Blockchain in SSI (Decentralized Identity Management)

Ashutosh Batra   
*BITS Pillani*   
Ahmedabad, India  
2021MT12025@wilp.bits-pilani.ac.in

Saquib   
*BITS Pillani*   
New Delhi, India  
2021MT12266@wilp.bits-pilani.ac.in

Rohit Joshi  
*BITS Pillani*   
Pune, India  
2021MT12355@wilp.bits-pilani.ac.in

*Abstract*— This paper is about using blockchain technology in the SSI decentralized identity management. Blockchain-based self-sovereign identity (SSI) solutions are being implemented as alternatives to current digital identification systems, or possibly as a foundation for standards for the upcoming global identity management system infrastructures.

Keywords—Blockchain, SSI, Decentralized

# Introduction

<Introduction about Blockchain, SSI, Decentralized identity management>.

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 machines being self-intelligent and performing a lot of automated tasks without considering much user privacy. Most of the companies 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 a new term evolved from this concept called self-sovereign identity is introduced. The self-sovereignty means that people are the owners 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 little 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 trust. 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 permission less and permissioned. Bitcoin Used permission less block chain. Anyone can join the bit coin 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 are taken care of by Proof of Work mechanism. Anyone can validate the block after data transaction. Unless 51% of the users decided to alter the chain. Hence if 51% attacks happen users can lose their money which leak their data. In the permissioned block chain extra security is provided on the 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 defines 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.

# Blochian & ssi

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

# 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 individuals 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 systems they allow access to a number of applications and services using a single set of credentials. It is mostly used in the organization to access multiple applications 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 a unique and persistent identity.

SSI technology allows people to manage their digital information and control it by themselves without any dependency on centralized service providers who store and manage their data. We can also say Self-Sovereign Identity also called decentralized identity.

There are three main components in the SSI system:

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

Diagram

Description automatically generated

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

The user is the manager 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 the SSI solution, there are multiple parties involved to carry the process of identity information storing, the user obtains and stores the verifiable claims and digital identity information that are issued by the Issuing authority. The claim is 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 on the basis.

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

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

* We can divide Self-Sovereign Identity into 3 parts : 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 participants have 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 the user can share to the verifiers.

# SSI Pillar 1: Blockchain

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

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

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

#### **Decentralized:** Block chain uses a 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 is responsible to approve the transaction, computer nodes are located anywhere in the world and take part in block validation, without any special permission.

#### **Distributed Ledger:** Block chain use distributed ledger to store blocks it is a kind of block chain database that is distributed across several nodes. Block chain networks physically located in different places have a 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 is 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 tampered with they will reject this block and won’t become the part of block chain.

Now we will understand with the help of one example how the block chain helps in implementing SSI.

Let's suppose in an organization there is only one person called accountant who has access to all financial records and data. If they want to commit fraud and steal the money, there is no way to trace the record because he is the only owner of all the money and data. If they wanted to change the entry of a record there are no limited ways to trace the actual records.

To avoid this fraud and loss, implement permissioned blockchain where people can audit and check the validity of transaction records regularly. We are now going to see how blockchain chains are used in self-sovereign identity systems.

**Holder** is the owner of the digital identity information e.g.: Driving license, Land Registry records so these tokenize information is stored on the blockchain in the form of a decentralized Identifier (DID).**Issuer** is the government, department authority, which provide certificate, verifiable claim to the holder like social security number they sign it with their decentralize identity (DID) and associated private key. The government's DID and associated public key available on the block chain. **Verifier** is the party asking for credentials like driving company asking for license, Bank authority asking for social security number now they can verify it from the block chain, because they trust these central authority government issued them trusted certificate, driving license or social security number signed by issuer's DID that is present on block chain.

Let's discuss the basic difference between decentralized and centralized management systems in the context of block chain technology.

| Centralized Identity Management | Decentralized Identity Management |
| --- | --- |
| User data can be shared with other organization without their knowledge | This will allow sharing data when users give consent. |
| There is high risk and data breaches due to storing of data in centralized systems. | Data is stored in the decentralized location by user wallet , which minimize the risk of data theft and breaches |
| Data owned by user and controlled by organization application and services | Data is owned and managed by the user only. |

# SSI pillar 2: decentralize identifiers (did)

A digital identity, such as an email address or user name, is a must for everyone with an online presence. To connect to websites and apps today, most of us rely on centralized identifiers like Google, Facebook, email providers, or mobile network carriers. However, these digital IDs are frequently used to collect, monitor, and share user data. Companies may be aware of who we messaged, what we purchased, where we live, where we are, and other details.

