The rise of identity ecosystems

This blog post explains "identity ecosystems", which are transforming the identity industry by enabling user-centric, decentralized identity systems on a global scale. You will learn what identity ecosystems are, why they are important, how they work and see practical examples driven by governments as well as the private sector.
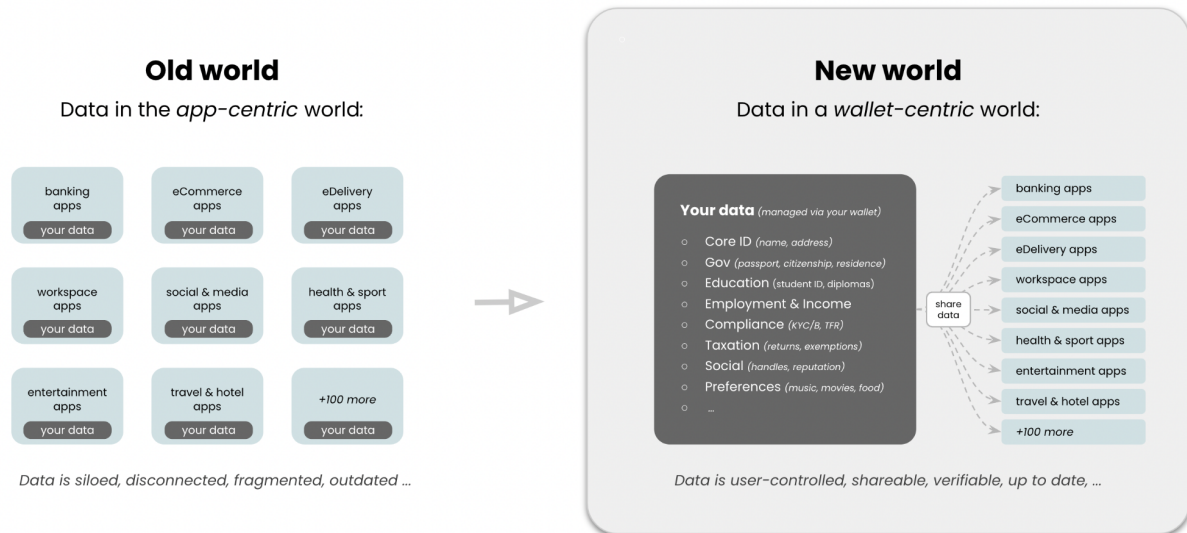
Let's dive in.

The paradigm shift: From silos to ecosystems

The internet was built without a native identity layer, which means that everybody who has built websites and apps over the last decades had to take care of identity themselves. As a result, digital identity has been built on top of centralized databases that ultimately enable visitors of a website or an app to create an account and populate it with data. This organic development of millions of identity systems that effectively establish "walled data gardens", created a digital world in which user data is siloed, fragmented and disconnected.

However, the world is changing and so is the identity industry and its underlying infrastructure. The reason for this is simple: User data is moving from apps (traditional model) to the users (wallet-centric model). It is this paradigm shift that enables a digital world in which users "bring their own identity". As a result, data is user-controlled, easy to share, reliably verifiable and always up to date.

Paradigm shift: Bring your own identity.

Old world

Data in the *app-centric* world:

banking apps — your data	eCommerce apps — your data	eDelivery apps — your data
workspace apps — your data	social & media apps — your data	health & sport apps — your data
entertainment apps — your data	travel & hotel apps — your data	+100 more — your data

Data is siloed, disconnected, fragmented, outdated ...

New world

Data in a *wallet-centric* world:

Your data *(managed via your wallet)*

- Core ID *(name, address)*
- Gov *(passport, citizenship, residence)*
- Education *(student ID, diplomas)*
- Employment & Income
- Compliance *(KYC/B, TFR)*
- Taxation *(returns, exemptions)*
- Social *(handles, reputation)*
- Preferences *(music, movies, food)*
- ...

share data →

- banking apps
- eCommerce apps
- eDelivery apps
- workspace apps
- social & media apps
- health & sport apps
- entertainment apps
- travel & hotel apps
- +100 more

Data is user-controlled, shareable, verifiable, up to date, ...

Considering that traditional approaches and technologies cannot enable such user-centric identity systems, the industry is moving from closed data silos to open data ecosystems - the topic of this blog post.

Why are identity ecosystems important?

When we talk about identity ecosystems, we refer to open, user-centric systems that enable people and organizations to interact directly with each other and freely exchange identity information. Identity ecosystems can be more or less decentralized, however, what is important is that users are in full control of their data and that there is no dependency on middlemen like today's large tech platforms.

