Introduction to **Digital Identity.**

by walt.id

TL;DR

What is “Digital Identity”?

Think of your digital identity as the sum of **all the (digitized) information that exists about you**. For example:

- core identity attributes (name, address or birthday),
- education and work history (diplomas, work records, certificates),
- health and insurance data (medical reports, prescriptions, vaccination passes),
- financial information (bank account information, transaction histories)..

To sum up, your digital identity describes who you are in every aspect of your (digital) life.

Evolution & Approaches

On a high level, we can distinguish two different periods in identity management:

The era of silos - dominated by centralized systems

- Centralized Identity (“one account per service”): The main issues with this approach are usability and security (e.g. passwords are cumbersome to use and a major attack vector).
- Federated Identity (“login with ...”): While offering superior usability and security, main issues are the aggregation of too much power in a few hands (lock-in, dependency, privacy issues) and built-in limitations (no centralized system can support every use case).

The rise of ecosystems - enabled by decentralized systems

Decentralized identity is solving the issues of centralized and federated approaches by freeing data from silos. Its’ main advantages come from a **user-centric architecture**, which **puts users in control of their data** and enables them to share it in an easy, secure and privacy respecting way.

Today, we can distinguish different approaches like Self-Sovereign Identity (SSI) or Non-Fungible Tokens (NFTs). While each approach has unique strengths and weaknesses which makes them more or less suitable for different use cases, they are all about **enabling users to “bring their own identity”**.

Outlook

While centralized and decentralized approaches will co-exist for a the foreseeable future, user-centric architectures will gain importance and replace silos, not merely due to its advantages for users but also because of market trends (e.g. web3) and emerging regulations (e.g. eIDAS 2).

Further Readings

Introductions to Self-Sovereign Identity (SSI) and Non-Fungible tokens (NFTs)

What is Digital Identity?

There are many different ways to define identity. For our purpose, it is sufficient to understand digital identity as the **sum of all the (digitized) information that exists about you**. In other words, your digital identity describes who you are and everything about you.

This definition of identity includes, for example, your **core identity** attributes like your name, address or birthday. But it also encopmasses data from very specific parts of your life such as

- **education and work** history (e.g. diplomas, student IDs, work records, certificates),
- **health and insurance** data (e.g. medical reports, prescriptions, vaccination passes, social security information)
- **financial information** (e.g. bank account information, transaction histories, liquidity data)
- **social information** (usernames, ratings, recommendations, event tickets).

As a result, your digital identity is important for every digital interaction you have across every sector and industry.

Evolution & Approaches

The increasing digitization of our world and the emergence of new technologies and innovations have changed the face of the digital identity landscape over the past years and are completely changing the way digital identity works.

From a high level, we can distinguish two different phases:

1. The era of silos - dominated by centralized systems
2. The rise of ecosystems - enabled by decentralized systems

Let's dive in...

The Era of Silos | Centralized Approaches

It is no secret that the **internet was built without an identity layer**. However, as the world is growing more digital, **we are confronted with seemingly insurmountable issues** ranging from cumbersome user experiences to privacy issues, large scale data breaches and our growing dependence on big platforms.

In other words, while digitization has many upsides it comes at a price:

- **Lack of control over data**: Power is aggregated in the hands of a few companies, which effectively control data and lock-in users.
- **Privacy issues**: As a result of users not being in control of their data, we witnessed privacy scandals and diminishing trust in data aggregators.
- **Compliance issues**: Online service providers must store and manage user data centrally which opens them up to regulatory scrutiny and penalties.

- **Security issues**: Conventional ways for securing access to services and user data - particularly password-based authentication - proved to be unreliable and caused countless large-scale data breaches.
- **Fraud and identity theft**: Due to the lack of reliable authentication and identification tools, identity theft and other types of fraud are thriving. Online service providers and marketplaces are struggling to ensure trustworthy interactions.
- **Cumbersome user experience**: Users are forced to juggle various authentication methods (inc. many passwords) and go through lengthy online identification processes.

