walt.id

The future of Decentralized Identity:
SSI vs NFTs.

by walt.id

TL;DR

What is SSI and what are NFTs?

Self-Sovereign Identity or **SSI** is a **new approach to digital identity** that enables people and organizations to control and "**bring their own identity**" in the form of digital identity credentials.

A Non-Fungible Token or **NFT** is a **digital thing that represents ownership of something and can be traded**. An NFT can represent anything like a physical thing (house), a digital thing (crypto punk) or even an idea (intellectual property).

Comparing SSI and NFTs

While SSI has been developed to model digital identity, NFTs are used to model digital ownership. As a result, the concepts and technologies on which each approach is based differ with far reaching consequences. For example, while NFTs require blockchains, SSI can be used with or without them which is particularly important in the context of compliance and privacy.

In a nutshell: **SSI is for proving who you are, NFTs are for proving what you own.**

Choosing between SSI and NFTs

SSI is a solution for **all types of identity-related problems**. I can, for example, use SSI for identity access management (e.g. logging into a service), identity verification (e.g. opening a bank account) or to digitize and prove any other type of identity-related information from education and work records to health and insurance or financial data. Moreover, SSI can be used **for people**, **organizations** and **things** (IoT).

While using **NFTs** for identity use cases comes with issues (privacy, compliance, costs, scalability), they enable **ownership-based access management** - the idea that ownership of an asset comes with access to services, products or other benefits. This is exciting because **access rights are becoming tradable** and are no longer tied to a person or their identity.

How to get started?

Based on our experience, **building a pilot** is the best way to get started and the most effective way to quickly **build-up knowledge** and **prove the value (ROI) of SSI for your organization**.

Further Readings

Introductions to [Digital Identity](#) | [Self-Sovereign Identity (SSI)](#) | [Non-Fungible Tokens (NFTs)](#)

[Contact us](#) if you have questions or remarks. We're happy to help.

What is SSI and what are NFTs?

The **digitization of our world** is a phenomenon that **is unfolding globally and across industries**. This process is driven not only by technological innovations but also other factors that have nothing to do with technology, such as the outbreak of COVID which forced digitization of every industry. Today, people do everything online.[1]

Now, in an increasingly digital world, it is **necessary to model identity and ownership in a digital way.** Self-Sovereign Identity (SSI) and Non-Fungible Tokens (NFTs) allow us to do just that. Due to their unique properties **SSI and NFTs offer a way to encode identity and ownership in a verifiable and trusted digital format**.

This white paper elaborates what SSI and NFTs are, explains their differences and provides guidance on where and how to use them.

Introduction to SSI

What is SSI?

Self-Sovereign Identity (SSI) is a user-centric approach to digital identity that **gives people and organizations full control over their data**. As a result, SSI enables anyone to easily share their data and reliably prove their identity (i.e. who they are and anything about them) without sacrificing security or privacy.

In other words, SSI enables you to "**bring your own identity**" and this is true for potentially any type of information - from your core identity (e.g. name, age, address) to your education and work records, your health and insurance data, bank account and financial information, etc.

Moreover, SSI cannot only be used to model the **digital identities of people**, but also of **organizations** and **things** (IoT).
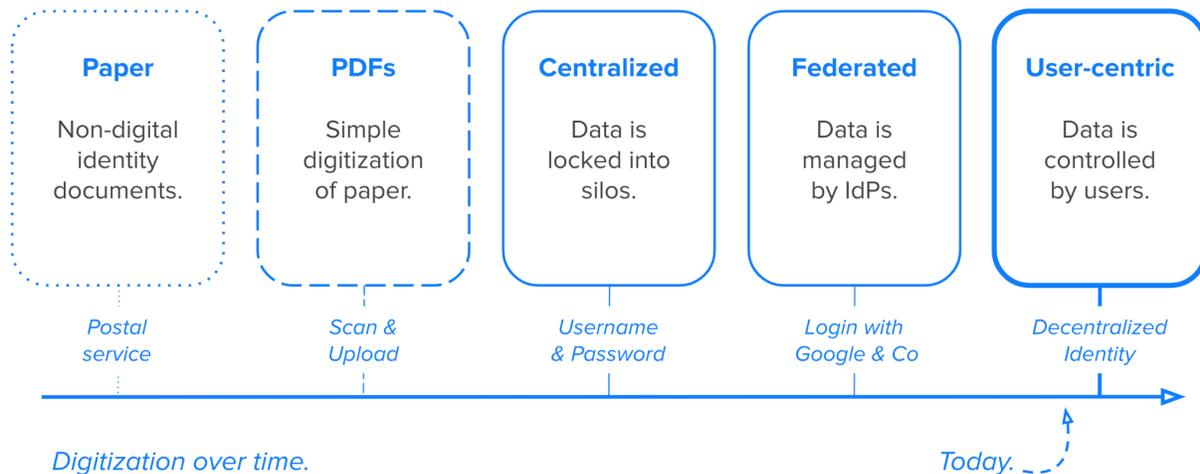
At the end of the day, SSI promises a digital world in which interactions are effortless and worry-free. It is **simply the next evolutionary step** in identity management, a new paradigm in which our digital identities are no

