SELF-SOVEREIGN IDENTITY

Prepared by:

21627711 - Halil Etka Tutkun

07.01.2021

TABLE OF CONTENTS

INTRODUCTION

Identity is a collection of claims about a person, place or thing and it is integral to a functioning society and economy. Having a proper way to identify ourselves and our possessions enables us to create thriving societies and global markets. [1]

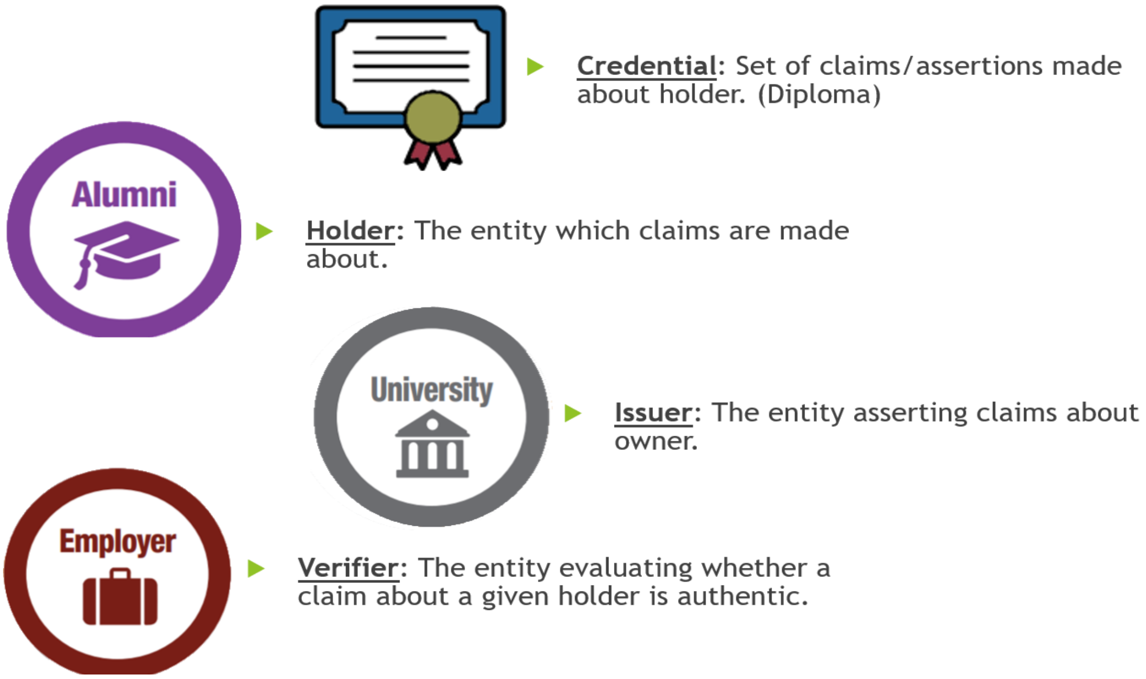
Traditional document-based identity systems cannot keep up with today's world due to large number of physical identity documents that needed to be stored and transported, inability to access needed information quickly, unreliable and insecure storing conditions etc.

To be able to catch up with today's digital world, identity systems also digitalized during the last two decades. The digital identity associated with real world identity helps people to prove that they are who they claim to be using their digital devices, and provides a fast, secure transmission of verified identities to legal entities. Even though they have solved most of our problems, they have their own problems as well.

In this research we are going to analyze those problems and the emerging technology called self-sovereign identity which is trying to find a solution to this problem. We are going to analyze strengths and weaknesses of this technology, and simply go over its workflow. Finally, we are going to propose a solution to the most important weakness according to us.

EXAMPLE CASE AND VOCOBULARY

Imagine a case where the employers want to verify that the applicants have a valid diploma issued by a university using digital identity.

