



# Decentralized Identity & Data Monetization.

by [walt.id](#)

*Funded by a Grant for the Web | the Mozilla Foundation*

# Table of Contents

<b>Summary   TL;DR</b>	<b>3</b>
<b>What is Decentralized Identity?</b>	<b>4</b>
Self-Sovereign Identity (SSI)	4
Non-Fungible Tokens (NFTs)	5
<b>Why monetize identity data?</b>	<b>7</b>
Identity and Payments	7
Incentives for building Ecosystems	7
<b>How to monetize identity data?</b>	<b>9</b>
Direct Monetization	9
Indirect Monetization	10
How it works	10
Wallet-Based Model	10
Registry-Based Model	11
Hybrid Model	13
<b>Comparing Monetization Models</b>	<b>14</b>
<b>Note on Payments</b>	<b>15</b>

# Summary | TL;DR

## What is Decentralized Identity?

The idea behind decentralized identity is to enable people and organizations to “bring their own identity” and control their data. Today, different approaches are used to build such systems like Self-Sovereign Identity (SSI) or Non-fungible tokens (NFTs). While both approaches have their unique strengths, a rule of thumb is to pick SSI for proving who you are (e.g. identity verification) and NFTs for proving what you own (e.g. ownership-based access management)

## Why monetize identity data?

At the end of the day, decentralized identity requires the creation of decentralized data ecosystems, which look a lot like three-sided marketplaces consisting of “Issuers” (data sources), “Holders” (data owners) and “Verifiers” (data consumers). Just like the success of marketplaces, the success of ecosystems depends on incentive structures that are aligned with and push its growth. This is where payments come in. They are a way to incentivize the most important early participants of identity ecosystems - i.e., the Issuer aka the supply side of the marketplace - to join, onboard users and provide them with re-usable identity credentials.

## How to monetize data?

We can differentiate between three different approaches for monetizing identity data:

- Direct monetization based on peer-to-peer transactions;
- Indirect monetization via a settlement layer which can be implemented via a wallet-based or a registry-based model;
- Hybrid models that combine peer-to-peer payments with a settlement layer.

## Comparing different monetization models.

While direct monetization models come with strong privacy features, are highly scalable and independent from third parties or external technical infrastructure, this approach comes with certain disadvantages such as that they are suboptimal for incentivizing credential life cycle management by Issuers and require consumers to pay for their data which creates barriers for adoption. On the other hand, indirect monetization approaches come with strong incentive structures but introduce privacy, security and dependency challenges.

## Further Readings

On [Digital Identity](#), [Self-Sovereign Identity \(SSI\)](#); [Non-Fungible tokens \(NFTs\)](#); [SSI vs. NFTs](#)

# What is Decentralized Identity?

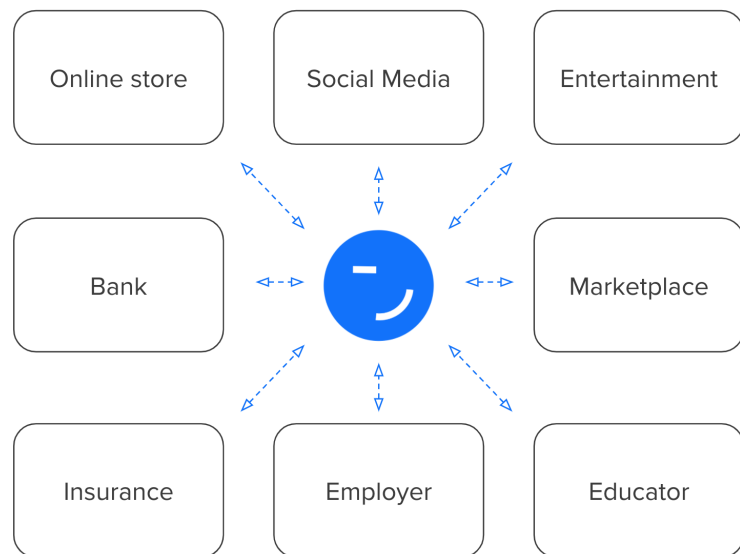
While there are many different flavors and ways to implement digital identity, we can distinguish at least two decentralized approaches that received mainstream attention: Self-Sovereign Identity (SSI) and Non-Fungible Tokens (NFTs).