Thanks to decentralized identifiers (DIDs), people can now securely connect their digital identities to Verifiable Credentials that don't automatically divulge personal information. We are able to fully own and govern our data because of DIDs. It is more difficult for someone to connect different DIDs when they have more than one.

A DID is an unrelated to any organization string of letters and digits that serves as a worldwide unique identifier. DIDs are publicly known by relevant parties.



A DID:

* Produced by the user.
* Includes one or more pairs of private and public keys.
* Allows for private and secure connections between two parties and may be confirmed anytime, anyplace, and does not contain personal data or wallet information.

People are free to create as many DIDs as they would like for various interactions and purposes. As an illustration, the following three DIDs can be produced:

DID 1: Only for their internet purchases

DID 2: For services relating to cryptocurrencies, such as trading and purchasing NFTs

## DID 3: Holding credentials from their schooling, such as a university degree and course certificates, for professional objectives

### **Private and Public Keys That Come With DIDs**

It's crucial to comprehend what encryption is in order to learn how private and public keys function. Encryption is the technique of taking a communication and shredding it so that only specific persons can read it..

There are 2 types of encryption:

***1. Symmetric encryption:*** It only takes one key (password) to encrypt and decrypt data. Think about selecting a password like "cats rule" to protect access to a document. Anyone can access the document by typing "cats rule" into the search bar. In this illustration, the document is encrypted and decrypted using the same password (key).

*2. Asymmetric encryption:*The matching decryption key (also known as the private key) differs from the encryption key, also known as the public key.

When security is crucial, asymmetric encryption is utilized, such as on websites with the https:// prefix, encrypted emails, or cryptocurrency to ensure that only the wallet owner may withdraw or transfer money from it.

Each DID have a single or more private and public keys.

Private key: A lengthy string of letters and numbers that can be used to sign Verifiable Credentials and establish ownership as well as provide permission to share specific data. An owner of a private key should never disclose it with anyone because, in an analogy, it functions as a master key that can access all of your information.

Public key: A lengthy string of characters and digits that you can safely share with anyone to whom you choose to provide specific information.

# SSI Pillar 3: Verifiable credentials (vcs)

ID cards, diplomas, and degrees can all be easily falsified, and corporations have little to no tools for validating their veracity other than the time-consuming, manual procedure of contacting the credential's issuer, such as a university or licensing agency. But with verifiable credentials, verifiers like an employer, a government agency, or an app can quickly confirm credentials!

Verifiable Credentials are digital versions of paper and digital credentials that are cryptographically secured and can be presented to those who require them for verification. An employer, for instance, doesn't need to spend days or weeks contacting universities to find out if a candidate's degree is genuine because they can just use an app to scan a job candidate's QR code to check that they have a bachelor's degree.

The World Wide Web Consortium (W3C) is a global community of member organizations, staff, and the general public working together to establish global standards for the World Wide Web. Digital credentials can be referred to as Verifiable Credentials if they adhere to the Verifiable Credentials Data Model 1.0 requirements that they developed.

A "specification [that] provides a standard way to express credentials on the Web in a way that is cryptographically secure, privacy-respecting, and machine-verifiable" is the Verifiable Credentials Data Model 1.0. Decentralized Identifiers, URLs, and other technologies were standardized by the W3C.

The main advantages of issuing verifiable credentials are time and money savings, fraud prevention, and a reduction in manual effort when issuing verifiable credentials effectively.

#### Verifying Organizations: Verifying credentials instantaneously without contacting issuing organizations can help you save time, money, and resources.

#### Individuals: Only confirm assertions without divulging the actual data, and only give a verifier the pertinent information without giving other information.

#### Developers: Improve user experience by securely authenticating without requiring passwords.

Self-Sovereign Identity blockchain companies can help people maintain their privacy in two ways:

#### **Selective Disclosure:**

#### You can choose which credentials' data to present a verifier without disclosing more information than is necessary. For instance, you can present your birthdate from a license that was issued as a Verifiable Credential without revealing your name or address if you must be at least 18 to receive a service.

#### **Zero-Knowledge Proofs (ZKPs)**

#### Self-Sovereign Identity providers go even farther to assist users keep privacy by demonstrating you are 18 years of age or older without even disclosing your date of birth using zero-knowledge proof technology. By using cryptography, the holder can demonstrate to the verifier that they meet a set of criteria without having to provide the supporting documentation (such as evidence of age, income, or place of residence).

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

Many authors, including Kim Cameron's "Laws of Identity" and the W3C Verifiable Claims Task Force FAQ, have written about identity concepts. Although diverse thought leaders and organizations may not all agree on what Self-Sovereign Identity is, there are ten basic concepts that encapsulate its most important features.

1) Existence: A user needs to be able to exist independently in the digital environment.

2) Ownership: Individuals must possess complete control over their digital identities and personal information.

3) Accessibility: Individuals must have quick and easy access to their data.

4) Transparency: An identity system's management and algorithmic updates must be accessible to the general public and sufficiently intelligible. The design of the solution ought to be based on open software and protocol standards.

5) Persistence: Identity must endure over time. Solution creators should create viable business and operational models and install enough supporting infrastructure.

6) Portability: Individuals must be free to move their data between platforms, carry their identities and credentials with them wherever they go, and not be tied to a single platform.

7) Interoperability: Different stakeholders should be able to use identities as extensively as possible. Through a digital identification system, organizations, databases, and registries must be able to swiftly and effectively connect with one another on a worldwide scale.

8) Users must expressly consent before an entity can use or access their data. The procedure for giving consent should be interactive and clear to all parties.

9) Minimization: To reduce the sharing of excessive and unneeded personally identifiable information, a digital identification solution should allow users to share the minimum amount of data required by a third party.

10) Protection: The right to privacy must be upheld, and measures should be in place to prevent data manipulation and surveillance. End-to-end encryption should be used for data traffic.

# IX. Issues and challenges problems with centralized digital identifiers, credentials and id’s.

## University degrees and other centralized digital credentials, such as certifications for health and safety training, are simple to fake.

* Contacting the issuing body is the only way to verify their legitimacy, and it may take days or even months to receive the necessary information.
* Traditional IDs, such as a driver's license or other government-issued IDs, are not private since the verifier can access all the information on the document, including the bearer's date of birth and address, which they frequently don't require.
* If the issuer's service is unavailable or ceases to exist, people will not be able to demonstrate the validity of their credentials to a verifier.
* Third parties have the ability to store, monitor, and share data.
* Hacking breaches that utilize brute force or the use of stolen or lost credentials account for more than 80% of all incidents.
* Data stored on a central issuer server is more likely to be the target of hacks, breaches, or leaks.

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

Organizations use centralized and federated identity management (logging in with a Google or Facebook account, for example) systems by default when we visit apps and websites. Organizations are often subject to significant hacks and data breaches due to centralized systems. With federated systems, credential system providers like Google may leverage people's private data without their consent to keep and track their web activity. For organizations, SSI innovation empowers them to form fraud-proof Irrefutable Accreditations and right away confirm the authenticity of a credential.

Certificate counterfeiting and a lack of product identification are major issues everywhere in the globe since ID & credential verification procedures are cumbersome, expensive, and delayed. Self-Sovereign Identity (SSI), a solution to several of these issues, was created. A model called "Self-Sovereign Identity" allows people complete control and sovereignty over their digital identities without depending on a centralized organization. Enterprises can produce Verifiable Credentials that are impervious to fraud and quickly confirm a credential's legitimacy thanks to SSI technology.

Self-Sovereign Identity technology can be used in a variety of use cases, such as offering fraud-proof certificates, tracking products in the supply chain, and shortening the hiring process.

**Organizations**

* By rapidly confirming credentials like nurse licenses or online course completion certificates instead of taking days, weeks, or months, you can significantly cut expenses, inefficiencies, and resource usage.
* Produce Verifiable Credentials that are fraud-proof quickly and inexpensively.
* Public-key cryptography can increase security.
* By retaining less user data, you can decrease your exposure to cyberattacks, data breaches, legal action, and penalties.

