the ledger is agreed upon by consensus in the network. The main advantage of DLTs is the absence of central administrators and data storage, eliminating the need for a trusted third party. The most known type of DLT is blockchain, but in the last few years another approach using Directed Acyclic Graphs (DAG) has been explored and utilized.

2.3.1 Blockchain

Bitcoin was the first application of a blockchain, and is based on a proof-of-work system to represent a majority decision. The miners collect pending transactions in the network and form potential blocks, illustrated in Figure 1, and then, hash the contents of this block with an variable nonce to meet a certain criteria [1]. For Bitcoin this criteria is that the hash must begin with a certain number of zeros, and this number of zeros can be increased or decreased to compensate for variable computational power in the network [1]. The complexity is varied to maintain approximately one block per 10 minutes, and can be modelled as a Poisson process. As long as the majority of computational power is controlled by nodes not trying to attack the network, the blockchain serves as a ledger of witnessed transactions with proved ownership. The computational power required to solve a block reduces the chances of a block being solved by more than one node before the new block is distributed to the entire network. If this still happens, the largest network will generate the

subsequent blocks faster and the longest valid chain will be adopted by the entire network.

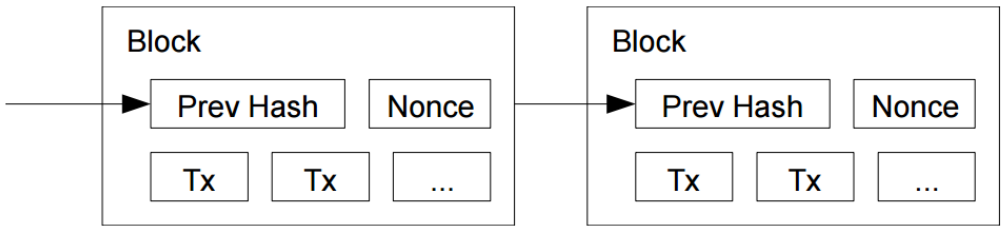


Figure 1: Visualization of blockchain [1]

After the success of Bitcoin, hundreds of other currencies has been introduced with variations and improvements to most aspects of the original technology. One of the big variations from the original technology is Proof-of-Stake as an alternative to Proof-of-Work, which in its essence is consensus reach based on majority stake voting. A nodes vote is weighed with the stake, or number of coins, the node owns - the argument being the more you own, the less likely you are to try to undermine the value of your own investment. The main advantage of Proof-of-Stake is that it is theoretically faster and requires considerably less computational resources.

With the growing success of cryptocurrency, or crypto tokens, the incentive for miners has increased with the price. [12] estimates the total power consumption to be between 100 and 500 MW, the equivalent of a small nation state, and the inefficiency of the Proof-of-Work (PoW) has made Proof-of-Stake (PoS) look like a strong candidate. In the later years, several PoS currencies has been proposed and launched [13, 14, 15] but have yet to achieve large market adoption. PoS implementations still suffer from some major security concerns, and proposed attacks like *nothing at stake* and *long-range attacks* is probably holding the adoption back [13].

2.3.2 Directed Acyclic Graphs

Directed Acyclic Graph (DAG) is a finite graph that can never loop back and is used instead of the 1-dimensional chain of blocks in traditional distributed ledgers for technologies like IOTA [2], NANO [16], and Obyte [17]. The transactions are theoretically instant and without traditional fees, and are designed to scale infinitely. The tangle of IOTA is based on a DAG rather than a traditional chain of blocks, where each transaction is stored separately in the graph, illustrated in Figure 2. One important distinction between blockchain and DAG is that a DAG does only provide partial ordering. In a blockchain each block is verified based on transactions in all previous blocks, with a DAG multiple transactions can be verified simultaneously. For financial transactions total ordering is necessary, but solutions providing only partial order might be suitable for identity management where total ordering is not required. To make a transaction on the IOTA network, the issuing party must approve two previous transactions effectivly doing the Proof-of-Work. This is the basis for the free transactions, as no miner is compensated.

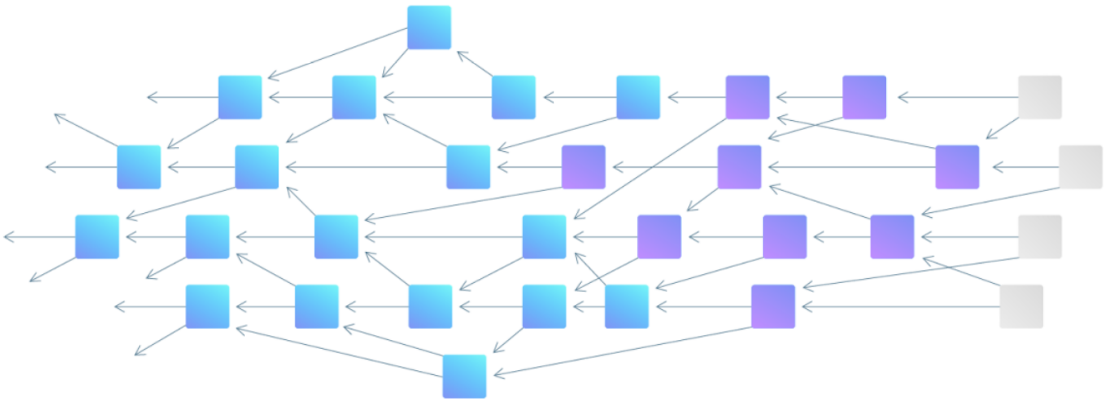


Figure 2: Visualization of the tangle [2]

2.4 Self-Sovereignty

Sovereignty is defined as "*Supreme power or authority*" [18] and Self-Sovereignty is a term for our right to control our own minds and bodies. While this is a great philosophy, this right cannot be unlimited when living in a society where all humans should have the same level of freedom and Self-Sovereignty. J.S. Mill proposed the theory "*The government may limit an adult's liberty against his will only in ways that can be justified as protecting others from harm*" [19] in 1978 limiting the Self-Sovereignty to not include actions that could harm others. Peter de Marneffe points out some drawbacks in this theory and proposes two principles to expand on Mill's theory; (1) *The Prohibition Principle* and (2) *The Opportunity Principle* [20].

The Prohibition Principle

A government violates a person's sovereignty over himself in prohibiting him from making a choice if and only if (a) this choice involves an important form of discretionary control over his own mind or body, and (b) there is no evident and substantial reason of welfare for someone (possibly him) to want him not to make this choice that has much greater weight than his reasons to make it, and (c) prohibiting this choice is not necessary to ensure that someone (possibly him) has adequate control over his own mind or body.