## Self-Sovereign Identity (SSI)

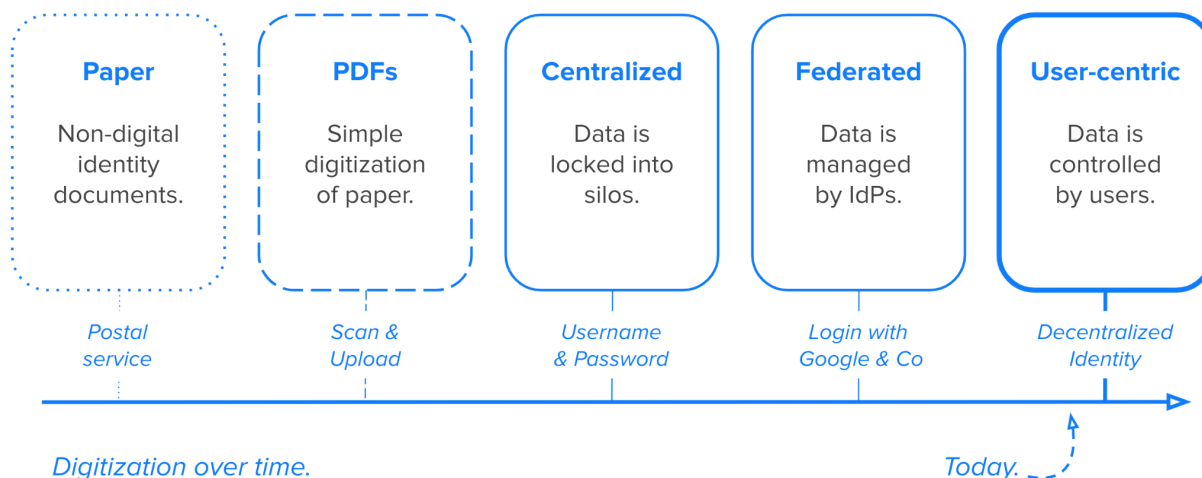
Self-Sovereign Identity (SSI) is a user-centric approach to digital identity that **gives people and organizations full control over their data**. As a result, SSI enables anyone to easily share their data and reliably prove their identity (i.e. who they are and anything about them) without sacrificing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



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](#).

Digital identity is important for every government and every business. There is no sector or industry that would not require it. As a result, the **use cases are endless**.

Examples range 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.

Read more about the [evolution of digital identity](#) and [Self-Sovereign Identity \(SSI\)](#)

## Non-Fungible Tokens (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**

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

**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.

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).

Read more about [NFTs for identity](#) or learn about the [differences between SSI and NFTs](#).

# Why monetize identity data?

## Identity and Payments

The internet was built without identity and payment layers. While we made good progress on building a layer for digital payments (PayPal, Visa, Stripe) and are seeing natively digital payment and property layers for money and assets emerge (blockchain ecosystems), we are still missing a natively digital identity layer: Our data is still fragmented across various data silos and hard to utilize. However, Self-Sovereign Identity (SSI) offers a promising approach for natively digital identity that is being built out and adopted by the private and public sector on a global scale.

Why is this important? Well, once we solve digital identity and payments every digital interaction will be trusted and effortless. Consider the following examples:

- User experiences will be seamless as information, products and services will be accessible with one click.
- Fraud will be preventable so that identity theft, SPAM, scams or document forgery will be a thing of the past.
- Compliance with diverse regulations from privacy and data protection to AML (anti-money laundering) will be ensured by design.