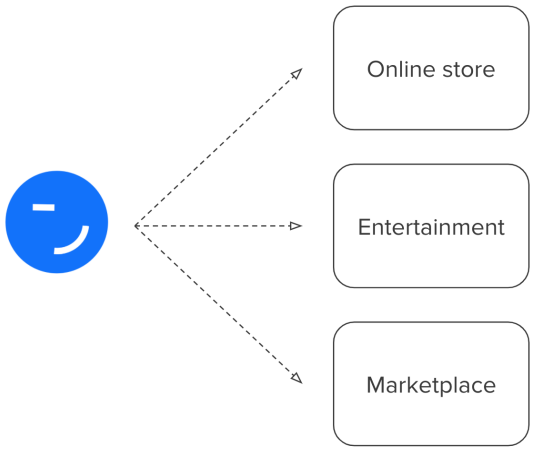
The **underlying reason** for all of these problems **is that the digital world is built on the premise of data silos**, which left us with only two ways to create something like digital identities:

Centralized Identity

In the simplest form, you can think of this approach as "**one account per service**".

To understand how it works, just think about how you conventionally use online services:

1. You create an account by offering a username (usually an email address) and a password.
2. You provide your information via forms and uploads, so that the service knows more about you.
3. Your information is then stored, managed and used by service.



This has a number of consequences:

First, you have different digital identities with each service you are using (depending on the information you share) and, in many cases, your data becomes outdated over time. Second, a part of your digital identity becomes locked into the database of the service. As a result, you end up with **fragmented digital identities which are often of poor quality and only exist in disconnected silos**.

However, the most important issues are:

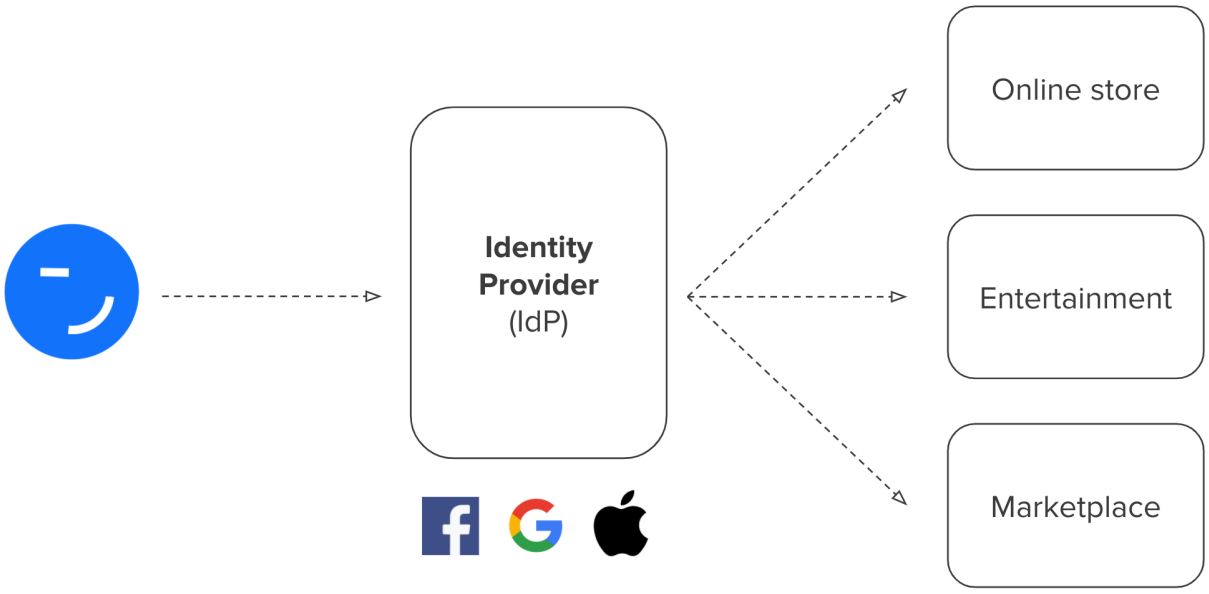
- **Cumbersome user experience** - To create and access accounts, you typically require usernames and passwords and handling a great number of those is very cumbersome.
- **Security issues** - Passwords are not only cumbersome, but also a major attack vector and a main cause for data breaches. Moreover, the centralized storage of data can create strong incentives for malicious actors to access and steal this information.
- **Lack of control** - Since users' information is stored by the service provider, users do not have control over their data or how it is used.

Federated Identity

Over time, enabled by the rise of platforms like Facebook or Google, a new paradigm emerged called “Federated Identity”. While the idea is more or less the same as with Centralized Identity (you create an account and fill it with information about ourselves), there is one major difference:

Instead of creating a new account with every service provider directly, you create a single account with a big platform, fill it with information about yourself and then use this account to share your data across different services.