The Opportunity Principle

The government violates a person's sovereignty over himself in having a policy that reduces his opportunities to make a choice if and only if (a) this choice involves an important form of control over his mind or body, and (b) the evident and substantial reasons of welfare for this person now to prefer his situation without this policy have much greater weight than anyone's reasons now to prefer their situation with this policy in place.

2.5 Self-Sovereign Identity

2.5.1 The Laws of Identity

Kim Cameron wrote The Laws of Identity in 2005 while working as Identity and Access Architect at Microsoft Corporation [21]. The Internet is missing the essential capability of an Identity Layer, and [21] defines a metasystem for identity that the author claims could offer the Internet this layer.

The paper discuss the exchange of real-world value online, and how criminals understand the vulnerable nature of the current system. It then outline the partial successes of SSL and Kerberos, and the challenges and obstacles of adding an Identity Layer that extend the entire existing Internet.

> **The Laws of Identity (excerpt)**
>
> **1. User Control and Consent**
>
> *Technical identity systems must only reveal information identifying a user with the user's consent.*
>
> **2. Minimal Disclosure for a Constrained Use**
>
> *The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution.*
>
> **3. Justifiable Parties**
>
> *Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.*
>
> **4. Directed Identity**
>
> *A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.*
>
> **5. Pluralism of Operators and Technologies**
>
> *A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.*
>
> **6. Human Integration**
>
> *The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.*
>
> **7. Consistent Experience Across Contexts**
>
> *The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.*

2.5.2 Christopher Allen's Principles

When Christopher Allen wrote about Self-Sovereign Identity in 2016 [7], he defined it using 10 principles. He expands on The Laws of Identity [21] to further define aspects of identity and privacy

preserving principles.

Christopher Allen's Ten Principles of Self-Sovereign Identity

Existence

Users must have an independent existence. Any self-sovereign identity is ultimately based on the ineffable "I" that's at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the "I" that already exists.

Control

Users must control their identities. Subject to well-understood and secure algorithms that ensure the continued validity of an identity and its claims, the user is the ultimate authority on their identity. They should always be able to refer to it, update it, or even hide it. They must be able to choose celebrity or privacy as they prefer. This doesn't mean that a user controls all of the claims on their identity: other users may make claims about a user, but they should not be central to the identity itself.

Access

Users must have access to their own data. A user must always be able to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers. This does not mean that a user can necessarily modify all the claims associated with his identity, but it does mean they should be aware of them. It also does not mean that users have equal access to others' data, only to their own.

Transparency

Systems and algorithms 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 updated. The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture; anyone should be able to examine how they work.

Persistence

Identities must be long-lived. Preferably, identities should last forever, or at least for as long as the user wishes. Though private keys might need to be rotated and data might need to be changed, the identity remains. In the fast-moving world of the Internet, this goal may not be entirely reasonable, so at the least identities should last until they've been outdated by newer identity systems. This must not contradict a "right to be forgotten"; a user should be able to dispose of an identity if he wishes and claims should be modified or removed as appropriate over time. To do this requires a firm separation between an identity and its claims: they can't be tied forever.

Portability

Information and services about identity must be transportable. Identities must not be held by a singular third-party entity, even if it's a trusted entity that is expected to work in the best interest of the user. The problem is that entities can disappear — and on the Internet, most eventually do. Regimes may change, users may move to different jurisdictions. Transportable identities ensure that the user remains in control of his identity no matter what, and can also improve an identity's persistence over time.

Interoperability

Identities should be as widely usable as possible. Identities are of little value if they only work in limited niches. The goal of a 21st-century digital identity system is to make identity information widely available, crossing international boundaries to create global identities, without losing user control. Thanks to persistence and autonomy these widely available identities can then become continually available.

Consent

Users must agree to the use of their identity. Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user. Though other users such as an employer, a credit bureau, or a friend might present claims, the user must still offer consent for them to become valid. Note that this consent might not be interactive, but it must still be deliberate and well-understood.

Minimalization

Disclosure of claims must be minimized. When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. For example, if only a minimum age is called for, then the exact age should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques, but non-correlatibility is still a very hard (perhaps impossible) task; the best we can do is to use minimalization to support privacy as best as possible.

Protection

The rights of users must be protected. When there is a conflict between the needs of the identity network and the rights of individual users, then the network should err on the side of preserving the freedoms and rights of the individuals over the needs of the network. To ensure this, identity authentication must occur through independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralized manner.

2.5.3 EGIZ's Requirements for Self-Sovereign Identity Systems

EGIZ Whitepaper on Self-Sovereign Identity [22] details the requirements of a Self-Sovereign Identity Concept.

> **EGIZ's Requirements for Self-Sovereign Identity Systems**
>
> **Each individual has to have the full control over her data**
>
> *Each user must have full control over her own identity data. This includes not only what identity data are being stored but also who has access to these data. The user should be able to add or import identity attributes as well as delete or revoke them at her leisure. Also, all access of identity data of a user should be logged for later verification.*
>
> **Ensure security and privacy of user's identity data**
>
> *All identity data have to be stored and processed in a highly secure manner. Additionally, the user's privacy has to be preserved. For instance, unlinkability between the user wallet and her identity data increases the user's privacy.*
>
> **Fully portability of the data**
>
> *This requirement describes that the user should be able to use her identity data wherever they want. For instance, a SSI system can be used as identity provider when the user tries to access an online service.*
>
> **No trust in a central authority is required**
>
> *The underlying blockchain technology solves the required trust related to a central authority.*
>
> **Ensure data integrity**
>
> *The integrity of identity data can be ensured by utilizing the blockchain. This is one of the main advantages using the blockchain technology.*
>
> **Transparency of the identity data is maintained**
>
> *The blockchain technology provides data transparency of all in the blockchain stored data. All changes to the data in the blockchain are fully transparent so that no one can alter of delete data without someone else noticing it.*

3 Related Work

There are not much related work to find in academic papers, specifically related to the definition of Self-Sovereign Identity. In table 1, 2 and 3 lists some of the search terms used and the number of results from Google Scholar, Link Springer and Web Of Knowledge respectively. Table 4 lists the relavant results from these search terms.