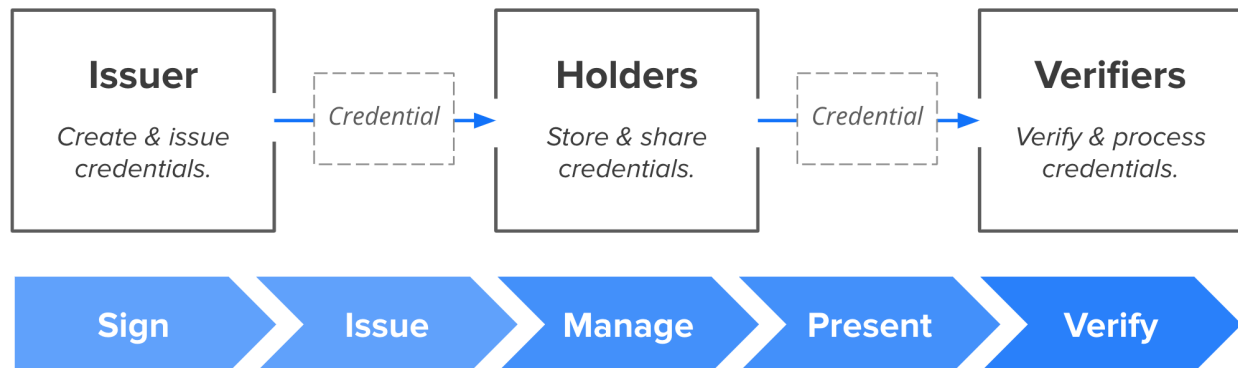
## Incentives for building Ecosystems

Incentive structures are crucial for the success of new innovations. This is particularly true for decentralized solutions which are based on ecosystems that cannot be controlled by any single party like Self-Sovereign Identity (SSI). Here is why:

SSI enables decentralized ecosystems in which different parties can exchange and verify identity-related information. Importantly, these ecosystems look like three-sided marketplaces, so that every party can take on three roles:

- **Issuers** - Parties who “issue” identity-related data to other parties (“Holders”) via digital credentials. They are the original data sources of an SSI ecosystem.
- **Holders** - Parties who receive digital credentials that contain identity data from “Issuers”. By aggregating credentials in digital wallets, Holders can build holistic digital identities.
- **Verifiers** - Parties who rely on data to provide products and services can reliably verify data that has been provided by “Holders”.

The three roles required for SSI ecosystems:



While all three types of actors must be present for SSI to function, Issuers play the most crucial role because they are the data suppliers of any ecosystem and capable of onboarding “Holders” by simply rolling out wallets and credentials to their stakeholders (users, clients, employees).

The problem is that Issuers are typically least incentivized to adopt SSI. In some cases, doing so could even disrupt their existing business models. This is why incentives for Issuers are important and where payments come in.

From today’s perspective we see two types of incentives strong enough to convert a significant number of Issuers to bootstrap a global SSI ecosystem:

- Regulatory Incentives - the idea that regulations facilitate or even force adoption like the EU’s emerging laws on digital identity wallets (eIDAS 2, AMLR).
- Financial Incentives - the idea that Issuers are being paid for supplying ecosystems with reusable identity data.

While we know that regulations will bring identity wallets (at least to Europe) within the next few years, financial incentives would enable ecosystems more rapidly and likely unlock more diverse use cases (assuming that not every potential Issuer will be forced to act as such under regulations). In other words, enabling organizations to earn money for acting as “Issuers” could significantly speed up the adoption of decentralized ecosystems and SSI.

With regards to the merits of incentivizing Issuers, it is important to understand that the value that is being monetized lies not in the data itself (which belongs to Holders) but in the reliability of an attestation of identity data which is directly linked to the trust that third parties bestow upon the Issuer. It is not the content of identity credentials that someone would pay for, but the fact that the contents have been attested by someone who is trusted to tell the truth. In other words, it is not the data that is monetized, but the trust that Issuers have built over time.

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



# How to monetize identity data?

Today, we are basically seeing three different approaches for monetizing identity data:

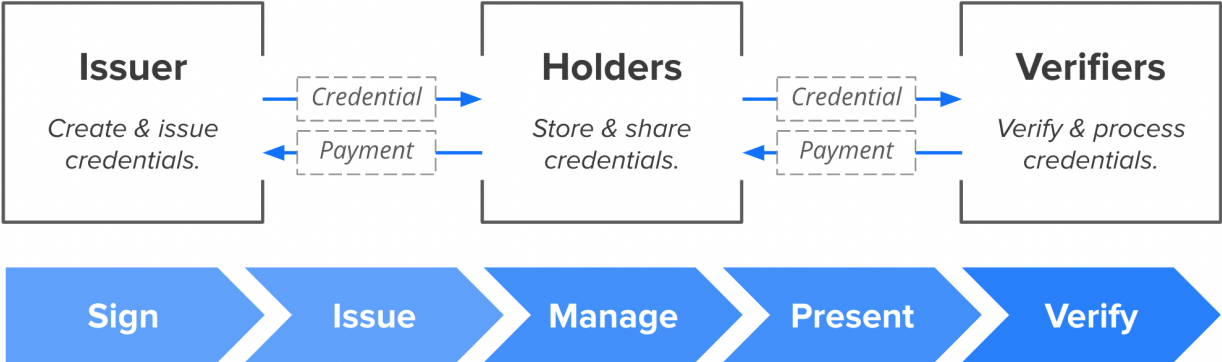
- Direct Monetization (peer-to-peer)
- Indirect Monetization (via a settlement layer)
- Hybrid Model (combining peer-to-peer payments with a settlement layer)