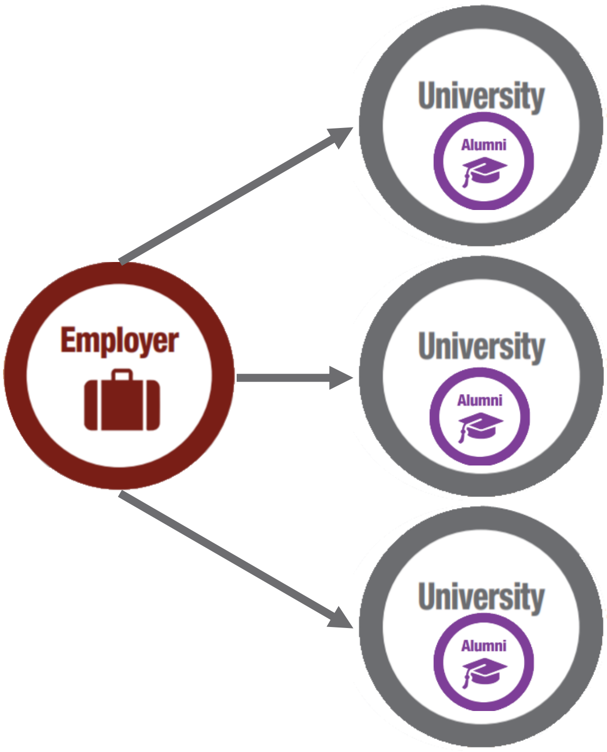


- **Credential**: Set of claims/assertions made about holder. (Diploma)
- **Holder**: The entity which claims are made about.
- **Issuer**: The entity asserting claims about owner.
- **Verifier**: The entity evaluating whether a claim about a given holder is authentic.

Throughout our report we will use this example case to explain the workflow of the technologies we are examining.

Now we will talk about different digital identity models we can use to achieve this kind of system.

CENTRALIZED IDENTITY

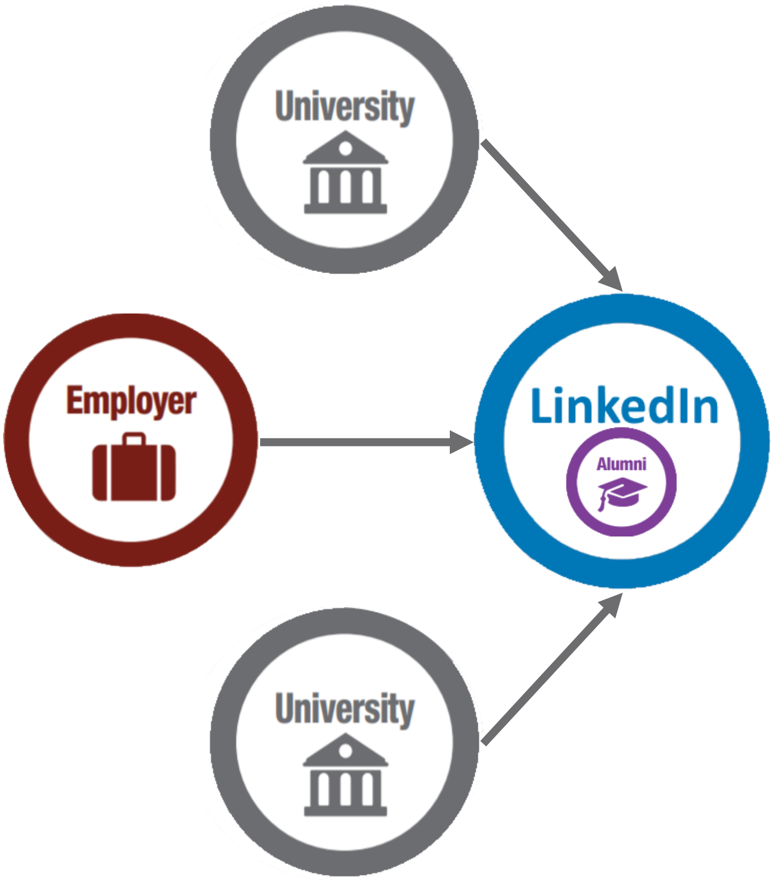


Centralized identity refers to model where issuers manages the identity credentials in their own system. In those systems verifier needs to ask directly to the issuer for the verification of the credentials.

In our example case it means that the universities would keep the record of diplomas in their own system and the employers would need to ask those universities to verify the diploma of a given alumni.

This type of identity model provides private communication between the verifiers and the issuers. However, it is harder to implement for multiple entities because it does not provide a standard protocol. Which means verifiers need to have a separate protocol for each issuer they want to interact with. The second problem is that the holders do not have much control over their own credentials. (In our case universities can do anything with the alumni's diploma without his/her permission.)

THIRD-PARTY IDENTITY



Third-party identity refers to model where third-party systems manage the credentials given by issuers and the interaction of verifiers with those credentials.

In our example it means that universities would issue the diplomas to the account of the alumni in a third-party system (e.g. LinkedIn) and employers would ask this third-party system to verify the diploma of a given alumni.

