The role of blockchains for decentralized identity

This blog post explains the role of blockchains for decentralized identity, which is changing the face of the identity landscape by enabling more convenient, private, secure and trusted digital interactions. You will learn what blockchains and decentralized identity are, why and how these concepts often go together and what to consider when building real world blockchain-based identity solutions.

Let’s dive in.

What is a blockchain?

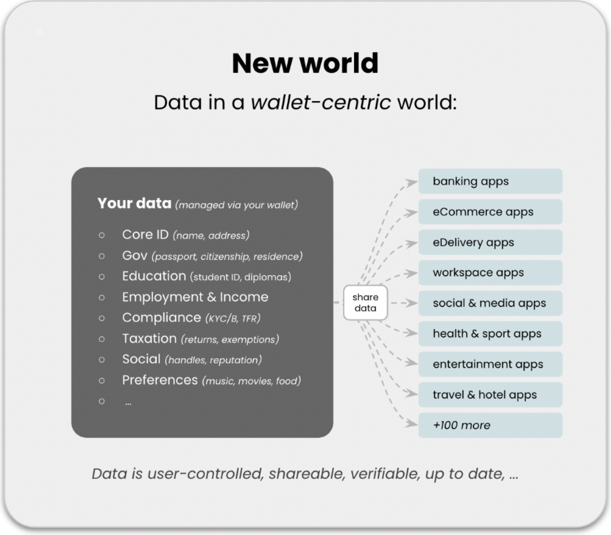
A blockchain is a decentralized, immutable ledger that records transactions using cryptography, creating a chain of blocks that are linked together through cryptographic hashes, providing security and transparency.

Here’s a more easy way to think about it:

Imagine a group of people who want to keep track of things they own and things they've done, like a shared record book. Instead of one person keeping the book and being responsible for it, everyone in the group keeps their own copy of the book and every time someone wants to add or change something, everyone else gets a copy of the new book. This way, everyone always has the same information, no one can cheat or change things without everyone else noticing, and there's no need to trust just one person to keep the book safe. That's basically how a blockchain works - it's a shared digital record book that's kept by lots of people, and when someone adds or changes something, everyone else gets a copy of the updated book. This makes it really secure and transparent because everyone has the same information and no one can change things without everyone else noticing.

What is decentralized identity?

Decentralized identity is a concept that emphasizes giving people (and organizations) greater control over their personal information online. Rather than relying on a central authority to manage their identity (as it is today), anyone can keep their own digital wallet that stores their personal information and identity documents like passports, diplomas, work records, financial or insurance information. This provides people and organizations with the ability to choose when and with whom they share their information, improving their privacy and security online, such as when they sign up for a new service or buy something. By using decentralized identity, anyone can maintain control over their personal data and reduce the risk of identity theft and other types of online fraud. It is a solution that empowers individuals and organizations and puts them in charge of their own digital identity.



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, ...

Importantly, there are different technologies or types of decentralized identity systems (which will be explored later) each of which come with different advantages and disadvantages like:

- Self-Sovereign Identity (SSI)
- Mobile Drivers License (MDL)
- Non-Fungible and Soulbound Tokens (NFTs, SBTs)

Why are blockchains important for decentralized identity?

Generally, decentralized identity typically requires so-called “identity ecosystems”, which can be understood as frameworks for creating trust between people and organizations that typically don’t know each other (by ensuring that the identity data that originates from the ecosystem is reliable). You can read more about identity ecosystems here.

One important component of every identity ecosystem are “Trust Registries”, which are the single source of truth - and act like a shared database - for information that is required to reliably verify identity data across different dimensions like data provenance, authenticity, integrity, validity and so on.

Blockchains are the preferred technology to implement Trust Registries because of their decentralization, immutability, transparency, security and efficiency. Blockchains’ strength of providing a permanent record that can be easily audited without the need for an intermediary that can control or manipulate Trust Registries is perfectly aligned with the requirements of Trust Registries in general.