---
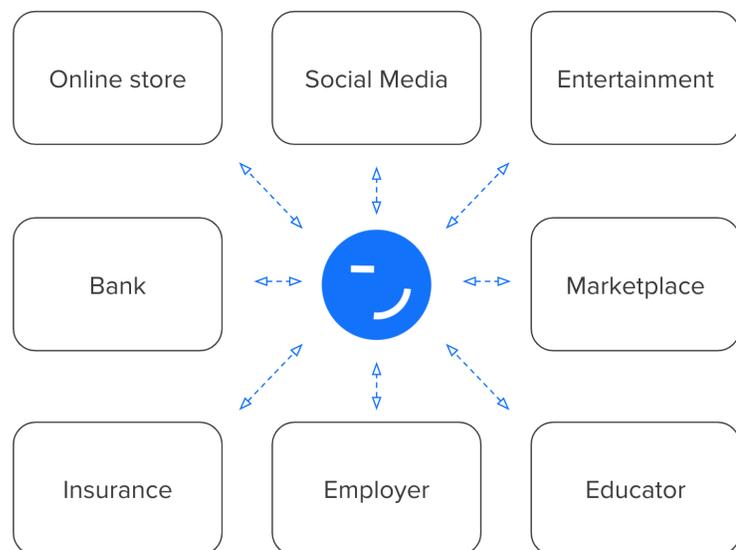
[1] *According to McKinsey [1], COVID accelerated the process of digitisation by several years: Today, more than 58% of customer interactions are digital and the majority of products and services are partly or fully digitised. In relative terms, this is a 40% increase in less than 3 years (2018-2021).*

longer fragmented and locked into silos that are under someone else's control, but only at our own disposal to be shared securely and privately.

Paper	PDFs	Centralized	Federated	User-centric
Non-digital identity documents.	Simple digitization of paper.	Data is locked into silos.	Data is managed by IdPs.	Data is controlled by users.
Postal service	*Scan & Upload*	*Username & Password*	*Login with Google & Co*	*Decentralized Identity*

Digitization over time.   *Today.*

If you want to learn more about the evolution of digital identity and understand how SSI differs from traditional approaches like Federated Identity ("login with Google & Co"), check out our Introduction to Digital Identity.

Why use SSI?

SSI offers numerous **advantages over traditional approaches to digital identity**, which is true for people and organizations. For example, user interactions become more effortless which creates better experiences for people while minimizing the friction of onboarding for service providers, such as by replacing the need for usernames, passwords, forms or online identification processes. As a result, online fraud and identity theft can be prevented and security improved.

At the end of the day, the **use cases are endless**: From official identity documents required for travel or KYC ("know your customer") to diplomas and certifications required to offer certain services or social information for creating more individual and unique experiences.

Moreover, **major players from the public and private sector are adopting SSI**, facilitated by emerging regulations and the standardization of underlying technologies. For example

- **Public sector** - Supranational organizations (European Union) and individual governments in Europe, the Americas (US, Latin America) and Asia (APAC) are subsidizing the development of solutions, adapting regulatory frameworks and building pilot projects.
- **Private Sector** - Globally, start-ups, scale-ups and large enterprises are launching projects across almost every vertical, such as banking, financial services, insurance, education, HR/employment, commerce, supply chain, health care, mobility, hospitality, among others.

How does SSI work?

SSI enables governments and businesses to issue **digital identity documents** to citizens, users and other stakeholders in the form of "Verifiable Credentials". These credentials can be anything like a passport, diploma or a bus ticket. They are stored and **managed via digital wallets and can be reliably verified by anyone they are shared with.**

Contact us if you have questions or remarks. We're happy to help.

Putting it differently, SSI allows us to model digital identity just like we are used to the way identity works in the non-digital world based on paper documents and cards. There are just some minor twists: Instead of our identity documents being made of paper or plastic, they are digital credentials made of bits and bytes and instead of storing them in wallets made of leather, they are stored in digital wallets on our phones.

You can find more information in [Introduction to Self-Sovereign Identity (SSI)](#)

Introduction to NFTs

What are NFTs?

In a nutshell, **a non-fungible token (NFT) represents ownership of something**. Let's unpack this:

First, **non-fungible** means that a token is unique in a sense that there is no other thing just like it. This means that **every NFT is one of a kind** just like there is only one painting that is the real Mona Lisa. A *fungible* token, on the other hand, is not unique. It would not make any difference if a fungible token would be exchanged for another token of the same kind such as a Bitcoin.

Second, representing ownership implies that **an NFTs is treated as the actual thing that it stands for** so that by selling an NFT you are also selling "the real thing" that it represents.

Third, **NFTs can represent anything** from physical things (like a house) to natively digital assets (like a crypto punk) or even ideas (think of intellectual property).

Once you put these properties together you can understand why people are excited about NFTs: Until recently, everyone thought that digital assets are necessarily fungible because any digital asset can simply be copied. In other words, the mainstream assumption was that digital assets are inherently abundant and cannot be scarce. As a result, digital assets could not really be "owned" by someone (since anyone can just make a copy) and if they cannot be owned, then they cannot really have value like scarce physical things do. **NFTs** change that. They **introduce digital scarcity**, **which means that digital assets can be just as valuable** (or even more valuable) **as physical things because they can be unique**:

For example, there can be NFTs that represent physical things and, therefore, have the same value as the thing they represent like an NFT that represents my actual car. However, there can also be NFTs that represent natively digital things. Their value would not be bound to any physical thing at all, which means that they could have any value. For example, an NFT that represents a handbag of which there is only one kind could be worth more than any physical handbag simply because of its uniqueness.

Why use NFTs?

While SSI allows us to model identity in a digital way using a special type of digital credentials, **NFTs allow us to model ownership of any type of asset in a digital way**. Moreover, since NFTs are anchored on blockchains, they are grounded in an immutable registry of records that cannot

be manipulated or controlled by any single entity or by malicious actors, which gives NFTs reliability in the sense that anyone can trust that they show the correct ownership distribution of assets.

Obviously, potential **use cases for NFTs are endless** and can be found wherever there's a need to digitally model ownership. As a result, NFTs will be among the most important **building blocks on which the digital world** (or something like a metaverse) **will be built upon**. Remember, NFTs can be anything which means that any type of asset will likely be encoded in NFTs, from something as intangible as ideas to physical assets that are digitized or natively digital assets that are given the quality of scarcity.

While NFTs are not a solution to most identity-related problems, one exciting set of use cases for NFTs is **ownership-based access management** or potentially also use cases which do not involve people and their personal data and, therefore, do not trigger privacy and compliance issues such as identity use cases for legal entities or machines (IoT). But more on this below…

How do NFTs work?

NFTs enable organizations or people to **create tokens that act as digital representations of potentially anything** in a way that these representations are unique, trustworthy (or at least a tamper proof record of ownership) and can be traded. NFTs are stored and **managed via digital wallets** and **can be traded.** Also, anyone can **verify which wallet controls an NFT**, without having to know who controls the wallet.

In other words, anyone can "mint" (create) NFTs and transfer them to any wallet. Whoever controls this wallet also controls the NFT, can trade and transfer it to a new wallet.

You can find more information in our Introduction to NFTs for identity.

Comparing SSI and NFTs

To build accurate mental models and understand how SSI and NFTs work, you must consider two perspectives:

- **Functional perspective** which is about understanding the implications of SSI and NFTs for adopters and the market, particularly what these technologies enable one to do.
- **Technical perspective**, which is about understanding the technologies on which SSI and NFTs are built and their properties which give rise to SSI's functionality in the first place.

We'll start with the technical perspective to provide a solid foundation for the functional analysis.

Technology

The following table shows a high level view of the core technical concepts behind SSI and NFTs.

Concepts	SSI	NFTs

Trust Registries are shared and trusted records of information.
 	
They serve as a "layer of trust" and a "single source of truth".
	SSI can be implemented with *or* without Trust Registries or even by using hybrid approaches (e.g. data of legal entities is stored on-chain but data of individuals is only stored off-chain).
	
	Different technologies are used to implement Trust Registries like blockchains or the Domain Name Service.
	
	Trust Registries are typically used as a mechanism to publish and distribute important information like:
	   ○ Information about legal entities (Issuers, Verifiers)
	   ○ Information about semantics (VC data models, contexts, policies).
		Typically permissionless blockchains are being used to implement Trust Registries due to their unique properties like their immutability and the fact that no single party controls them.
		