This type of identity model is easier to implement for multiple entities because it provides a standard protocol where issuers and verifiers can talk through. However, it brings privacy problems to the table because the communication between verifiers and issuers are not direct. Third-party systems control the credentials of the holders and all the interactions they have with holders and verifiers.

SELF SOVEREIGN IDENTITY (SSI)

With SSI we are trying to build a system that is private, easy to use by multiple entities and controllable by the holders all at the same time. To accomplish this SSI uses the blockchain as a source of truth.

Blockchain Technology refers to the technology behind decentralized databases that provides control over the evolution of data between entities through a peer-to-peer network, using consensus algorithms that makes it hard or impossible to make changes or defraud the system. [2]

We will start by defining some of the important SSI standard terms.

Decentralized Identifier (DID): Identifiers with a blockchain address and public private key pair tied to it.

DID Document: Documents that are stored in the blockchain which has a DID, corresponding public key and a URL to interact with the identity owner.

Identity Wallet: Applications where DIDs, the keys and verifiable credentials are stored.

Verifiable Credentials: Interoperable, cryptographically-verifiable digital credentials.

Decentralized Key Management System (DKMS): Systems that store and manage private keys inside a wallet across devices. Enables key synchronization and recovery.

Trust Hubs: Trust hubs are registries keeping the list of trustworthy entities They are usually managed by the wallet application creators.

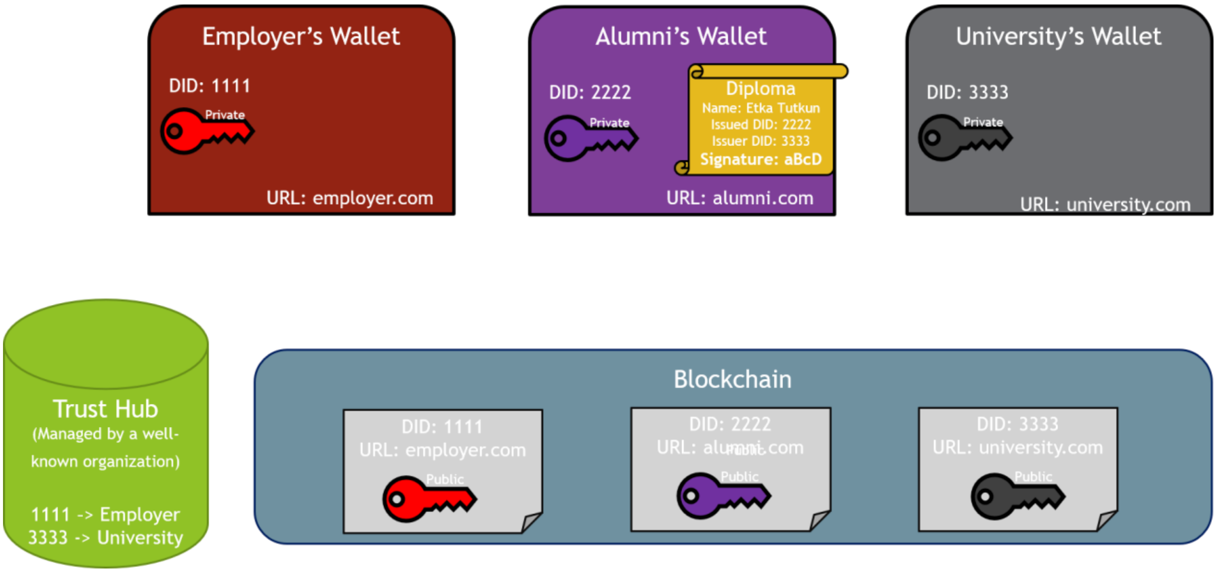
These standard terms emerged over time in the community and played an important role to make SSI possible in real life. Here is the simple workflow of this model for our example case:

1- All the entities in the system creates a DID and public-private key pairs tied to it cryptographically. They create a DID document that includes: DID, wallet URL and public key. And they store it on the blockchain in the chosen DID address.
2- The university and the employer apply to a well-known organization to get registered to the trust hub server. And this organization registers their DIDs with their organization name as a trusted DID.
3- The alumni applies to the university with his/her DID to get a digital diploma.
4- University's wallet goes to the DID blockchain address, gets the public key of the alumni and connects to alumni's wallet through the URL written in the DID document. To establish a secure connection university's wallet signs a challenge with the alumni's public key and sends it to the alumni's wallet. Alumni's wallet decrypts the challenge with his/her private key and send it to the university with a similar challenge. After university's wallet decrypts and sends the challenge coming from alumni's wallet back to it, both wallets trust each other and establishes a secure connection. (this process is called DID Auth)
5- University's wallet creates a diploma with the alumni's and its own DID in it. Later it sends this diploma to the alumni by signing it with university's private key. Alumni stores the digital diploma in its wallet.
6- The alumni applies to the employer by giving his/her DID.
7- To establish a secure connection with DID Auth step 4 repeats between the employer's wallet and alumni's wallet.
8- Alumni's wallet checks if the give DID really belong to the employer by asking to the trust hub server.
9- Alumni's wallet sends the digital diploma to employer's wallet.