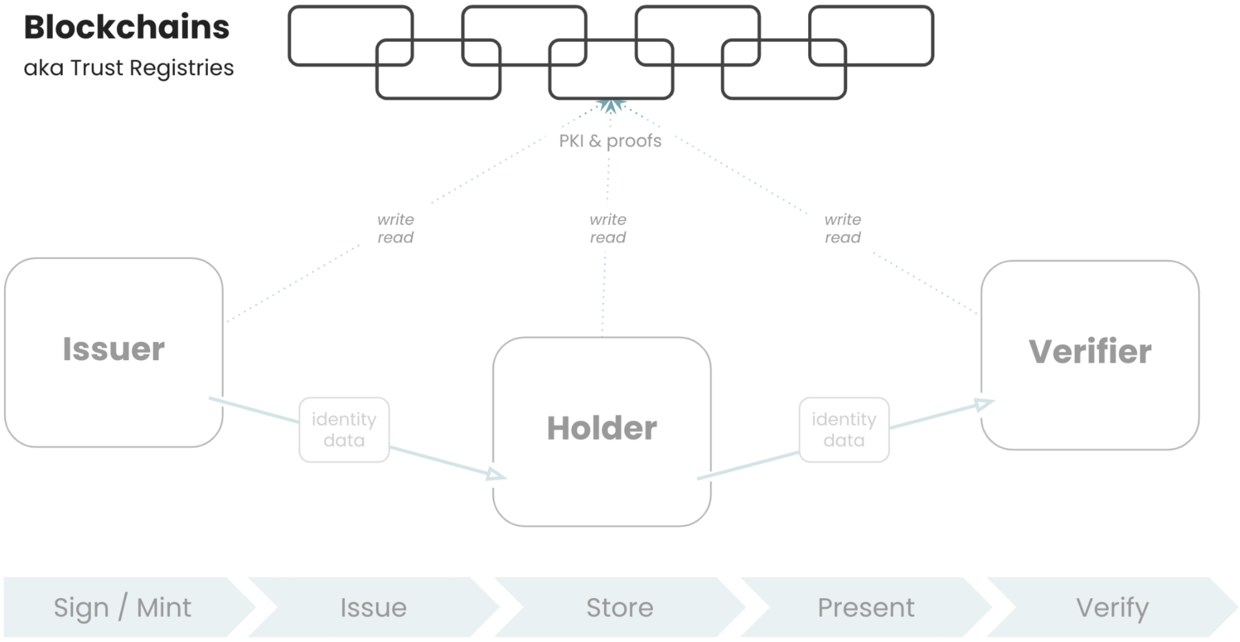
However, as we will see later, there are certain challenges that come with the use of blockchains. Moreover, different types of decentralized identity systems require blockchain to a different degree. As a result, we can say that blockchains are not a necessary component of decentralized identity systems, but definitely a useful one.

How are blockchains used in decentralized identity?

As outlined, blockchains can enable decentralized identity systems by providing a secure and transparent way to store and manage certain information without relying on a central authority - like the information typically contained in Trust Registries, for example:

- Public Keys: Decentralized identity systems use public/private key cryptography to ensure the authenticity of identity claims and to allow individuals to control their personal data. For this to work, public keys must be made public and blockchains are often used to achieve exactly that: establish a decentralized public key infrastructure (DPKI).

- Organization data: In order to reliably verify identity data, one needs to know who the sources of identity data are and if they can be trusted. Similarly, before sharing data, one should know who the party that is requesting data is. In both cases, blockchains can act as a public company registry that provides all of this information.
- Data objects and semantics: In order to ensure reusability and interoperability of data sets, it needs standardized data models and guidelines on semantics. Blockchains can act as a shared database with which these standardized data objects can be communicated efficiently.
- Lifecycle data: Most identity data changes or invalidates over time. Consequently, there is a need to manage the lifecycle of data, particularly to enable data sources to revoke data. As blockchains are not controlled by a single party (like the data source), they can be used to publish information that allows the verification of data validity. As a result, data can be validated by interacting with a blockchain, instead of the data source, which would introduce a single point of failure and compromise the privacy of data subjects.



Apart from Trust Registries, different types of decentralized identity systems, require blockchains to a different degree:

- Self-Sovereign Identity (SSI) has been specifically designed for identity use cases, and is, therefore, suitable for sharing data-rich identity credentials privately and off-chain. SSI can be implemented with or without blockchains. If blockchains are used, their main purpose is typically to establish Trust Registries aligned with data protection regulations.
- Non-Fungible and Soulbound Tokens (NFTs, SBTs) have been initially designed for the tokenization of assets, not for identity use cases. As a result, this approach is suitable for data that is not protected by regulations (like information about organizations) or for use cases that require only minimal or anonymized data proofs (aligned with privacy considerations), or use cases in which access to a service is not necessarily linked to one's identity (like tickets). While certain data associated with NFTs/SBTs can be stored off-chain, this approach can only be implemented with blockchains.
- Mobile drivers license (MDL): This approach is the most traditional one and has been developed without considering blockchains as a native component. While blockchains could theoretically be used in combination with MDL, they have not been used in practice.

You can learn more about these technologies here and here.

What are the challenges of using blockchains for decentralized identity?

The main challenges that come with the use of blockchains in the context of identity can be put into four buckets: costs, scalability, privacy and compliance. While all of these challenges can be resolved by using the right types of decentralized identity systems (e.g. SSI, MDL, NFTs/SBTs) for the right use cases, it is still important to understand their implications:

- A byproduct of blockchains' strengths like security and decentralization are transaction fees. While these fees are becoming cheaper and cheaper due to technological advances, they typically exceed costs for off-chain operations.
- Similar as with costs, blockchains may introduce scalability issues such as due to the time required for settling and executing transactions.

- Another concern are privacy issues which are particularly important to consider when using public blockchains (which are accessible to anyone). This is because the transparency of transactions can be potentially used to infer information from processes like data correlation. Hence, it is important to consider which information is handled on-chain vs off-chain.
- As the digital world is increasingly regulated, particularly privacy and data protection laws (like EU's General Data Protection Regulation, GDPR) create potential compliance issues. For example, the immutable nature of blockchains creates a tension with the GDPR's "right to be forgotten".

Finally, note that these challenges mainly arise if so-called "unpermissioned" or "permissionless" blockchains are being used (as explained in the next section).

Which blockchains are being used for decentralized identity systems?

While different blockchains can be used to enable decentralized identity it is useful to distinguish between two types: Permissioned and permissionless blockchains. The main difference lies in their access control and governance model. While permissioned blockchains are restricted to a specific group of participants who are granted rights to access and participate in the network, permissionless blockchains are open to anyone. Consequently, permissioned blockchains tend to be more centralized and controlled, with known validators and pre-defined rules, while permissionless blockchains are more decentralized and rely on consensus mechanisms to validate transactions and maintain the integrity of the network.

Examples of permissioned blockchain technologies:

- Hyperledger Besu, which is used by the EU Blockchain Service Infrastructure (EBSI) and the Velocity Network.
- Hyperledger Indy, which has been used early on in the development of SSI systems such as by the Sovrin network.
- Hedera Hashgraph, which is used by consortia in various industries.

Examples of permissionless blockchains:

- Ethereum
- Polygon
- Near
- Polkadot
- Flow
- Tezos

Takeaway: Get ready for a "multi blockchain" future

Considering that different blockchains have different advantages which make them more or less suitable for different use cases as well as the fact that the number of identity ecosystems (which often rely blockchains to establish Trust Registries) is growing, it is safe to say that we are looking at a multi-blockchain future.

Consequently, decentralized identity solutions must support various blockchains in a way that abstracts all complexities for developers, businesses and consumers. (Solutions should even go beyond this and support alternative technologies like traditional PKI systems or the Domain Name Service.) Moreover, as many new blockchains have emerged over the last years and are still emerging, it is not clear which ones will remain relevant in the long term. By limiting decentralized identity solutions to certain blockchains, implementers may be faced with big problems down the line if the blockchains they used turn out to not be amongst the "winners". Therefore, only blockchain-agnostic solutions can be considered future-proof and as such provide implementers with the piece of mind they need to build use cases across industries.

About walt.id

We are building open source decentralized identity and wallet infrastructure that supports various blockchains 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.