Ref #	Search Term	Filter(s)	Results	Relevant
1	Self-Sovereign Identity Definition	Page 1-3	30	3
2	Self-Sovereignty Definition	Page 1-2	20	1
3	Self Sovereignty Definition	Page 1	10	0

Table 1: Search terms and results from scholar.google.com

Ref #	Search Term	Filter(s)	Results	Relevant
1	Self-Sovereign Identity Definition	Discipline: Computer Science	5	0

Table 2: Search terms and results from link.springer.com

Ref #	Search Term	Filter(s)	Results	Relevant
1	Self-Sovereign Identity Definition		0	0
2	Self-Sovereign Identity		3	2

Table 3: Search terms and results from apps.webofknowledge.com

Some researchers have done some relavant work in the field, and the most relevant work is done in [11] were the authors propose several solutions to register identities and attributes in a system built on public ledgers and compare them in terms of privacy, usability and integrity. Two of their solutions satisfy attribute integrity and privacy, and are named *Multi-Casascius* and *Mix-Network*. Both these solutions provide for passive verification, something the authors describes as the possibility to verify the identity only by looking at the public ledger - without the need for additional transactions or information from external sources.

In the broader academic landscape, it is worth mentioning several academic papers that propose Identity Management in blockchain applications. Most notably the proposed implementation

Title	Author(s)	Source
The Inevitable Rise of Self-Sovereign Identity [23]	Tobin, Andrew and Reed, Drummond	Table 1.1
Towards Self-Sovereign Identity using Blockchain Technology [24]	Baars, Djuri	Table 1.1
Self-Sovereign Identity [22]	Abraham, Andreas	1.1
Sovereign God, Sovereign State, Sovereign Self (1990)	Jean Bethke Elshtain	Table 1.2
A survey on essential components of a self-sovereign identity [25]	Muehle, Alexander et al.	Table 3.2
Self-Sovereign Identity framework and Blockchain	Joosten, Rieks	Table 3.2

Table 4: Overview of results from the systematic literature review

described in [26] provides functionality close to what is required in a Self-Sovereign Identity System as described in Section 2.4. They propose three types of actors; *Identity Providers* (IP), *Service Providers* (SP) and *Users* (USR), and require three steps in their protocol; *Setup Phase*, *Enrollment Phase*, and *Operational Phase*. In the *Setup Phase*, the *Identity Provider* chose some set of attributes and makes them publicly available on the Bitcoin ledger. In the *Enrollment Phase*, a *User* brings proof of identity to the *Identity Provider* (Physically or virtually, based on the policy of the *Identity Provider*) that verifies all the attribute values of the claimed identity. This is finalized with a single transaction to the bitcoin ledger, that is considered a *Authentication token*. In the *Operational Phase* the *User* issues a transaction with the authentication token with outputs to both the *Identity Provider* and back to itself for future transactions. The *Service Provider* issues an Acknowledgement of the identity by sending output from the transaction to the *Identity Provider*. The system is more complicated than described here, with possibilities for revocation and suggestions for storage outside of the blockchain by including the hash of the information in the *OP_RETURN* instead of the data itself.

In [26] the system relies on a Discrete Logarithm Representation (DLREP) proposed in [27] to efficiently reveal selected parts of an identity to verifiers, while any other information remains hidden. The DLREP can be used to prove boolean functions about the identity, and will satisfy our principle of *Minimalization*.

4 Self-Sovereign Identity (SSI)

Self-Sovereign Identity as a term is now established both in academia and in the industry, but there is no agreed upon definition of the requirements and specifications of a Self-Sovereign Identity System. As shown in Chapter 2, published papers on self-sovereign identity are few and far between, and they are all from the last few years.

Using Peter de Marneffe's principles for Self-Sovereignty and Martin H. Weik's definition of Identity, we can describe Self-Sovereign Identity in it's 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*.

The Laws of Identity [21] precedes the first distributed ledger [1] and the first mention of the concept Self-Sovereign Identity [7]. 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 interoperable system.

While The Laws of Identity is a good foundation for Identity in it's time, one of the first references to identity sovereignty occurred in February 2012 by Moxie Marlinspike in his post about "Sovereign Source Authority" [28]. Then in 2016 Christopher Allen introduces the term Self-Sovereign Identity, to the best of my knowledge, for the first time [7]. Christopher Allen expands on the Laws of Identity by defining how the identity should exist, why the system and it's algorithms must be transparent, and how it must be persistent while still being portable and interoperable.

The definitions of EGIZ aligns well with Christopher Allen, but Christopher Allen's principles are more comprehensive. EGIZ 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.

EGIZ and Cameron does not address *existence* and how Identities are created. This is something that differentiate Allen's work, where this is explicitly a right reserved for the Identity Owner.

All three of these definitions all omit, conscious or not, the topic of cost. While a free Self-Sovereign Identity System might be unfeasible to develop, maintain and store, the definition in this paper aims to be the *ideal* Self-Sovereign Identity System, and as such, it should be available to all regardless of economic resources.

4.1 Proposed definition

The definition in this paper uses Christopher Allen's principles as base, but without *Existence* and extended with another principle called *Unrestricted*. The description on each principle is re-written to emphasize *why* this principle is important in the context of Self-Sovereign Identity as it is defined above. A Self-Sovereign Identity system is in it's nature an extension of the physical person that owns and controls it, and therefor the first principle is redundant in the definition and the right to create or delete is added to *control*. This will be the definition the self-proclaimed Self-Sovereign Identity Systems are measured against in Chapter 7.

Definition of Self-Sovereign Identity

1. Control

The Identity System must ensure that the Identity Owner is the ultimate authority over their own information. They must be able to add, update or delete attributes at their own discretion. To exist or not in this digital form must be both a right and a choice.

2. Access

An Identity Owner must be able to retrieve all attributes and claims related to their identity at any given time. Verifications and proof of ownership must be stored in a redundant and decentralized way such that a Identity Owner with connectivity can link their attributes to verifications and prove ownership when needed.

3. Transparency

The systems and algorithms must be well documented and open-source such that anyone can examine how they work. If not, there is no certainty that the system works like advertised - and the Identity Owner does not know if they fully control their Identity.

4. Persistence

Identities must be long-lived and preferably last for as long as the Identity Owner wishes. There must be a separation between the identity and its claims so that even if verifications are retracted, the identity itself lives on.

5. Portability

The system must use established and known structures for data storage so that the Identity Owner can retrieve and move their information to another system or storage medium when needed.

6. Interoperability

Identities should be as widely usable as possible and facilitate for characteristics, descriptions and identifiers in all formats.