10- Employer’s wallet checks the issuer DID of the diploma (the university’s DID), goes to its address in blockchain and gets the public key to check if the signature on the digital diploma authentic.

11- Employer’s wallet checks if the give DID really belong to the university by asking to the trust hub server.

12- The process is complete as the employer makes sure the alumni has an authentic diploma given by the university.



STATE OF THE ART – HYPERLEDGER INDY

Hyperledger-Indy is an opensource blockchain project created specifically for SSI. This project is the leading implementer of the standards and mostly where these standards are emerged. Hyperledger-Indy is in production for more than two years and managed by The Linux Foundation. Here are some properties of this project:

- Has two types of nodes: Validator (handles writes) and Observer (handles reads).
- Only permissioned entities can join to blockchain network as a node.
- Everyone can read from the blockchain to verify the identity of an entity.
- Uses Redundant Byzantine Fault Tolerance consensus protocol.
- Optimized for efficient read and validation with state proof and BLS aggregated signatures.
- Consists of two sub-projects Indy-Plenum (general purpose blockchain) and Indy-Node (identity specific implementations).

Hyperledger Indy is adopted by multiple identity networks but the biggest adopter is the Sovrin Network. Sovrin Network is used for many digital identity projects from enterprise applications to health and humanitarian sector applications. They are the biggest example for self-sovereign identity in real life.

THE PROBLEM

As we mentioned trust hubs are registries keeping the list of trustworthy entities. They provide us a way to identify the real owner of a DID. However, as you can see in the standard workflow this introduces the problem of **centralization of trust**. Entities need to trust to the maintainer of the trust hub server without any alternatives. Usually, maintainer of these servers are the creators of the wallet applications which entities uses to interact with the system. And the decision of trust is prebuilt into these applications without giving any options to the entities.

PROPOSED MODEL

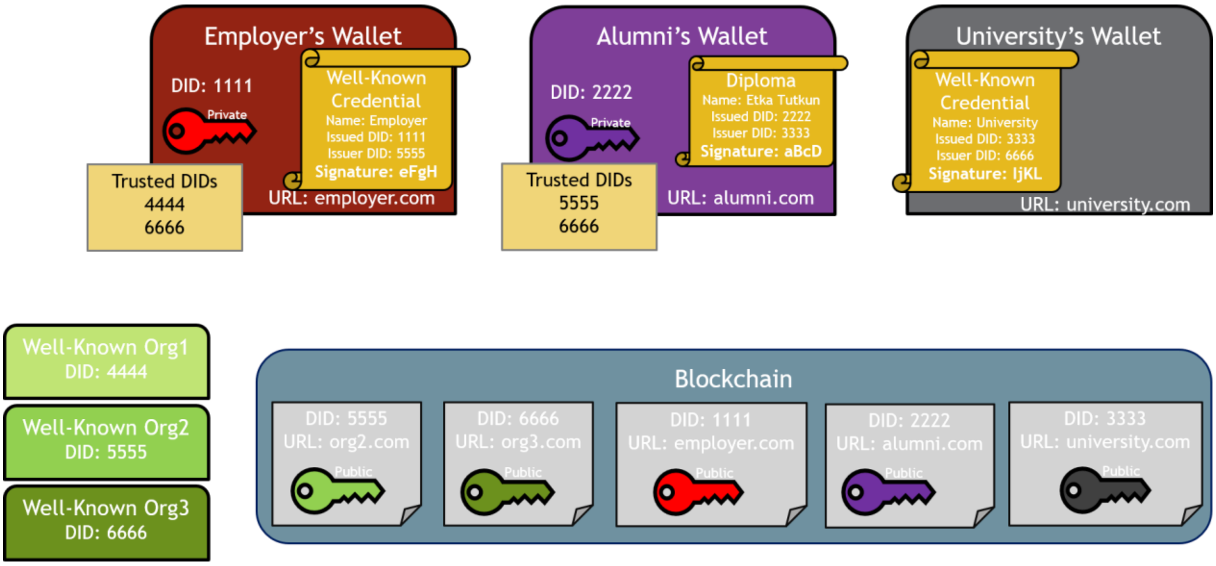
To solve this problem, we are suggesting a system where entities can create trust relationships by providing **well-known credentials** they got from different **well-known issuers**. This will allow entities to trust any well-known issuer they choose without forcing them to trust a single organization. Providing multiple alternatives to entities removes the centralization point from the system.