### **Individuals**

* Complete Ownership and control of your identity, independent of any third parties
* With a digital wallet, you may make your own DIDs and handle all of your data.
* You have control over the information you share and with whom, and you have the option to revoke access to information at any time.
* No centralized servers are used to store personal information.
* You don't have to submit extraneous information, such as your full address, if all that is needed to validate your age is your age.

### **Developers**

* Create applications that do not require a password, improving the user experience.
* eliminates ineffective authentication procedures such as supplementary email or SMS verification
* Ask users for information directly rather than through a third party

# Self-Sovereign Identity Standards

The SSI standards that assist individuals in developing and maintaining their digital identities are constantly being improved. Data models, Schema, open-source code, APIs, and other things are all standards. The main standards that have been created are as follows:

### **W3C Verifiable Claims Data Model and Representations**

The development, storage, presentation, validation, and user control of credentials are all topics covered by the W3C Credentials Community Group. The Verifiable Claims Data Model & Representations 1.0 was released by the organization in May 2017. The specification goes over what constitutes verifiable claim criteria. According to this definition, a SSI architecture for verifiable claims is one in which the person who owns a verifiable claim has total control over their identification and how it is utilized.

### **W3C DID: Decentralized Identifiers (DIDs)**

As we have seen, the purpose of **Decentralized Identifiers (DIDs)** is to create a verified, decentralized digital identity. A DID identifies any topic that the DID's controller determines it identifies (for example, a person, organization, Entity, abstract etc.). These new IDs are intended to be used independently of any centralized registry, identity provider and to allow the controller of a DID to demonstrate control over it. DIDs are URLs that link a subject to a document, enabling secure interactions with that topic. Each DID document has the ability to include cryptographic information, verification techniques, or service endpoints, which offer a variety of ways for a DID controller to demonstrate control over a DID.

### **Decentralized Identity Foundation (DIF)**

To create an open ecosystem of decentralized identity that is open to all, the Decentralized Identity Foundations, an engineering-driven organization, is cooperating with a wide range of organizations and people from across the world.

DIF Allows below set of rules for the communicate data between assets/devices:

* **Identifiers and discovery:** How to identify and find individuals, groups, and equipment without the need of centralized identification systems is a crucial component of the decentralized identity equation.   Members of the DIF are continuing to develop protocols and implementations that facilitate the discovery, creation and resolution of decentralized names and IDs across decentralized systems, such as distributed ledgers and blockchains.
* **Authentication:** DID-based authentication specifications, standards, and libraries that are used to authenticate DIDs across several exchanges and use cases
* **DID Communication:** Create one or more excellent specifications that represent a technique called "DIDComm" for secure, private, and (if applicable) authenticated message-based communication, where trust is based on DIDs as well as rely on the messages' internal content rather than the external characteristics of the transport(s) being used.
* **Secure data storage:** A foundational layer for secure data storage (including PII data) should be established by creating one or more specifications that cover data models for storage and transport, syntax, DIR protection, CRUD API, access control, synchronization, and at least a minimally workable HTTP-based interface that is compatible with W3C DIDs/VCs.
* [**Claims and Credentials:**](https://identity.foundation/working-groups/claims-credentials.html)Establishing confidence among entities on a decentralized system without a centralized hierarchy requires the capacity to validate identity claims and assertions. To make it simple for ecosystem participants and their users to incorporate DID-signed claims into their apps and services, the DIF Foundation has just started work on defining the standards, protocols, and tools it may offer to the ecosystem.
* **Storage & Compute:** Decentralized identity systems require the storage and computation of data to be encrypted, secure, and privacy-preserving. A user's identity data must stay private and only be accessible to such entities they permit, much like identifiers and names must be self-sovereign to the owning entity. For provider-neutral, anywhere-running systems that offer these features, DIF members are working hard to create specifications and reference implementation.

# **Trust-over-IP: full-stack governance**

Amid 2020, the Trust-over-IP foundation was established. It is designing a comprehensive architecture for Internet-scale digital trust that blends human trust at the corporate, legal, and social layers with cryptographic trust at the machine layer. It has the following working groups in addition to several others that are still in the beginning stages.