7. Consent

Identity Owners must agree to the use of their identity, either by making attributes public or by manually accepting all requests.

8. Minimalization

Disclosure of claims must be minimized so that the Identity Owner can chose to only present the information required by the Service provider. This must also include the ability for zero-knowledge proof for boolean statements.

9. Protection

The rights of users must be protected by independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralized manner.

10. Unrestricted

Identity must be free and unrestricted. We all have an identity, and a true global identity system must be available to all. There should be no economical burden and no gatekeepers, other than the required technological restrictions of a device and connectivity.

5 Components in a DLT-based SSI

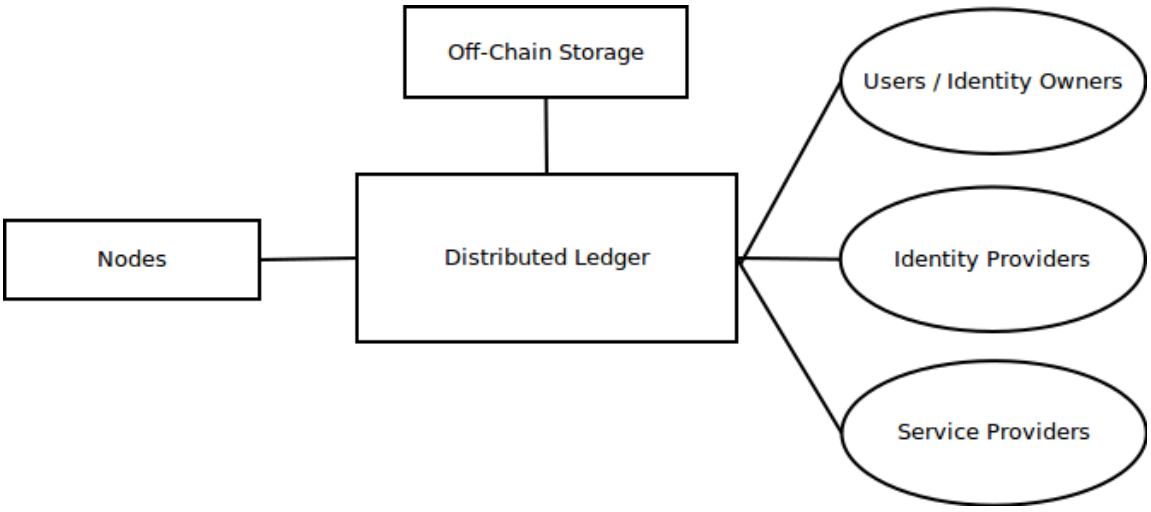


Figure 3: Components of a DLT-Based Self-Sovereign Identity System

A Self-Sovereign Identity system based on a Distributed Ledger have several essential components and functional requirements. The distributed ledger replaces the trusted third party that we all are accustomed to both online and offline. While distributed ledgers have been used for close to a decade, it needs some alterations to be able to protect personal identifiable information. Traditional distributed ledgers have two types of users; network nodes (also often referred to as miners) and users that own some value stored on the ledger. In an identity system we still need the network nodes, but we can split the users into Identity Owners, Identity Providers and Service Providers. And to be a fully functional system for identity management we need off-chain storage for documents and images, and we need a system for enrollment, verification and revocation of claim and identities.

While these components are essential for a Self-Sovereign Identity system, they can be named and grouped together differently while still providing the same services. As an example, some SSI Systems does not differentiate between Users, Identity Providers and Service Providers, but instead have only Identity Owners that can act in any of the above roles. Others split up the Network Nodes in specialized capacities, such as having some nodes appending new events to the network, while others serves as lookup-nodes for read requests.

5.1 Stakeholders

The stakeholders make up the distributed network of contributors and beneficiaries in the identity system. Together they build a web of trust to minimize information leakage while still providing sufficient proof that the attributes of users are genuine and verified.

5.1.1 Identity Owners

The identity owners, often referred to as Users, are the individuals that owns the online identity. They must be the ultimate authority over the Identity.

5.1.2 Identity Providers

Identity Providers are individuals, companies, or governmental bodies that verify claims that a user wants associated with their identity. Its essential for Identity Providers to have or build trust among Service Providers.

5.1.3 Service Providers

When a Service Provider deliverers a service that requires the user to prove some attribute or claim to access, they can grant access or privileges based on verified claims in the ledger. This requires the Service Provider to place trust in an Identity Provider, but allows them to accept users into their service without more knowledge than strictly needed.

5.2 Functional Requirements

5.2.1 Enrollment

The process of creating and adding the Identity base in the system.

5.2.2 Claims

Attributes related to the Identity claimed by the Identity Owner.

5.2.3 Verification

Claims can be verified by another party to provide trust to the claimed attribute.

5.2.4 Access granting

The right to control access to an attribute or zero-knowledge proof about their own Identity.

5.2.5 Revocation

The right to remove access to an attribute or zero-knowledge proof about their own Identity.

5.2.6 Privacy and segregation of attributes

Separation of attributes and Identity such that they cannot be linked without the Identity Owners consent.

5.2.7 Recovery

The ability to recover a lost account if a user loses access to their private key, there should be some sort of model for how a recovery process can be used to rotate key-pairs.

5.3 Distributed Ledger

5.3.1 Protocols

One of the main components of a working distributed ledgers are the protocols that validates additions to the ledger. Each addition to the ledger are associated with an identity and digitally signed by the identity owner. In addition, the appended data is hashed together with the previous hash, creating a chain of hashes that breaks if anything is manipulated after its accepted into the network. For each new addition of data, each node is validating it based on the protocols and cryptographic primitives that the ledger relies on.

5.3.2 Consensus Algorithm

In the absence of a central authority, the network must establish consensus on the history of events in the ledger. This consensus is traditionally achieved among the nodes in the network by competing to "solve" the next block. The network nodes store and update the ledger by verifying new information based on the public keys of the other stakeholders. Nodes must validate and relay all new information to neighbouring nodes and in addition work as lookup-nodes for read requests to the ledger. Their role is both to store the entire ledger and operate the consensus algorithms to agree on additions.

5.3.3 Off-Chain Storage

For a truly global decentralized identity management system, the amount of data stored in the actual ledger would be substantial even only short text attributes. For a sustainable solution for images, large text records, biometric templates, and other larger data attributes and claims, there is a requirement to support some sort of off-chain storage.

6 Available Self-Sovereign Identity Systems

This is a non-comprehensive list over available Self-Sovereign Identity Systems. These systems were selected because, individually, they serve as key examples of innovative design decisions. Together they cover the broader landscape of blockchain-based Self-sovereign identity management schemes. The analysis for each system is based on the principles defined in Section 4.1.

6.1 uPort

uPort is a platform for user centric identity and communication using the Ethereum blockchain [29]. 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. To be able to recover, identity owners must add trustees who can activate a vote to regenerate the a new key-pair. The uPort Registry cryptographically links profile data or attributes to a uPort identitier and stores the data as JSON structures [30].

Analysis

Users can create and control their own identity (1) and can share personal information with third-parties at their own discretion (7). The core Identity is stored on the Ethereum blockchain and duplicated on thousands and thousands of computers around the world (4). The personal information is stored on-device and off-chain with IPFS and is always accessible by the user (2). uPort has some centralized elements (9), such as the messaging server to transfer attributes, a push notification center and an application manager (5). uPort is built on open standards and open source libraries (3), and developers can freely create uPort compatible applications (6). uPort has the ability to generate JWT tokens as verification on claims and provides "Selective Disclosure Request" for sensitive information. The JSON profile of user in the registry is visible to the public, which could leak information about specific attributes and compromise privacy of users (8). The cost of usage is bound to the cost of gas on the Ethereum network (10).

6.2 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 such that anyone can issue or verify it [23]. The Sovrin blockchain has been implemented only for identity, and is taking steps to move 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 fundamental principles. Sovrin has implemented

their identity system in a specific instantiation of Hyperledger's Indy project. 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, and was officially launched with the first 10 Stewards on July 31, 2017.

Analysis

While the ledger itself is partly decentralized and replicated over a number of nodes, a permissioned ledger requires a governing body (9). The transparency and trust are managed through the reputation of the Stweards. Identities are free to create, but Sovrin will support "Premium Claims" to create economic incentive for issuers (10). Attributes can be share only with consent from the Identity Owner (7), and while the Foundation has power over the ledger, all private information is encrypted by the Identity Owners own keys and unavailable to Stewards and administrators. All code that operates, validates and provide access to the ledger is Open Source (3) and can be deployed on any distributed ledger that meets the requirements (6). Sovrin decentralised identifiers and public keys for every relationship the provide selective disclosure of verifiable claims based on zero-knowledge proof (8). Private data is stored on the users device or a chosen Agent and does not exist in any service provider's system or database (2) and "Local Containers" can be utilized to maintain an encrypted backup on private storage or with an Agent (4). The Identity Owner's key pair is the only way to unlock their Identity and everything that can be done with it (1) [31]. Data should use system-independent semantic graph formats such as JSON-LD to ensure portability across providers (5).

6.3 Civic

Civic is creating an ecosystem for low-cost access to Identity Verification (IDV) and Know Your Customer (KYC) processes. Civic is created as a ERC20 token on the Ethereum network, and key pairs are generated by a third party wallet. Identity information is stored on the user's device [32], and civic and the blockchain only receives hashes of the data and stores this in the blockchain. The User provides identity information to a validator for validation, and signs up for a service by providing proof of identity to a service provider (requestor) [32]. Attested personal identity information is stored in a Merkle tree and recorded in the blockchain [32]. A token called CVC is used to reward and pay for services in ecosystem, and are created in a fixed supply.

Analysis

The Identity is stored on the user's own device (1) so the user will always have access to their own information when the device is in their possession (2). While the actual data is reliant on the user ensuring long-lasting storage (4), Civic uses the public Ethereum blockchain and has no proprietary software or infrastructure (3) and the network is wide-spread and likely to be available in the foreseeable future. Information can be used in applications connected to the Civic ecosystem (9),

but is not portable outside to any other services (5). Civic can provide passwordless login as well as claimed and verified identity attributes for all types of services (6). As all information is stored on the user's device, the Identity Owner must chose what information and to who information is shared (7). The portions of the Merkle tree can selectively be revealed with hashes for any elements the User prefers not to reveal (8). The cost of usage is bound to the cost of gas on the Ethereum network as a minimum, and with the added expense with CVC-tokens for some services (10).

6.4 ShoCard

ShoCard was founded in 2015 and is a blockchain-based Identity Management ecosystem providing authentication, auditable authorization and attestation of credentials [33]. ShoCard only uses the blockchain to verify and does not store any personal data on the blockchain. They provide their own SDKs for mobile devices that perform all verifications checks locally and independently retrieve blockchain records directly so that no other service must be trusted. ShoCard supports zero-knowledge registration and login, as well as a full KYC process.

Analysis

ShoCard is able to utilize multiple blockchains at the same time and adopt new ones in the future [33] (5) but it is partly centralized (9) and this is creates uncertainty for future availability (4). A public blockchain is inherently accessible but access to identity data could be disrupted by issues with the ShoCard service (2). The Users own and control their own digital identity (1), and they decide with whom and when to share their personal data (7). ShoCard facilitates for a multitude of different authentication and verification purposes, including KYC, authentication, auditable authorization, and attestation of credentials (6). ShoCard has been issued four patents and have nine pending and eleven additional provisional patents filed but is still sharing its technology and algorithms through open standards as well as open source (3). The User can control how much of their data is shared and are not required to expose irrelevant private data (8). ShoCard is blockchain independent, but is currently operating mainly on public ledger with the accompanying transaction fees (10).

7 Comparison

The definition of Self-Sovereign Identity as described in Section 4.1 represents an ideal system for identity management and is used as characteristics of the comparison. While distributed ledgers given us a tool to remove the trusted third party and move the control back to the identity owner, the solutions presented in Chapter 6 all have some shortcomings. The comparison of the four Self-Sovereign Identity Systems are presented in Table 5.

All the compared Self-Sovereign Identity Systems 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.

To some degree they all also provide portability and persistence by using well established data formats and self-hosting of data, while *uPort* also facilitates for storage in IPFS and *Sovrin* enables storage and backup with trusted network Agents. Both *uPort* and *Civic* is storing the identity information on the user device, which provides full control over the information while utilizing the blockchains for verified and signed hashes of the data. *Sovrin* is storing most of the data encrypted on chain, which provides better accessibility and usage without interactions with a mobile device. *Sovrin* provides functionality to use almost any form of storage but have, to the best of my knowledge, not landed on a primary solution yet. This will be essential for mass adoption, assuming that the system will be used for medical records, official documents and other files that is unfeasible to store distribute among all nodes.