In short, **you give so-called “Identity Providers”** or “IDPs” **your information and ask them to manage and share your data with other services**.



While Federated Identity offers a superior user experience (handle one account instead of many), there are two particularly **biggest issues** with this approach:

- **Power aggregation** - Federated Identity aggregates too much power in the hands of a few organizations with dire consequences for everyone else (e.g. lock-in effects, dependence, abuse of power, privacy and compliance issues)
- **Built-in limitations** - It is simply not possible to build a centralized system that can accommodate every type of identity data for every use case in every industry.

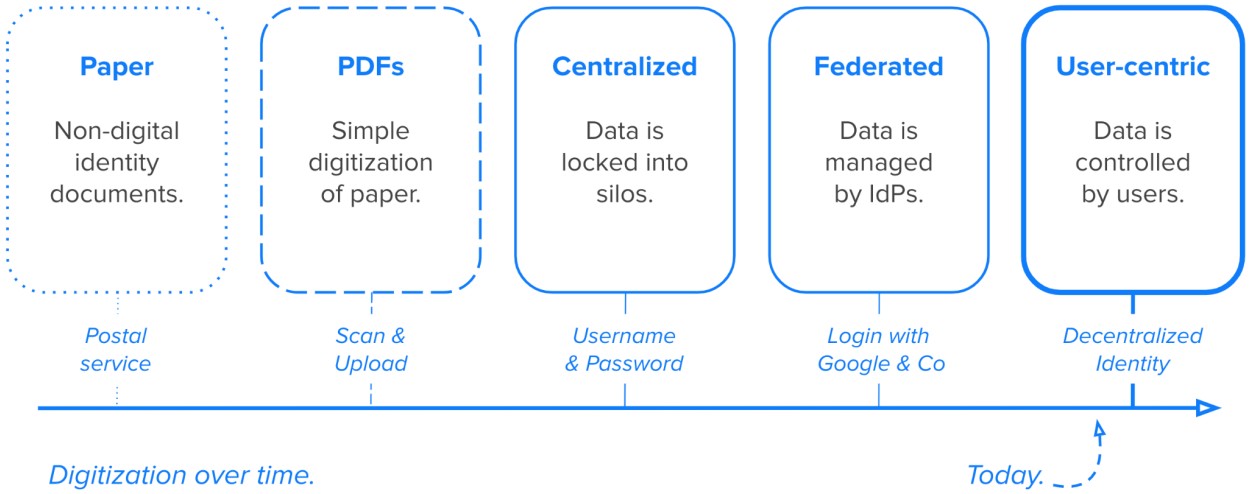
The Era of Ecosystems | Decentralized Approaches

Data silos are the villains of this story. They are the root cause of the downsides of centralized approaches to digital identity. But what **would happen if we could avoid data silos altogether?**

Imagine our interactions with digital services becoming so effortless that it would almost feel like magic. Imagine never having to worry about violations of your privacy, your independence or about falling victim to data breaches or online fraud.

This is the promise of ecosystems based on decentralized approaches to identity: **A digital world in which digital interactions are effortless and worry-free.**

It is **simply the next evolutionary step**, a new paradigm in which our data and our digital identities are no longer fragmented and locked into silos that are under someone else's control, but only at our own disposal to be securely and privately shared with others.

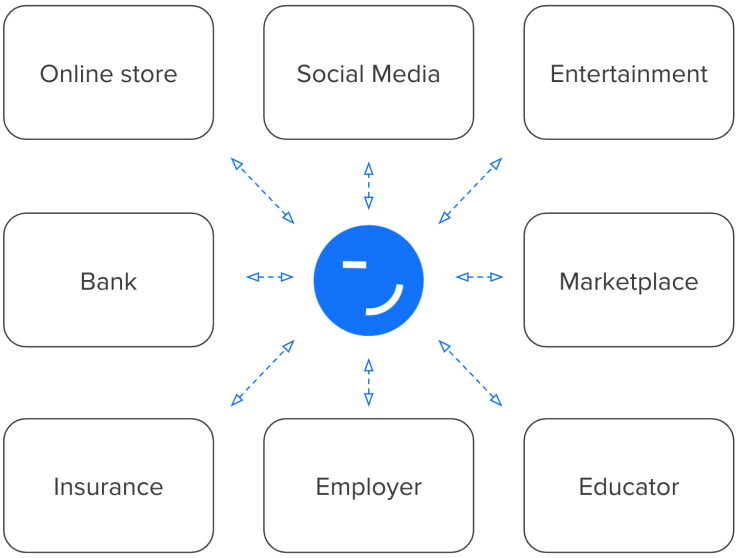


Self-Sovereign Identity (SSI)

SSI is a **user-centric approach to digital identity** that puts users in control of their data and enables them to share it with others in decentralized identity ecosystems.