Here is the simple workflow of the proposed model:

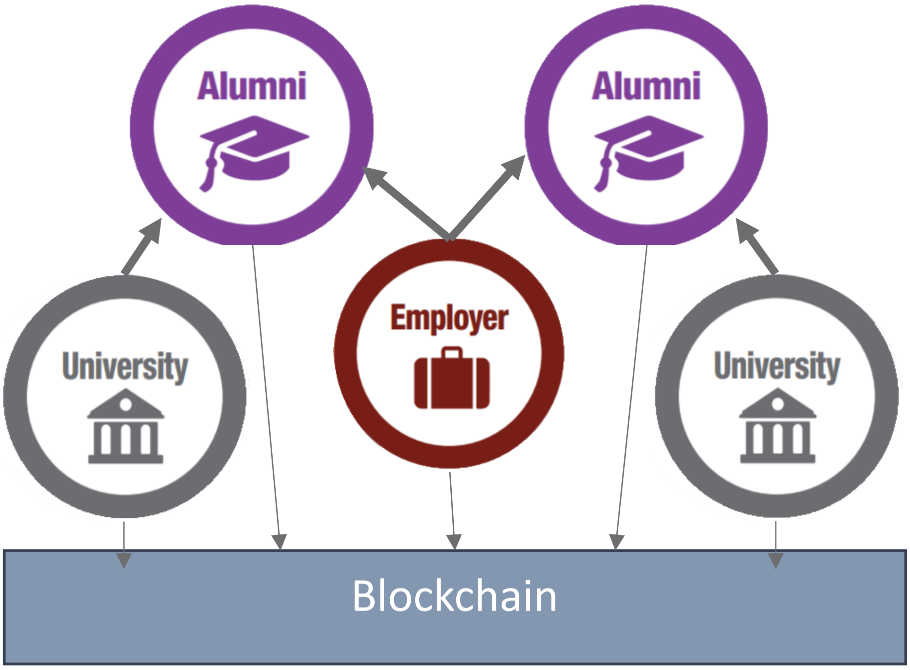
1- All the entities in the system (including well-known issuers) creates a DID and public-private key pairs tied to it cryptographically. They create a DID document that includes: DID, wallet URL and public key. And they store it on the blockchain in the chosen DID address.
2- The university and the employer apply to any well-known organization they choose to get a well-known credential. And these organizations issue them a credential with their DIDs in it.
3- The alumni applies to the university with his/her DID to get a digital diploma.
4- Secure connection established with DID Auth between the university's wallet and alumni's wallet.
5- University's wallet creates a diploma with the alumni's and its own DID in it. Later it sends this diploma to the alumni by signing it with university's private key. Alumni stores the digital diploma in its wallet.
6- The alumni applies to the employer by giving his/her DID.
7- Secure connection established with DID Auth between the employer's wallet and alumni's wallet.
8- Alumni's wallet sends to employer's wallet a list of DIDs the alumni chose to trust (among well-known issuers) in order to check if the give DID really belong to the employer.
9- Employer's wallet sends a well-known credential issued by one of the DIDs in the list alumni's wallet sent.
10- Alumni's wallet checks the signature on the credential by going to the blockchain and taking the public key of the well-known issuer.
11- Alumni's wallet sends the digital diploma to employer's wallet.
12- Employer's wallet checks the issuer DID of the diploma (the university's DID), goes to its address in blockchain and gets the public key to check if the signature on the digital diploma authentic.
13- Employer's wallet sends to university's wallet a list of DIDs the employer chose to trust (among well-known issuers) in order to check if the give DID really belong to the university.
14- University's wallet sends a well-known credential issued by one of the DIDs in the list employer's wallet sent.

15- Employer’s wallet checks the signature on the credential by going to the blockchain and taking the public key of the well-known issuer.

16- The process is complete as the employer makes sure the alumni has an authentic diploma given by the university.



By adopting this model, we got closer to creating a system where an entity can create private identity relationships with any other entity through a standard protocol without depending on a centralized authority using the blockchain technology.