* **Governance Stack**: The Governance Stack Working Group's mandate is to develop models and interoperability guidelines for governance frameworks that enable social, legal, and commercial trust amongst organizations utilizing the Trust over IP architecture stack as specified in Hyperledger Aries RFC 0289.Technical Stack : The Technical Stack Working Group's mandate is to specify the technical requirements, test suites, and interoperability accreditation standards for the Trust over IP architecture stack as specified in Hyperledger Aries RFC 0289 (either explicitly or by reference) (or its successor as identified in the RFC document itself).
* **Utility Foundry**: To foster a community of practice among governance bodies, implementers, operators, and service providers for Integrity over IP Layer One utilities is the goal of the Utility Foundry Working Group. Whether new To IP Layer One utility projects are hosted by the Linux Foundation or somewhere else, the WG will offer methodological direction for their creation and oversight. Other WG activities include developing sample requests for proposals (RFPs) for service providers, keeping track of affiliated Foundry Service Providers, finding synergies and areas of agreement between related and/or dissimilar utilities, and, if applicable, acting as a center of expertise for the promotion and education of ToIP Layer One utilities.
* **Ecosystem Foundry**: The Ecosystem Foundry Working Group's mandate is to support a community of practice among governing bodies, implementers, operators, and providers of Trust over IP Layer Four ecosystems. Whether new ToIP Layer Four ecosystem projects are hosted by the Linux Foundation or somewhere else, the WG will offer process direction for their creation and oversight. Other WG activities will include developing sample requests for proposals (RFPs) for service providers, keeping track of associated Foundry Service Providers, identifying areas for collaboration and alignment between related and/or disparate ecosystems, and, if applicable, acting as a center of expertise for the advertisement and education of the role of ToIP Layer Four ecosystems.

XIII. Self-Sovereign Identity Use Cases & Industry Implementation

**Use Case**

**a) Bosch Implementation of Master Data Management**

Bosch has already implemented Master data management with SSI ensures data quality and data sovereignty.

Bosch Team is trying to create corporate agent software, which is similar to a digital certificate wallet and represents each legal company to the public. An individual, self-managed DID is assigned to each legal organization. The company's legal records are concealed behind this. A corporate identity card serves as a digital business card and is comparable to a digital ID card for businesses, according to Werner. It can be provided to business partners, if necessary, together with other electronic IDs like bank cards or tax IDs.

The process is digital: Data is sent from the company's agent software to the partner companies' agents’ software. Data exchanges can be done across secure connection channels thanks to the SSI technology because they are encrypted and cryptographically safeguarded during transmission. Collaboration between participants is facilitated by a blockchain. It's no longer necessary to save the data with outside services. Data on business partners is not also kept in the firm agent software. However, because it remembers the DID that was exchanged, data may be updated, sent, and searched instantly. The master data is therefore constantly current. Manual maintenance and inspection are not required on a regular basis.

**b) SSI Implementation in Travel Industry**

One of the most applicable SSI applications made necessary by pandemic advances is arguably found in the travel industry. Traveling both domestically and internationally has always necessitated the exchange of identifying documents such as passports and visas. This has become much more complicated in the era of COVID-19 as a new level of health certification has been added. One of the major drawbacks of the "track and trace" method, for instance, is that a great deal of private information is shared with a huge number of third parties. The Covid Credentials Initiative is one of the initiatives in this area; it intends to create "privacy-preserving verifiable credentials" to distribute the infection through SSI.

Airlines are currently evaluating international credentials to confirm health passports utilizing SSI and digital identification, and the International Air Transport Association (IATA) is creating the IATA Travel Pass. It saves encrypted data, including validated test and/or immunization results, on the traveller’s mobile device, making it completely decentralized because there isn't a single location where all of this data is kept.

**c) SSI Implementation in Finance & Crypto**

The Centralised Decentralised Finance (CeDeFi) finds a strong use for SSI that goes beyond traditional banking. Since both centralized and decentralized finance require identity verification, yet neither is satisfied with the current KYC and identity systems, SSI can offer the identity layer that satisfies both worlds. It builds a link between conventional data-intensive interactions and an anonymous DeFi strategy, and CeDeFI will offer the necessary financial support for SSI adoption in a crucial market.

Peer-to-peer (P2P) transactions inside the Crypto and DeFi domains are made possible by SSI. To establish their identity without making it public, one can share a little bit of data, such as their Telegram handle. Therefore, there won't be any further test payments to check wallets. Another choice is to do KYC'ed loan pools without saving the data, merely preserving "yes" or "no" responses.

**d) SSI & Non-Fungible Tokens (NFT)**

Self-sovereign identification enables ownership of fractions as well as the ability to demonstrate who invented, owned, and/or currently possesses Non-fungible Tokens (NFT) during their existence. Whatever ledger NFTs are hosted on, SSI can address the provenance problem. To put it another way, SSI can enable direct consumption of media and material from creators without the need for a distribution intermediary. This type of consumption includes identity verification and payment. Through direct communication with their audiences and proper compensation for their labor, creators can benefit from this. Check out our opinions on how combining NFT and SSI can provide a novel gaming experience here.

Identification tied to payments is a problem that self-sovereign identity can resolve. Well beyond wallet address, there is presently no method to confirm the legitimacy of the recipients of cryptocurrency or DeFi payments. Even for transfers with low volume, it's a concern, but it gets worse for transfers with large value. Cryptocurrency transfers must always be anonymous, but there are times when it's helpful to confirm who is receiving money.

# Future Aspect of SSI

Since cyber-frauds are becoming more prevalent, it is necessary to find new solutions that will prevent them while also protecting customer privacy, business integrity, and security. In this situation, SSI concepts and blockchain are combined. By reducing cybersecurity risks and placing more emphasis on striking a balance between user self-advocacy and precise digital identity verification, they are revolutionizing the field of digital identity management. As opposed to blockchain, which provides the operational engine that maintains trust through encryption, decentralization, consensus, and self-executing smart contracts, SSI provides a framework for establishing trustworthy design architecture

In terms of the future of digital identification, SSI principles combined with blockchain have a proven track record of success by bringing stakeholders together to build a network that benefits all parties. While the global identity environment moves to greater acceptability and a better knowledge of the benefits, the use cases will continue to grow in quantity, providing the key to a more secure and practical digital identity ecosystem for everyone.

**Conclusion**

Many Digital Identity programmes are currently operating on a public and private blockchain that successfully applies SSI to guarantee privacy and security and give full user control by design. These digital identities are used for a variety of purposes, including giving proof of existence, data access and control, transparency, durability, identity portability, interoperability, minimal architecture, and full data protection capability.

There are many use cases for this technology.

Strong data privacy and security features are included into self-sovereign identity implementations at the communication layer, where identity wallets and cryptographic messaging are located, as well as the distributed ledger layer, which maintains information about decentralized identities (DIDs). These qualities make it easier to comply with some of the strictest data protection rules, such as the Consumer Privacy Act of California and the General Data Protection Regulation (GDPR) of the European Union (CCPA). The administration of the refugee population and maintaining the protection of their data is another significant use case. User account data cannot gather in honeypot situations because of the decentralized structure of SSI. As a result, unlike centralized and federated identity systems, which may expose millions of accounts to hacking, only individual accounts are at danger.

SSI technology is anticipated to open up new prospects globally, particularly for marginalized communities. One in two women in low-income nations lack an ID, which makes it difficult for them to access government services, enroll in school, and create bank accounts, according to the World Bank, which estimates that there are one billion individuals worldwide without formal identification. Given that the systems are decentralized, and all players are treated equally, SSI is anticipated to be a more democratic choice for customers.

##### References

##### 

1. <https://www.dock.io/post/self-sovereign-identity#ssi-pillar-1-blockchain>
2. <https://www.bosch.com/stories/self-sovereign-identities/#:~:text=With%20SSI%2C%20all%20public%20identifiers,any%20quantity%20%E2%80%93%20encrypted%20and%20pseudonymized>.
3. https://www.businessworld.in/article/Self-sovereign-Identity-SSID-Buoyed-By-Technology-To-Keep-Trust-Afloat-/04-10-2022-449235/
4. <https://www.tcs.com/perspectives/articles/covid-19-how-blockchain-technology-and-self-sovereign-identity-enables-the-new-normal-of-remote-learning-training-and-working>
5. <https://www.researchgate.net/publication/341130365_A_Survey_on_Blockchain-Based_Self-Sovereign_Patient_Identity_in_Healthcare>
6. <https://essif-lab.github.io/framework/docs/ssi-standards>
7. <https://101blockchains.com/self-sovereign-identity-and-decentralized-identity/>
8. <https://link.springer.com/article/10.1007/s10676-020-09563-x>
9. <https://cheqd.io/blog/self-sovereign-identity-use-cases>

**.**