As such, identity ecosystems establish the foundation on which new user-centric identity solutions are being built that will extend (and potentially even replace) traditional, centralized solutions ("data silos"). By freeing data from silos, identity ecosystems create various benefits compared to traditional approaches:

- People benefit from a superior user experience, enhanced privacy and security as well as full control over their data and independence from third parties.

- Organizations benefit from higher conversion rates as data sharing becomes easier, more reliable data as well as less fraud, data breaches and compliance-by-design.

What is an identity ecosystem?

One can think of identity ecosystems as a framework for creating trust between people and organizations that typically don't know each other - particularly trust that the identity information that originates from the ecosystem is correct. Identity ecosystems have two major components: One is technology ("Trust Registries"), the other is a shared set of rules ("Governance and Trust Framework").

Trust Registries

The main purpose of Trust Registries is to enable the verification of identity data. As such, they are the single source of truth - and act like a shared database - for information that members of an identity ecosystem consult in order to trust each other (based on the identity data that is being exchanged).

Trust Registries can be implemented with different technologies, such as

- Domain Name Service,
- Permissioned/consortium blockchains,
- Public/unpermissioned blockchains.

(While traditional databases could be used, they come with the drawback that the whole identity ecosystem would have to rely on the database provider, who would effectively know and control everything, which is hardly ever an option.)

Apart from the technology, there are different types of Trust Registries, each of which enables the verification of identity data across a different dimension. For example:

- "Organization Registries" verify and provide information about organizations that act in different roles such as data sources ("Issuers") or data consumers ("Verifiers").

- "Schema Registries" establish standards for and provide information about semantics and data models to ensure reusability and interoperability of data sets.
- "Revocation Registries" are used to manage the lifecycle of data. In particular, they enable data sources ("Issuers") to revoke data if it becomes invalid.

Governance and Trust Frameworks

Technology itself is not sufficient to establish trust between different parties in the context of identity. *(For example, anyone can use technology to claim to be Elon Musk, but others will trust this claim only if it comes from a trusted third party like a government.)*

To effectively establish trust, one needs Governance and Trust Frameworks which are like the constitution of the identity ecosystem. They establish a shared set of rules and practices which ensure that identity data that originates from (Issuers of) the identity ecosystem can be relied upon.

Governance and Trust Frameworks typically regulate topics such as:

- Governing bodies and processes (e.g. responsibilities for maintaining the ecosystem)
- Onboarding and accreditation (e.g. processes by which people or organizations can join the ecosystem)
- Liability and enforceability (e.g. consequences of protocol breaches)
- Trust and assurance levels (e.g. rules for Trust Registries maintenance, standards for technologies and processes like digital signatures)
- Privacy and data protection (e.g. rules for data requests and utilization)
- Security (e.g. standards managing data and secrets like keys).
- Interoperability (e.g. technical standards and specifications).

Finally, Governance and Trust Frameworks must also be aligned with regulations that impact the identity industry like data protection and privacy (GDPR), anti-money laundering (AMLR6), eID (eIDAS2) or crypto (TFR) regulations.

How do identity ecosystems work?

To enable the digitization, exchange and verification of data within an identity ecosystem, different approaches and technologies can be used like Self-Sovereign Identity (SSI), mobile drivers license (m-docs) or non-fungible and soulbound tokens (NFTs, SBTs). You can find more information about these approaches [here](#).

Regardless of which approach is used, there are always three different roles a party can play in an identity ecosystem:

- Issuer - The party who digitizes and "issues" identity data to a Holder.
- Holder - The party who controls and shares their identity data.
- Verifier - The party who verifies identity data presented by a Holder.
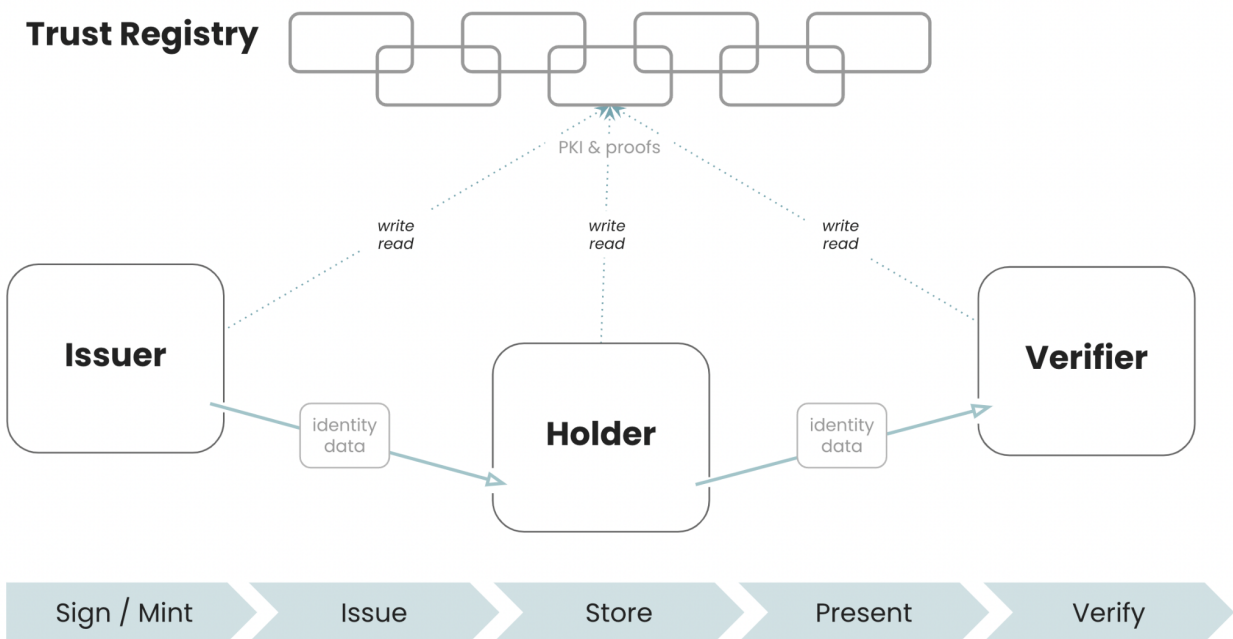
Note that a single party can take on different roles in different interactions. For example, a university may issue diplomas to graduates (Issuer), manage their own accreditations (Holder) and request education records from incoming students (Verifier).

To sum up, an identity ecosystem works by combining Trust Registries and other technologies (e.g. SSI, NFTs/SBTs) with a Governance and Trust Framework according to which different parties operate and participate in the ecosystem.

Which identity ecosystems exist?

The concept of identity ecosystems is fairly new, however, the rise of decentralized identity (based on SSI and NFTs/SBTs) automatically leads to the emergence of more and more identity ecosystems all over the globe. A useful way to think about different ecosystems is by putting them into two buckets: public and private ecosystems.

Public ecosystems

Public ecosystems are created by governments or supranational organizations (e.g. European Union) and are typically based on regulations and policies. As such, the public sector is becoming a major driver of decentralized identity by forcing the adoption of user-centric identity and wallets across industries.

Examples include Europe's decentralized identity ecosystems based on "EBSI" (the EU Blockchain) as well as its emerging eID ecosystem (based on the eIDAS2 regulation). Similarly, new identity ecosystems are emerging in the UK, US, New Zealand, Australia, South Korea and Africa.

Private ecosystems

Private ecosystems are created by private sector entities like industry consortia. They are based on contracts (not regulations and policies) that only bind organizations and people who consent to their Governance and Trust Frameworks which are typically determined by industry or even use case specific requirements.

Today, we can distinguish two types of these ecosystems: First, consortium-based ones like the Velocity Network, Alastria or ID Union. Second, open and permissionless ones like IOTA, CHEQD on the Cosmos network, identity-specific parachains on Polkadot as well as ecosystems built on blockchains like Ethereum, Polygon, EVM-compatible "Layer 2s", Near, Tezos, Flow, Algorand and others.

Takeaway: Get ready for a "multi ecosystem" future

As outlined, identity ecosystems are a useful concept to make sense of what the future of digital identity will look like, because they establish the foundation on which new (decentralized) identity systems are being built. By acknowledging that different

use cases come with different requirements depending on the jurisdictions in which they are realized (shaped by regulations) as well as their nature (shaped by customer needs and business models), it is evident that we are looking at a future in which a great number of identity ecosystems will exist - each with different Trust Registries, Governance and Trust Frameworks and consequently different flavors of decentralized identity technologies like SSI, m-docs and NFTs/SBTs.

To make decentralized identity useful on a global scale and across industries, it is necessary to build solutions that abstract all of these differences and resulting complexities for organizations and people. At the end of the day, identity should simply work, regardless of where users are and with whom they interact.

About walt.id

We are building open source decentralized identity and wallet infrastructure that supports various identity ecosystems and is used by thousands of developers as well as governments, cities, public authorities, DAOs and businesses across industries.

[Get in touch](#) with us to learn more or join our community on [Discord](#).