		Moreover, NFTs are created by "smart contracts", which can be thought of as programs or apps that run on a blockchain and are responsible for "minting" (creating) NFTs.
		
		Thus, NFTs (or at least token IDs) are stored on-chain.

Keys and a **public key infrastructure** enable core functionality like encryption or authentication.	Typically Decentralized Identifiers (DIDs) are used to establish a public key infrastructure by linking public keys or other metadata (e.g. service endpoints) to a unique identifier or address. Today, there are different types of DIDs such as did:web (uses DNS for key distribution) or did:key (peer-to-peer key distribution).	Token IDs are used to distinguish NFTs in a smart contract instance on a blockchain. Each token ID is linked to a unique identifier or address establishing a public key infrastructure as well as to metadata like the asset

		which the token represents. This way different parties can easily find and interact with each other as well as benefit from blockchains' unique properties like immutability.
Metadata In the context of identity, metadata refers to actual identity data. In the context of asset ownership, metadata describes or encodes assets.	Verifiable Credentials (VCs) are digital identity documents that contain actual identity data (e.g. name, birth date). VCs can easily and securely be shared with and verified by anyone in a privacy preserving way. Importantly, VCs (of people) are never stored on a blockchain due to privacy and compliance reasons.	Metadata can be anything like physical things, digital assets or ideas. Metadata can be stored on- or off-chain. However, to reliably model ownership of assets, metadata (or at least a hash) should be stored on-chain so that it cannot be tampered with.
Wallets are applications used to store and manage keys, VCs, and NFTs.	Today, SSI wallets are not yet broadly adopted. One of the reasons for this is because SSI wallets are more complex than today's wallets in the web3 space.	Most of today's wallets in the web3 space can be used to hold and transfer NFTs.

Deep Dive: The SSI Tech Stack

Understanding SSI requires the understanding of a few core concepts:

1. **Trust Registries**

Trust Registries serve as a single source of truth in which all participants of an SSI ecosystem can trust. Depending on the ecosystem, registries make information accessible to anyone or just a limited group.

Registries are important because they serve as a mechanism to publish and distribute keys - establishing a Public Key Infrastructure (PKI) - and other important information such as data about legal entities (Issuers, Verifiers) or about semantics (data models, semantic contexts, policies) to ensure that different parties can trust each other and the identity-related data they exchange.

Different technologies can be used to implement Registries. For example:

- **Blockchains**: Typically blockchains are used because it is unfeasible (or even impossible) to tamper with them. The fact that no single organization can change the contents of a blockchain or manipulate the terms by which it is governed are very aligned with the requirements for identity ecosystems. Today, we see a growing number of developers and organizations focusing on so-called permissioned blockchains (i.e. only a selected group can "write") like Ethereum Quorum/Enterprise. Permissionless blockchains, like Ethereum,

are still used, but less than the permissioned alternatives for a variety of reasons like scalability, costs, lack of customisable governance frameworks.

- **Domain Name Service (DNS)**: Considering certain drawbacks of blockchains, DNS can be used to serve as a Registry. Though it is not fully decentralized (considering its underlying governance framework), DNS has many advantages like its maturity and global adoption.

Importantly, SSI can be implemented with and without Trust Registries (incl. blockchains) or even by using hybrid approaches (e.g. data of legal entities is stored on-chain but data of individuals is only stored off-chain).

2. Keys and Public Key Infrastructure

Keys typically come in pairs so that there is a public key and a private key. While public keys are shared with others, private keys are never shared because they convey control over digital identities. Also, different types of keys exist which come with unique advantages and disadvantages such as ed25519, secp256k1, RSA.

Given the importance of keys, they are stored securely in specialized applications which are called "wallets".

A (distributed) public key infrastructure or (D)PKI is simply a mechanism to distribute public keys so that they can easily be found. For example, by using a public blockchain to establish a DPKI, public keys are automatically accessible to potentially anyone.

Together, keys and (D)PKI enable core functionality like encryption, authentication and signatures.

3. Decentralized Identifiers (DIDs)

DIDs are unique identifiers (URIs) which are standardized by the W3C. They are typically linked to "DID Documents" which contain metadata like keys or service endpoints. Thus, DIDs can be understood as an abstraction layer for establishing a (distributed) public key infrastructure.

A variety of "DID methods'', which are different implementations of the DID specification, exist. Considering that DID methods differ in terms of how they are created, registered and resolved, different methods come with unique properties. For example, did:web leverages DNS for key distribution, while did:key enables pure peer-to-peer key distribution. In other words, everybody can create new types of DIDs which can have different advantages or disadvantages.

Note that DIDs and public keys are considered pseudonyms and, therefore, protected under the GDPR (EU's General Data Protection Regulation), which is why DIDs and keys of people cannot be stored on a blockchain without compliance and privacy issues.

4. Verifiable Credentials (VCs) and Verifiable Presentations (VPs)

Verifiable Credentials (VCs) and Verifiable Presentations (VPs) are digital credentials that contain actual identity data of people or organizations (e.g. name, address, licenses, VAT numbers) and are standardized by the W3C. They are the digital equivalents of paper-based identity documents like passports or diplomas and as such never stored on a blockchain due to privacy and compliance reasons.

VCs are created and signed by "Issuers'' in order to provide people or other organizations with a way to prove identity-related attributes. In other words, Issuers are the data sources within an SSI ecosystem and they are typically organizations like governments, universities or banks.

VCs are usually standardized by identity ecosystems and/or industry consortia. However, they typically contain at least an Issuer's DID, the recipient's DID (also called "Holder"), the recipient's identity attributes (e.g. name, age, address, …) and information about the VC's validity (e.g. expiration date, references to revocation mechanisms) among other things.

VPs are composed and signed by "Holders". They can contain identity information from one or multiple VCs and are signed by the Holder for the purpose of presenting them to a "Verifier". In other words, VPs are the format with which the contents of VCs are shared by the person or organization that is described by the VCs.

5. Data Exchange Protocols

Different authentication and data exchange protocols are used to securely transfer identity data (e.g. VCs, VPs) between parties (e.g. from an Issuer to a Holder). They typically establish a mutually authenticated and encrypted data channel between the communicating parties.

The most common data exchange protocols used for SSI are:

- OIDC4SSI / SIOP (Self-Issued OpenID Connect Provider): An extension of a mature authentication and authorization protocol called "OpenID Connect" (OIDC).
- DIDComm: A novel protocol specifically designed for SSI and maintained by the Decentralized Identity Foundation (DIF).

The following graphic illustrates how SSI works:
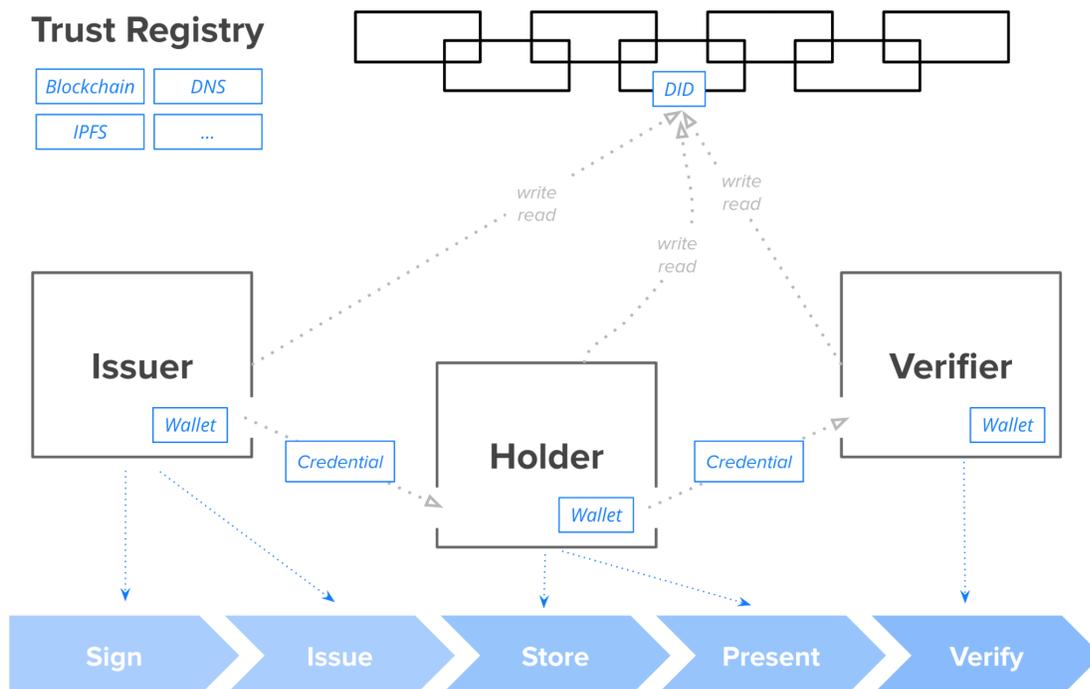
Deep Dive: The NFT Tech Stack

This section elaborates the technologies and concepts underpinning NFTs in more detail.

1. Blockchain

A blockchain is a highly secure, reliable, and decentralized infrastructure that is used to store data, exchange value and record transaction activity in a shared ledger that is not controlled by any central authority, but instead maintained by multiple parties.

Today, a variety of blockchains exist like Ethereum, Binance Smart Chain, Polygon, Solana, Cardano, Bitcoin, Avalanche, Algorand and Flow among others. Moreover, we witness the emergence of a growing number of so-called "Layer 2" networks which sit on top of blockchains and aggregate data before anchoring it in order to circumvent common challenges of permissionless blockchains like scalability and cost issues.

In the context of NFTs, it is important to mention that the most mature ecosystem is made up of blockchains that are compatible with the Ethereum Virtual Machine (EVM).

2. Smart contracts

Smart contracts are computer programs that automatically execute all or parts of an agreement between parties without the need of a trusted third party. Smart contracts are stored and executed on a blockchain.

3. Keys

Private keys are how we control and prove ownership of tokens. For more information on keys, see the last chapter (Deep Dive: The SSI Tech Stack).

4. Token

An NFT is mainly composed of two distinct parts: a token and metadata. A token is a unit of value. They are used to represent value in the digital world typically using blockchain infrastructure. Tokens are programmed using smart contracts and used to distinguish NFTs in a smart contract instance on a blockchain.

5. Metadata

Metadata is a set of data that describes and provides information about potentially anything. In the NFTs space, metadata is the actual content and the description of what the token represents. This is what gives meaning to an NFT.

NFT metadata is one of the core components of an NFT. It is typically a JSON document that contains attributes like name, description and traits among others.

Metadata can be stored on-chain or off-chain (e.g. using decentralized storage systems like IPFS or even private storage). However, in order to reliably model ownership of assets, metadata (or at least a hash) should be stored on-chain so that it cannot be tampered with.

The following graphic illustrates how SSI works and highlights the main concepts (blue):
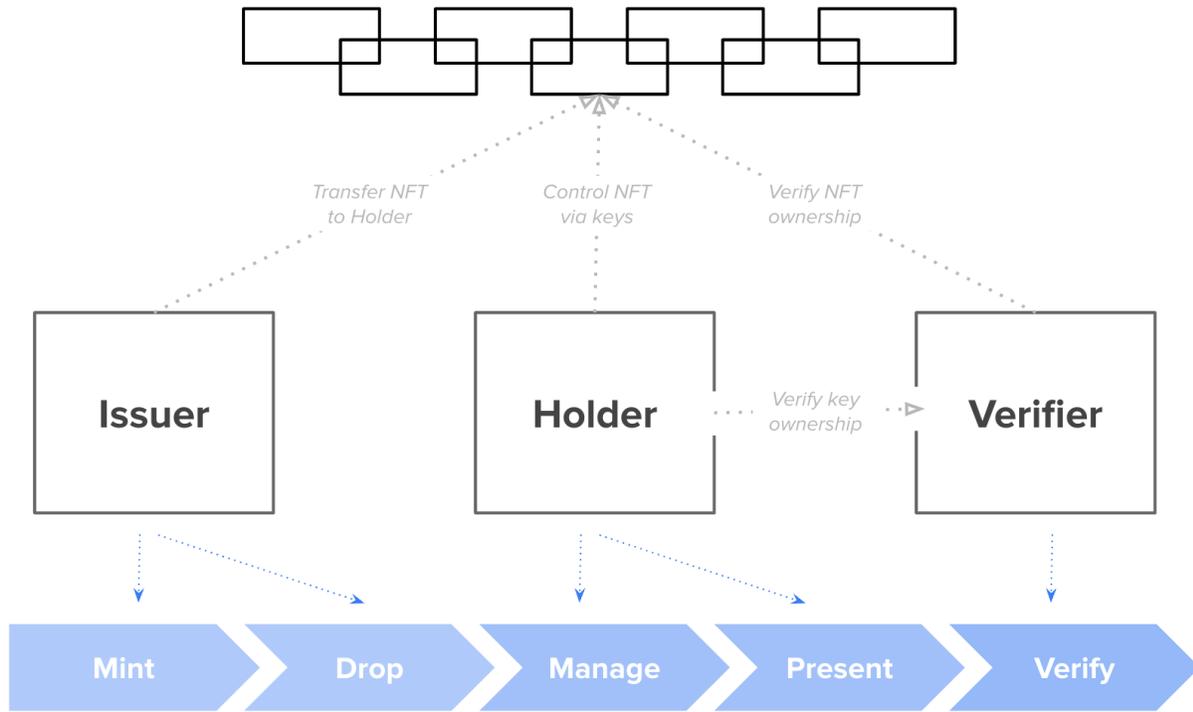
Functionality

Based on the technical elaborations, we can compare SSI and NFTs on various dimensions to understand their potential applicability for identity use cases.

Dimension	SSI	NFTs
Intrinsic attributes		
Privacy.	**Private.** Identity data (DIDs, VCs) are kept private and off-chain. Different approaches to selective disclosure further enhance privacy.	**Public.** Data (token ID, metadata) is typically stored on-chain to guarantee immutability or at least publicly accessible (e.g. IPFS).
Compliance.	**Compliant.** Compliance with data protection and privacy regulations (e.g. GDPR) if implemented correctly.	**Compliance Issues.** Storing metadata of people on a blockchain is in conflict with data protection regulations (e.g. GDPR).
Cost.	**Cheap.** SSI is cheap considering that VCs are	**(Potentially) Expensive.** NFTs require smart contracts and

Contact us if you have questions or remarks. We're happy to help.

	created and transferred "off-chain".	transactions which trigger fees that can be expensive depending on the underlying blockchain.
Scalability.	**Scalable.** SSI is scalable considering that VCs are created and transferred "off-chain".	**Limited Scalability.** NFTs require smart contracts and transactions which imply potential scalability issues of the underlying blockchain.
Zero Trust.	**Requires Trust in a 3rd party.** SSI requires trust in the "Issuers" of VCs in a sense that their claims are true and free of unintentional errors.	**Requires Trust in a 3rd party.** NFTs require trust in the "creators" of NFTs actually having the rights required for minting it (e.g. legal ownership, intellectual property).
Dependency.	**(Potentially) Dependencies.** While SSI can be run without 3rd party dependencies, the fact that many SSI operations happen off-chain (e.g. creation/signing of VCs, data storage) implies that most adopters will likely outsource certain operations to 3rd parties.	**No Dependencies.** Given that NFTs are created by smart contracts and can be stored on-chain, it is comparably easy to minimize or even prevent dependencies on 3rd parties.
Verifiability.	**Verifiable.** VCs can verified across multiple dimensions like integrity (consistency), authenticity (not corrupted), validity (not revoked or suspended), provenance (data origin), accreditations (authority of data sources), semantics (ontologies, vocabulary, policies (issuance, verification)	**Verifiable.** NFTs can also be verified across multiple dimensions like integrity, authenticity, provenance or semantics.
Flexibility.	**Identity Binding.** VCs are bound to a specific party ("holder binding") and are therefore not transferable. However, SSI allows for delegation, mandates and custodianship.	**Tradable Commodity.** NFTs are not bound to a specific party. They can be traded and change owners at any time. However, it would be possible to construct something akin to the holder binding in SSI.
Complexity.	**Complex.** SSI is comparably complex considering the many on- and off-chain concepts and protocols	**Simple.** NFTs are comparably simple, considering that they are created by a smart contract and can simply be

Contact us if you have questions or remarks. We're happy to help.

	involved in SSI implementations.	transferred via on-chain transactions.
Interoperability.	**Abstraction Layer.** SSI allows the abstraction of Trust Registries (blockchains), data storage, data representation and data exchange protocols, which implies a high potential for interoperability.	**On-Chain Limitations.** NFTs are bound to their underlying blockchains, which introduces well-known interoperability challenges between different blockchains.
External Factors		
Standards.	**Maturing Standards.** SSI technologies are being standardized in various standardization groups like W3C, OpenID Foundation, Decentralized Identity Foundation and even by the EU Commission (EBSI, ESSIF)	**Early Standards.** While there are two EVM standards driven by the Ethereum community (ERC-721, ERC-1155) NFTs are comparably nascent and less standardized.
Adoption.	**Public Sector & Enterprise.** SSI has seen most adoption in the public sector as well as with enterprises (e.g. banking/finance, HR, education, supply chain).	**Web3, creators & consumer brands.** NFTs have mostly been used by the web3 and creator communities as well as a growing number of consumer brands.
Readiness.	**Missing Wallet Infrastructure.** One of the biggest barriers to adoption is the current lack of SSI wallets on the market.	**Ready for adoption.** Considering the simplicity of NFTs they can already be used via existing web3 wallets.
Regulatory.	**Emerging Regulations.** New regulations such as eIDAS 2 and AMLR in Europe will force the adoption of identity wallets across Europe, which may also foster the broad adoption of SSI.	**No Regulatory Backing.** Today, there are no regulations in sight that would allow or constitute a legal foundation for the use of NFTs for identity use cases, particularly not for (AML) regulated industries.

Choosing between SSI vs NFTs

As a rule of thumb, we can say that **SSI is for proving who you are** and **NFTs are for proving what you own.** You can use this principle to guide technology selection for different use cases.

When to choose SSI

SSI is a solution for all types of identity-related problems. Consider the following examples:

- **Identity Proofing / Verification** - SSI can be used to identify people, organizations or even things in order to provide them with information, services or products. Identity proofing is particularly important in the AML (anti-money launder) regulated industries, but is seeing growing adoption by non-regulated industries and platforms to prevent fraud, SPAM and other malicious behavior. Simply put, you can use SSI to identify stakeholders you do not yet know.
- **Identity and Access Management** (IAM, CIAM) - SSI can be used to enable your users, customers, employees or partners to access information, services or products. In other words, you can SSI to authenticate stakeholders you already know.
- **Risk and Compliance Checks** - SSI can be used to verify any identity-related information beyond a person's or company's core identity, which can be important when evaluating risks or performing compliance assessments. For example, you can use SSI for employment background checks (education, work, criminal history) or financial due diligence (bank account information, liquidity events, credit ratings) or to verify potentially any other type of information required for transactions from insurance or health data to social proofs like ratings or recommendations.
- **Digital Credentials** - SSI can be used to digitize any type of identity-related data in order to replace physical identity documents such as paper documents or cards with digital documents that are easier to manage, share and verify as well as harder to forge. For example, think about official public sector documents such as identity certificates or about licenses or certificates that convey allowance to perform regulated activities.
- **Identity Wallets** - Finally, SSI can be used to offer new types of identity wallets or to extend applications like today's wallet solutions with the SSI capabilities.

When to choose NFTs

While **NFTs** are not designed to solve identity problems, they can be used for at least two different types of use cases:

- **Ownership-based access management**: The idea is that ownership of an asset comes with access to information, services, products or other benefits. This is exciting because access rights are becoming tradable and are no longer tied to a person or their identity.

In other words, NFTs unlock new types of use cases where access depends only on what you own, not on who you are. For example:

- Content, like articles or podcasts, can only be accessed by people who already hold NFTs from the respective creator.
- Special discounts for or early access to new products that can only be claimed by holders of NFTs from a special series.
- New maps or challenges in online games that can only be played by holders of NFTs that represent certain digital assets like skins or trophies.

- **Non-human identity (maybe)** - NFTs may be used to model the digital identity of non-human entities like organizations or things considering that data protection laws and privacy issues only concern individuals. In other words, for use cases in which data about organizations or things must be public or even stored on-chain, NFTs may offer a solution. In such cases, concepts from NFTs and SSI may even be merged such as by combining the concepts of DIDs and token IDs or by encoding VCs as NFT meta data.

You can find more information on these use cases in our [Introduction to NFTs for Identity](#).

How to get started?

Based on our experience, the best way to get started is to **collect practical experience by building pilot projects**. This will help you to quickly **build-up knowledge** and **prove the value (ROI) of SSI or NFTs for your organization**.

If it turns out that NFTs are not the right technology for solving your problem (which is typically the case if you're trying to solve identity-related problems) you can check out our **Pilot Playbook** which guides you through the process of planning and building pilots with SSI in five steps:

1. **Identify Use Cases**: A framework and examples to help you discover opportunities.
2. **Select Use Cases**: A matrix and different selection criteria will help you analyze and prioritize use cases.
3. **Select an Ecosystem**: An elaboration of ecosystems and a simple approach for selecting the right one for your organization's operating model.
4. **Plan your Implementation**: Guidance on setting project requirements and the technology selection and the question of "buy vs. build".
5. **Implement your Pilot**: Guidance to ensure the successful implementation of your project.

View and download a [free copy of the Pilot Playbook.](#)

Walt.id offers developers and organizations an easy and fast way to adopt decentralized identity.

All products are open source (Apache 2), based on open standards (W3C, DIF, OIDF, EBSI) and used by governments, public authorities and businesses across industries (e.g. banking and financial services, web3, education, HR, marketplaces).

To ensure client's success, industry-leading experts provide holistic services from conception over the implementation of pilots and production system to enterprise support and managed cloud services.

For more information visit our **website** or **contact us**.

Contact us if you have questions or remarks. We're happy to help.