At its core, SSI enables you to "**bring your own identity**" in order to easily and reliably **prove who you are and anything about you** (e.g. name, age, address, diplomas, work records, vaccination status, financial information, ...).

Importantly, SSI can be used to model the **digital identities of people, organizations and things** (IoT).



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

SSI is the **native approach for digital identity in decentralized ecosystems** and resolves the main issues we encountered with Centralized and Federated Identity:

- **Seamless user-experience**: SSI offers basically the same user experience as Federated Identity, allowing users to share data effortlessly with the click of a button.
- **No security or privacy issues**: SSI offers to avoid the need for passwords (a major attack vector) and centralized aggregation and storage of data by service providers.
- **User control to avoid power imbalance**: Users are ultimately in control of their data. They can decide where data should be stored, who has access and even enjoy data portability.
- **No built-in limitations**: SSI only exists in decentralized ecosystems which are built by a great number of individuals and organizations based on open-standards. As a result, decentralized ecosystems can be extended over time to incorporate any type of identity data for any use case in any industry.

You can read more about Self-Sovereign identity here.

Non-Fungible Tokens (NFTs)

Non-Fungible Tokens or NFTs are another approach that gained popularity over the last years, particularly in the context of the creator economy (e.g. art, music).

On the surface, **NFTs appear quite similar to SSI** considering that both approaches introduce wallets which are used to control data. In this sense, both approaches are user-centric and enable decentralized identity ecosystems. However, when comparing SSI and NFTs in more detail, it becomes clear that they are **fundamentally different creatures** which have been created for different purposes:

- **SSI is about who you are.** It is the native approach for digital identity.
  For example: There is just one passport that proves my core identity and this passport is inherently tied to myself in a sense that it makes no sense to sell or trade it.
- **NFTs are about what you own.** It is the native approach for digital ownership of assets.
  For examples: There is just one specific digital piece of art (e.g. crypto punk #5822) which exists completely independently of its owner and it makes sense to sell or trade it.

While it makes sense to use SSI in most identity-related use cases, there is still room for NFTs in identity management.

Read more about NFTs here.

Outlook

Today, centralized approaches to digital identity are clearly dominating as data silos are deeply backed into the very fabric of our digital world. Consequently, centralized and decentralized approaches will co-exist for the foreseeable future. However, it is also evident that user-centric architectures will become the new standard for various reasons, such as:

1. **Added value**: Decentralized identity has too many advantages over centralized approaches (e.g. user experience, data control, privacy, security). It simply is the native way to model identity in the digital world.
2. **Trends**: The COVID pandemic forced the digitization of every industry creating a world in which people do everything online. At the same time, the rise of web3 forces re-decentralization and the disintermediation of centralized platforms and gatekeepers. The increased digitization combined with the emergence of decentralized ecosystems is perfectly aligned with the value proposition of Decentralized Identity.
3. **Regulatory Pressure:** Regulators are putting users in control of data to correct today's power imbalances - Europe is leading the way with the GDPR (data protection), PSD2 (opening up financial information), eIDAS 2 (forcing the adoption of user-centric eID and wallets), AMLR (allowing user-centric eID for highly regulated industries), DMA (limiting the power imbalance in favor of big tech).
4. **It's becoming a thing**: While Decentralized Identity (SSI, NFTs) was widely unknown one or two years ago, it is something that everybody is talking about today - from governments to thought leaders of the identity industry. Moreover, a broad set of global standards is being finalized and setting the stage for rapid adoption.

To sum up, **Decentralized identity is** nothing less than **the next evolutionary step in digital identity management**. It is better suited to meet the needs of today's highly digitized world and even being pushed by regulators. **It will only continue to gain importance and replace silos**.

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.