Civic and *uPort* both use the Ethereum blockchain and inherit the security and computational power of the network making it very resistant to third party influence, while *Sovrin* and *ShoCard* is designed to be blockchain-independent to position themselves to take advantage of future advances in technology. The systems are all usable for a wide range of identity needs, and non of them are created for a niche market.

uPort is using Etherium's smart contracts and the usage price is based on the current Ether price, while *Civic* is using their own ERC20 token that have its own fluctuation and demand-driven economy in the addition to the ether price of making ERC20 transaction on the network. *ShoCard* have their own pricing structure with a yearly fee and a per-use cost for services like KYC.

All of these systems leverages some decentralization techniques but none of them are truly decentralized. *Sovrin* is running on a Hyperledger blockchain and is reaching network consensus between approved nodes, *Stewards*, that are run by organizations with a interest in keeping the network healthy. While this removes the economic aspect and usage price, the trade-off is a network that is not truly decentralized as each node must be accepted by the Sovrin Foundation. *ShoCard* utilizes a centralized server making them an integral part of the chain. *Civic* also have a central

role in their ecosystem and uses verification providers known as *Validators* that can verify identity information.

Criteria	Sovrin	uPort	Civic	ShoCard
1. Control	(+) Identity Owner's key pair is the only way to unlock their Identity and everything that can be done with it.	(+) Users create and control their own identity.	(+) The Identity information is stored on the user's own device, and is under their control.	(+) The Users create, own and control their own digital identity.
2. Access	(+) Private data is stored on the users device or a chosen Agent and does not exist in any service provider's system or database.	(+) Personal information is stored on-device and off-chain with IPFS and is always accessible by the user.	(—) The user will always have access to their own information if their device is in their possession.	(—) A public blockchain is inherently accessible but access to identity data could be disrupted by issues with the ShoCard service.
3. Transparency	(+) All code that operates, validates and provide access to the ledger is Open Source.	(+) uPort is built on open standards and open source libraries.	(+) Civic uses the public Ethereum blockchain and has no proprietary software or infrastructure.	(+) ShoCard has been issued four patents and have nine pending and eleven additional provisional patents filed but is still sharing its technology and algorithms through open standards as well as open source.
4. Persistence	(+) "Local Containers" can be utilized to maintain an encrypted backup on private storage or with an Agent	(+) The core Identity is stored on the Ethereum blockchain and duplicated on thousands and thousands of computers around the world.	(+) The Etherium network is wide-spread and likely to be available in the foreseeable future, while the actual data is reliant on the user ensuring long-lasting storage.	(—) Is partly centralized and reliant on ShoCard specific infrastructure. This is a concern for future existence of a ShoCard ID.
5. Portability	(+) Data should use system-independent semantic graph formats such as JSON-LD to ensure portability across providers.	(+) Private data is stored on the user's device and uses a JSON format.	(—) Information can be used in applications connected to the Civic ecosystem, but is not portable outside to any other services.	(+) ShoCard is able to utilize multiple blockchains at the same time and adopt new ones in the future.
6. Interoperability	(+) Sovrin local storage and Agents to store any attribute of an Identity.	(+) uPort work with all sorts of attributes and has the ability to generate JWT tokens as verification on claims.	(+) Civic can provide passwordless login as well as claimed and verified identity attributes for all types of services.	(+) ShoCard facilitates for a multitude of different authentication and verification purposes, including KYC, authentication, and attestation of credentials.
7. Consent	(+) Attributes can be share only with consent from the Identity Owner.	(+) Users can share information with third-parties at their own discretion.	(+) As all information is stored on the user's device, the Identity Owner must chose what information and to who information is shared.	(+) Users decide with whom and when to share their personal data.
8. Minimalization	(+) Sovrin uses decentralised identifiers and public keys for every relationship the provide selective disclosure of verifiable claims based on zero-knowledge proof.	(+) uPort has "Selective Disclosure Request" for sensitive information, but the JSON profile of user in the registry is visible to the public, which could leak information about specific attributes and compromise privacy of users.	(+) The portions of the Merkle tree can selectively be revealed with hashes for any elements the User prefers not to reveal.	(+) The User can control how much of their data is shared and are not required to expose irrelevant private data.
9. Protection	(—) While the ledger itself is partly decentralized and replicated over a number of nodes, a permissioned ledger requires a governing body.	(—) Some centralized elements such as the messaging server to transfer attributes, a push notification center and an application manager.	(—) Information can be used in applications connected to the Civic ecosystem.	(—) ShoCard central servers makes it partly centralized.
10. Unrestricted	(+) Identities are free to create and use, but Sovrin will support "Permium Claims" to create economic incentive for issuers.	(—) The cost of usage is bound to the cost of gas on the Ethereum network.	(—) The cost of usage is bound to the cost of gas on the Ethereum network as a minimum, and with the possibility of CVC-tokens for some services.	(—) ShoCard is blockchain independent, but is currently operating mainly on public ledger with the accompanying transaction fees.

Table 5: Tabular comparison of Self-Sovereign Identity Systems currently available

8 Discussion

The definition presented in Section 4.1 represent requirements for an ideal Self-Sovereign Identity System. Distributed Ledger Technology has given the industry a tool to finally decentralize applications that previously required a trusted third-party, and this has presented an opportunity to rethink how we manage identities and personal information online.

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

The comparison in Chapter 4 and its accompanying Table 5 give an overview of the current state of the Self-Sovereign Identity landscape. This comparison revealed three major shortcomings that in one way or another is present in all the compared solutions.

Centralization

A system is not decentralized just by incorporating partial storage in a blockchain, and to create a truly decentralized system every aspect of the system must be outside any one organizations control when released. 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.

Localized Storage

On-device storage increases security by being inaccessible for adversaries even in its encrypted state. In addition, a ledger that is replicated over thousands of nodes can't contain all aspects of every Identity Owners attributes such as images and biometric templates in a sustainable way. But, the current on-device solution that is used in many of these systems are not persistent through failure or loss of device. The Interplanetary File System as implemented by *uPort* might provide an acceptable peer-to-peer solution for storage, but requires extensive research to determine the exact implementation.

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 having so much 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 highly unlikely that they

will agree to foot the bill in exchange for less data about their users. Running a permissioned ledger like *Sovrin* does create a solution for the cost challenge but is at the same time shifting the system in a far more centralized state. Blockchains with Proof-of-Stake consensus also requires a stake, usually a monetary value, associated with an account. There might be an opportunity for reputation stakes, but this have to be explored further. During Section 2.3 the recently explored technology of Directed Acyclic Graphs present an opportunity where these ledgers can be utilized for verification and hash storage while piggybacking on a healthy network driven by economic value - while "paying" for the service with a small amount of computational power directly from our own devices. One of the main concerns around a DAC based approach is the succession of transactions. In a regular blockchain, the block number clearly states what order bulks of transactions occurred, while in a DAC it can be impossible to determine the order of two transactions with respect to time. If the attribute of an identity is confirmed by an identity provider that the service provider trusts, the time of this confirmation is irrelevant for most attributes that are claimed. I argue that this does not pose as much of an issue for Identity Systems unless verifications and revoking of verifications must be instant or sequential.

9 Conclusion

We can achieve most of the proposed principles in Section 4.1 with a system based on Public Key Infrastructure and agreed upon protocols without any Distributed Ledger Technology — as long as the Identity is created by the Identity Provider. A Distributed Ledger might be the most practical implementation regardless, but if the Identity Provider is limited to verifying claims for the user self-created Identity, the Identity and it's verifications must be stored in a single common source of truth that can be trusted by all parties and replicated to a single global state. The distributed ledger creates a jurisdictional space that cannot be manipulated by powerful actors. A system for truly self-sovereign online identities are not yet archived in the current state of the field. The recommendation based on the research in this thesis would be to reevaluate how we approach the issue. Corporations and for-profit organizations will never benefit economically from a truly self-sovereign identity system, and therefor it is paramount that a non-profit organization or academia take the reins on this effort and deliver a standardized way of managing online identities.

9.1 Future Work

9.1.1 Standardizing

Instead of one organization creating an entire system for Self-Sovereign Identities, I propose that academia and non-profit organizations collaborate on a standard for managing identities and propose it as a Internet Standard. Organizations can then create implementations, for-profit or non-profit, delivering services on the decentralized foundation.

9.1.2 Identity Management on DAG-based DLTs

Explore the validity of Identity Management on DAG-based DLTs such as IOTA, NANO or Obyte. Can we successfully "piggyback" on this established network to create a truly Self-Sovereign Identity System were the only payment required is a few seconds of computing power?

9.1.3 Proof-of-Stake based on reputation

Explore blockchains with Proof-of-Stake and see if stake based on reputation can work for Self-Sovereign Identity Systems.

9.1.4 Storage

Is Interplanetary File System the best solution for distributed peer-to-peer storage of encrypted data? What other alternativs exist, and what are the requirements for such a system in a Self-Sovereign Identity System setting?

9.1.5 Actual cost of using current SSI Systems

What does it actually cost to have and use an Identity on uPort, ShoCard and Civic?

9.1.6 In-depth analysis of SSI Systems

in-depth analysis with state-diagrams and information flows. Review the specific protocols that would fit to achieve specific objectives under a specific trust models.

Bibliography

[1] Nakamoto, S. 2017. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org, Available at https://bitcoin.org/bitcoin.pdf, Visited 19 November 2017. URL: https://bitcoin.org/bitcoin.pdf.

[2] Popov, S. The tangle. Available at https://iota.org/IOTA_Whitepaper.pdf, Visited 12 December 2017. URL: https://iota.org/IOTA_Whitepaper.pdf.

[3] Cadwalladr, C. 2017. The great british brexit robbery: how our democracy was hijacked. *The Guardian*, 7.

[4] Cadwalladr, C. & Graham-Harrison, E. 2018. The cambridge analytica files. *The Guardian*, 21, 6–7.

[5] Weik, M. H. *Computer Science and Communications Dictionary*. Springer US, Boston, MA, 2001. URL: https://doi.org/10.1007/1-4020-0613-6_8580, doi:10.1007/1-4020-0613-6_8580.

[6] Just, M. *Identity Management*, 586–587. Springer US, Boston, MA, 2011. URL: https://doi.org/10.1007/978-1-4419-5906-5_78, doi:10.1007/978-1-4419-5906-5_78.

[7] Allen, C. 2016. Self-sovereign identity principles. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[8] Hardt, D. The OAuth 2.0 Authorization Framework. RFC 6749, RFC Editor, October 2012. URL: https://tools.ietf.org/pdf/rfc6749.pdf.

[9] Hammer-Lahav, E. The OAuth 1.0 Protocol. RFC 5849, RFC Editor, April 2010. URL: https://tools.ietf.org/pdf/rfc5849.pdf.

[10] Heinrich, C. *Pretty Good Privacy (PGP)*, 955–958. Springer US, Boston, MA, 2011. URL: https://doi.org/10.1007/978-1-4419-5906-5_215, doi:10.1007/978-1-4419-5906-5_215.

[11] Azouvi, S., Al-Bassam, M., & Meiklejohn, S. *Who Am I? Secure Identity Registration on Distributed Ledgers*, 373–389. Springer International Publishing, Cham, 2017. URL: https://doi.org/10.1007/978-3-319-67816-0_21, doi:10.1007/978-3-319-67816-0_21.

[12] Vranken, H. 2017. Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability*, 28(Supplement C), 1 – 9. Sustainability governance. URL: http://www.sciencedirect.com/science/article/pii/S1877343517300015, doi:https://doi.org/10.1016/j.cosust.2017.04.011.

[13] Li, W., Andreina, S., Bohli, J.-M., & Karame, G. *Securing Proof-of-Stake Blockchain Protocols*, 297–315. Springer International Publishing, Cham, 2017. URL: https://doi.org/10.1007/978-3-319-67816-0_17, doi:10.1007/978-3-319-67816-0_17.

[14] Community. 2014. Nxt whitepaper. Available at https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf, Visited 13 December 2017.

[15] Vasin, P. Blackcoin's proof-of-stake protocol v2. Available at http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf, Visited 13 December 2017.

[16] LeMahieu, C. Nano: A feeless distributed cryptocurrency network. Available at https://nano.org/en/whitepaper, Visited 1 June 2019. URL: https://nano.org/en/whitepaper.

[17] Churyumov, A. Byteball. Available at https://obyte.org/Byteball.pdf, Visited 1 June 2019. URL: https://obyte.org/Byteball.pdf.

[18] Oxford Dictionary. Definition of sovereignty in english. Available at https://en.oxforddictionaries.com/definition/sovereignty, Visited 23 May 2019.

[19] Mill, J. S. *On Liberty*. Hackett Publishing, 1978.

[20] de Marneffe, P. Jan 2013. Vice laws and self-sovereignty. *Criminal Law and Philosophy*, 7(1), 29–41. URL: https://doi.org/10.1007/s11572-012-9157-x, doi:10.1007/s11572-012-9157-x.

[21] Cameron, K. 2005. The laws of identity. *Microsoft Corp*, 5, 8–11.

[22] Abraham, A. Self-sovereign identity. Available at https://www.egiz.gv.at/files/download/Self-Sovereign-Identity-Whitepaper.pdf, Visited 1 March 2018.

[23] Sovrin Foundation. 2018. Sovrin: A protocol and token for self-sovereign identity and decentralized trust. Available at https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf, Visited 2 March 2018.

[24] Baars, D. Towards Self-Sovereign Identity using Blockchain Technology. Master's thesis, University of Twente, 5, Drienerlolaan, 7522 NB Enschede, Nederland, 2016.

[25] Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. 2018. A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80 – 86. URL: http://www.sciencedirect.com/science/article/pii/S1574013718301217, doi:https://doi.org/10.1016/j.cosrev.2018.10.002.

[26] Augot, D., Chabanne, H., Chenevier, T., George, W., & Lambert, L. *A User-Centric System for Verified Identities on the Bitcoin Blockchain*, 390–407. Springer International Publishing, Cham, 2017. URL: https://doi.org/10.1007/978-3-319-67816-0_22, doi:10.1007/978-3-319-67816-0_22.

[27] Brands, S. A. 2000. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, Cambridge, MA, USA.

[28] Marlinspike, M. 2012. Sovereign source authority. Available at http://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html, Visited 23 May 2019.

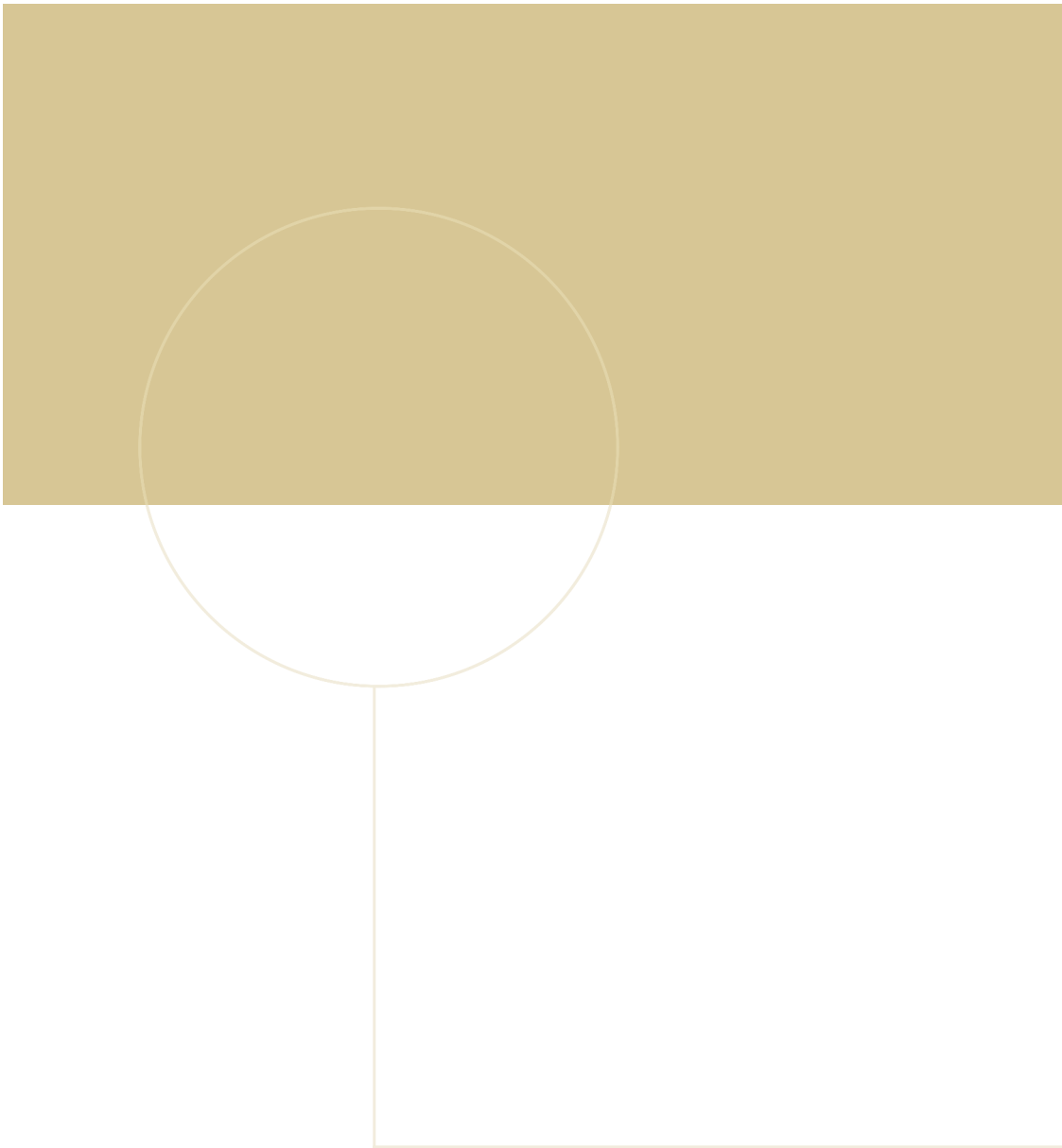
[29] uPort. 2018. uport specs. Available at https://github.com/uport-project/specs, Visited 15 April 2018.

[30] Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., & Sena, M. 2016. Uport: A platform for self-sovereign identity. *Available at http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf, Visited 24 March 2019*.

[31] Reed, D., Law, J., & Hardman, D. 2016. The technical foundations of sovrin. Available at https://sovrin.org/wp-content/uploads/2018/03/The-Technical-Foundations-of-Sovrin.pdf, Visited 28 May 2019.

[32] Civic Technologies. 2017. Civic whitepaper. Available at https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf, Visited 16 April 2018.

[33] ShoCard, inc. 2017. Identity management verified using the blockchain. Available at https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf, Visited 23 May 2019.



NTNU

Kunnskap for en bedre verden