OTHER PROBLEMS

Wallet Certification

We have a question in our minds and that is the question of how can we store this identity data safely. First answer appears to be “Digital Wallets”. But what is this Digital Wallet? Digital Wallet is basically a wallet that can store secure digital versions of official documents such as identity cards, passports and driver's license in citizens' smartphones. The main problem with these digital wallets is privacy and protection of personal data. These digital wallets have risks such as the place of data stored and security of that place, privacy of the data, will it be shared with third parties, is it secure for ID theft or does it prevent fraud IDs. In conclusion we ask this question: “Which digital wallet can be trusted?”.

Answer to this problem is that at the moment there are some Digital Identity Wallet brands but if we need to solve this problem we found that Open Source Digital Wallets will be the safest among them. But another best solution for this is a government based digital wallet. If the government gets involved with this technology, they can create digital identity wallets that are secure and trustable just like they secure our identities for the first time. With this way different governments citizens that are interacting with other governments can solve identity problems in a common way.

No Device / Smartphone

As we explained what a digital wallet is, we saw that for a digital wallet, we need a smartphone. With the datasets we saw that 1 billion people don't have an official proof of identity [3]. This is only the case of traditional identity, if we add the reachability of smartphones, this number increases. The problem of not having devices or smartphones occurs. So how can we use digital identity or digital identity wallet if we have this number of people who don’t have availability to use this system?

As we proposed a solution for the previous problem that if the wallet system works within governments hands if the government develops the technology that citizens can reach their wallet even if they don’t have a device or smartphone. Not having a smartphone and using a digital identity wallet does require more safety but creating a web site that citizens can reach their wallet without a phone might be the solution. We can use the “E-Devlet” system for the base layer for this technology.

Guardianship & Delegation

Usage of these Digital Wallets creates Guardianship and Delegation problems for children that are younger than the age of 18 and families of these children. When creating or having digital identities for children at these ages, generally parents will be responsible, but in this condition who will have the digital wallet for the child or does it require a new device/smartphone for every digital identity. If the child’s identity will be used, who will be delegated to use that identity? Does it require both child and delegated persons approval to use the digital wallet?

For this problem we see that even without digital identity parents hold their child’s identity card and when there is a situation that child’s id needs to be used parent’s use their child’s id and for security reasons they show their personal id as well.

Digital Identity Wallet technology can have such a feature that parents have their child’s digital identity so if needed they can use the digital identity of the child from their wallet.

Bare Minimum Portability

As we all experienced, if a wallet or smartphone is missing the recovery of information within those items will be hard and costly. And in real life situations if an information or data needs to swap to another place how easily that can be done is important because this portability needs to be minimum to secure the information. We have this same problem with digital identity and digital wallet, the problem called bare minimum portability.

To solve this problem, at the moment we have a lot of technologies to secure user accounts. Such as 2-step verifications, sending mail or SMS systems are seen as some security systems. Like we mentioned in the wallet certification problem's solution, if the government is involved in this technology, for portability purposes they can attend only one device for a citizen within their website so that if the citizen wants to change the device, they can contact the department, or website that is responsible for the wallet system.

Rendering

When the user retrieves data from the wallet to use their identity information for some process, the data should be readable in a suitable format for ID. Also it should be easy to understand for the user and the other party who will use the information. How will wallets handle this problem?

Considering the format that the person who requested the information, a template can be determined by the person who has requested their information from, using drag and drop or select and paste features, the readability of the format can be obtained.

SUMMARY

In this report we have tried to explain why self-sovereign identity is a good model for the future of the digital identity. Even though it is hard to build a reliable system without trusted authorities, it is important to remember that centralization of trust is almost as bad as no trust. To solve this problem, it is best to create hierarchical authorities without a centralized point and let the identity owners decide which authority to trust.

It is important to note while many commentators focus on outcomes such as scalability, security, auditability and cost-effectiveness, none of these are necessarily unique to blockchain based digital identity systems. What SSI accomplishes is bringing privacy, controllability and standardization together in a system. Our goal is to build a system where an entity can create private identity relationships with any other entity through a standard protocol without depending on a centralized authority.

Even though there are still areas which require more study to fully accomplish this, through our study we have shown why SSI can be a good model to solve this problem. The model we proposed is just another step to reach this goal.

REFERENCES

[1] https://consensys.net/blockchain-use-cases/digital-identity

[2] https://tykn.tech/identity-management-blockchain

[3] https://id4d.worldbank.org/global-dataset

https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf