Block Chain & Systems

ASSIGNMENT

Topic: Block Chain and SSI (Decentralize Identity Management)

M.Tech. Software Systems

WILP

BITS, Pilani

**Team Members:**

|  |  |
| --- | --- |
| **Name** | **Mail ID** |
| Ashutosh Batra | [2021MT12025@wilp.bits-pilani.ac.in](mailto:2021MT12025@wilp.bits-pilani.ac.in) |
| Saquib | [2021MT12266@wilp.bits-pilani.ac.in](mailto:2021MT12073@wilp.bits-pilani.ac.in) |
| Rohit Joshi | [2021MT12355@wilp.bits-pilani.ac.in](mailto:2021MT12353@wilp.bits-pilani.ac.in) |

**Index**

**Introduction**

Internet discovery revolutionized the idea of computer systems used by people across the globe. However, this also imposes a major threat to user privacy and sharing information consent. This is due to because machines are now self-intelligent and perform a lot of automated tasks without considering much user privacy. Most of the company take the help of big Identity providers like Google and Facebook to track and store online services for users. As they manage store user profiles that replicate the sentiment and behavior of the online user which provide real insight into the user history profile. This is dangerous, as this promotes for eg, data theft and illegal sharing, and data mining, which can be used by the government or malicious parties for their own benefit without users knowing it. This creates a controlling atmosphere for the user through their online identity. Hence new term evolved from this concept called **self-sovereign identity** is introduced. *The self-sovereignty means that people are the owner of their digital identities. It provides people get back their ownership rights. This is done by disclosing personal identity on a need-to-know basis and having verifiable credentials*. Privacy can be defined as the right of a person to keep their personal and relationship secret. People feel there is very less control they have over their digital identity anybody can use it without their consent in the current internet world.

Today’s digital environment operates mainly in a centralized mode. When an online service is used, either that service or a Federated Identity Management (FIM) platform like Facebook implements digital identity management. The service owns, monitors, and stores the digital identity. The user of such a service must therefore have a lot of trusts. But frequently there isn't a substitute. This raises a real issue about privacy abuse a genuine concern.

**Self-sovereign identities are digital identities that are managed and decentralized (SSI).** Without relying on other companies to centrally store and manage their data, people can take ownership of their digital identities by using this technology. An approach to digital identity known as "self-sovereign identity" (SSI) provides users authority over the data they use to authenticate themselves to websites, services, and applications across the internet.

In academic literature, several SSI implementations have been suggested, including many blockchain systems. However, there haven't been many proposals for critical analyses of the current SSI technology. To make sure user’s privacy is protected in blockchain-based applications is one of the main issues.

**Privacy Issue in Blockchain**

The block chain implementation can be classified as permissionless and permissioned. Bitcoin

Used permissionless block chain. Anyone can join the bitcoin network, all users are equal and able to participate in any role, no trust required It is based on zero trust where consensus and security taken care by Proof of Work mechanism. Anyone can validate the block after data transaction. Unless 51% of the user decided to alter the chain. Hence if 51% attack happen user can lose their money which leak their data. In permissioned block chain extra security provided on access control layer to the block chain. Based on the already created role the user can perform the operation or access the resource. There is some central authority which define the permission and rules for this type of block chain used mainly by the big industries. Here the data privacy is directly controlled by central authority.

**Block Chain & SSI**

It is not wrong to say that Blockchain and SSI technology are related. SSI provide the control of data for individual or organization, the actual owner of data it prevents sharing of data to third party, the user has complete ownership and control of the private data how they share and used. In block chain technology ledger are stored, It uses cryptographic has function and information is transmitted using digital signature where cryptographic key pairs used to encrypt the information.

Now the role of block chain to implement SSI can be seen as storing private information in the form of cryptographic block which block chain store. Suppose a person visiting airport to board the flight, he has to show vaccinated certificate at the time of boarding, In this case multiple parties involved like, there are airport official we call them as verifier, the health care facility is the issuer of vaccine certificate and person call the owner of the information. Now the question is how the airport official verify the authenticity of vaccine certificate. The possible solution of this problem to use block chain technology to store digital vaccine certificate. In this way we can use blockchain technology in implementing SSI.

**Detailed technical description**

In this section we will understand more details about SSI and its implementation, Decentralized identifiers (DIDs) can be used to enable self-sovereign identities.

**Defining Self-sovereignty Identity**

Chart, pie chart

Description automatically generated

**Fig1: Centralized Identity, Federated Identity, and Self-Sovereign Identity.**

The concept of Self Sovereign Identity implies that individual control the full ownership of their digital identities data includes, private data, health certificate, degree certificate passwords, usernames, bank accounts, and social media photos. In centralized identity management personal information held at central authority they can share personal data to whosoever they like. In federated identity system they allow to access number of application and services using single set of credentials. It mostly used in the organization to access multiple application using one employee account.

SSI models allow flexibility to have full ownership and control of digital identities without involvement of any central authority. The user decides who will get to access their data, they can add or remove the access permission to see data anytime. The good point about this technology is to map the digital world function with the physical world identity in which every person has unique and persistent identity.

SSI technology provides people to manage their digital information and controlled by self without any dependency on centralized service provider who store and mange their data. We can also say Self-Sovereign Identity also called decentralized identity.

There are three main components in the SSI system:

* **User:** Someone who creates their decentralized identifier with a digital wallet app and receives Verifiable Credentials.
* **Issuer**: Party with the authority to issue Verifiable Credentials.
* **Verifier:** Party checking the credential.

Diagram

Description automatically generated

**Fig2: The role of Information flow used in SSI solutions.**

The user is the manger of the information, he chooses whether to allow or access the data, there is interaction between holder, issuer and verifier sometimes referred to as “trust triangle”

Let’s discuss the information flow in SSI solution, there are multiple party involved to carry the process of identity information storing, the user obtains and store the verifiable claims and digital identity information that are issued by the Issuing authority. The claim then stored in block chain using hashes in the form of immutable ledger signed by digital signature of the user in the system, which later can be used for third party attestation. Now when the verifier needs to access these digital identity data of the user first, they require permission to do attestation then they validate signature based on block chain verifiable credentials, based on that they can verify and check the user claim. In this way knowledge is shared only need to know basis.

SSI technology allows privacy protection. This can be achieved only by sharing identity information need to know basis using verifiable credentials. In this case user is in control of the information and free to choose whether to share verifiable claim to verifier or not. The user may decide to reject the verifiable claim based on the situation.

Principle of self-sovereignty involve identity data ownership and management. Due to advance research, it is possible to store, share authenticate identity data and third-party credentials in very secure and privacy preserving manner. SSI allows the trust individual ownership and control their data without the administrative or central authority or federated identity provider (IDP). As shown in the Fig1 individual interacting 3rd party directly without the intervention of central authority using public-key cryptography, decentralized identifiers, and blockchain technology.

* Self-Sovereign Identity is made up of 3 pillars: blockchain, decentralized identifiers, and Verifiable Credentials.
* Self-Sovereign Identity technology can be applied to diverse use cases including issuing fraud-proof certifications, supply chain product tracking, and speeding up workforce recruitment times.

Self-Sovereign Identity is made up of 3 pillars:

1. **Blockchain:** A decentralized distributed ledger that is shared among computers in the blockchain network that records information in a way that makes it very difficult to change, hack, or cheat the system. In this technology participant has equal permission to view the data and trust is not rooted to single authority.
2. **Decentralized Identifiers (DIDs):** Cryptographically Digital identity created by the user using cryptography techniques, they do not depend on any organization and contain no personally identifiable information.
3. **Verifiable Credentials (VCs):** Secure Digital Certificate or credential of the document that user can share to the verifiers.

Will learn more about these SSI pillars in the subsequent report.

## 

## 

## 

## **SSI Pillar 1: Blockchain**

Block chain is a secure series or chain of timestamped records stored in database that a group of user manages who are part of decentralized network. Block chain is decentralized or distributed ledger where each node in a network has access to the data or records stored in blockchain. The encryption of all the important data records in block chain is done using cryptographic techniques.

Block chain is a network of interconnected nodes, its database shared among computers in block chain network. The mechanism of block chain design in such a way that is very difficult to change, sabotage, cheat the system. Data is stored in the form of chain of previous each block has the information of previous block once new block verified it has been added to the block chain.

**Key feature of a self-sovereign Identity block chain**

* **Decentralized:** Block chain use peer-to-peer network, a distributed ledger that provides a way for data to be recorded and shared by multiple nodes or users. No single authority responsible to approve the transaction, computer nodes are located anywhere in the world and take participate in block validation, without any special permission.
* **Distributed Ledger:** Block chain use distributed ledger to store blocks it is kind of block chain data base that is distributed across several nodes. Block chain network physically located in different places it has single ledger that is shared by all nodes. It is immutable and used to verify the data has not been tampered with. Once the data verified it has been added to the block chain.
* **Security with Immutability:** Every block chain block contains the information about previous block in the form of cryptographic hash function, so to alter the information in one block means to change the content of very previous block and then again change the content of previous to previous block so it means we need to change the content of whole big chain that is almost impossible unless someone own 51 % of the power to perform this attack.so if somehow one can change the hash which act like digital fingerprint of one block everyone in the network able to identity the information has been tempered with they will reject this block and won’t become the part of block chain.

## **SSI Pillar 2: Decentralized Identifiers (DIDs)**

## **SSI Pillar 3: Verifiable Credentials (VCs)**

### 

### 

### 

### 

### 

### **Principles of Self-Sovereign Identity**

## **Problems With Centralized Digital Identifiers, Credentials, and IDs**

## **Benefits of Self-Sovereign Identity Management for Organizations, Individuals, and Developers**

## **Self-Sovereign Identity Standards**

## **Self-Sovereign Identity Use Cases**

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# **How Blockchain Technology and Self-Sovereign Identity Enables the New Normal of Remote Learning, Training, and Working**