## Direct Monetization

The idea of direct monetization is that identity and payment flows are inherently linked so that:

- “Holders” pay “Issuers” (for issuing data)
- “Verifiers” *may* pay “Holders” (for presenting data)

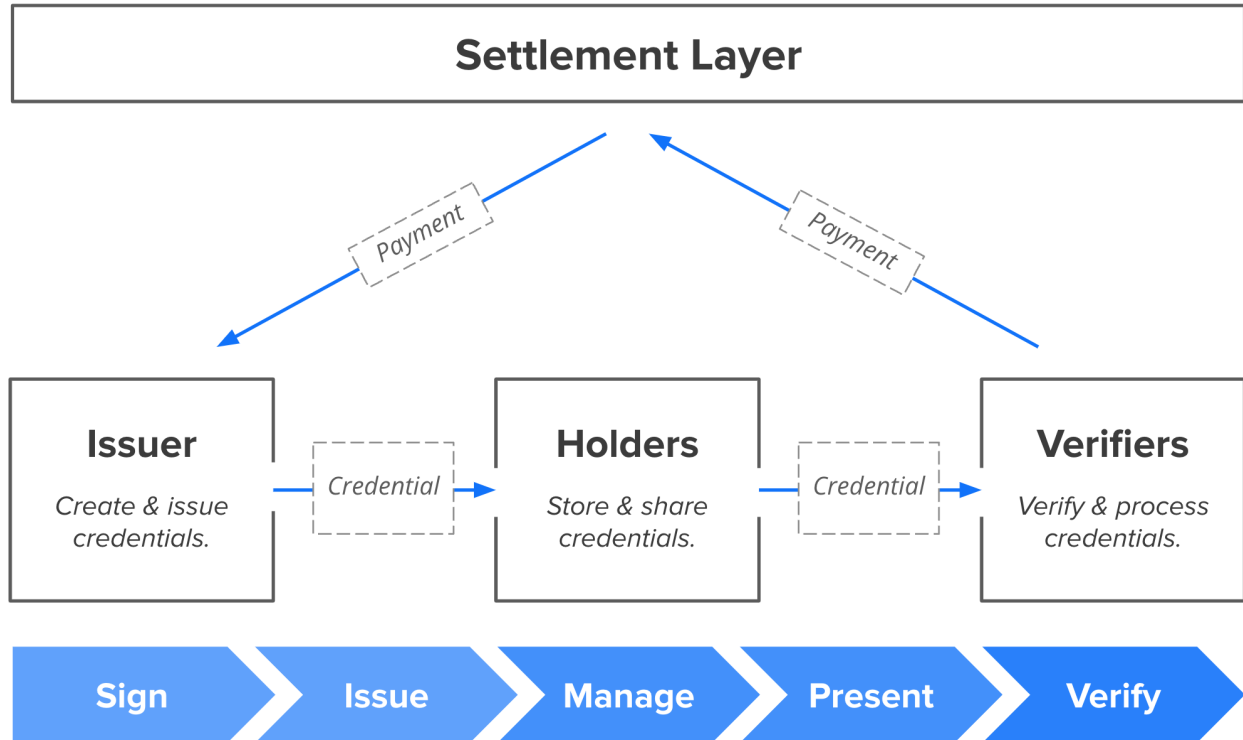
Just like identity data is exchanged directly between two parties, payment flows happen directly between two parties in a peer-to-peer fashion, possibly preceding the exchange of identity data:



For many use cases, this approach is also aligned with user expectations considering that people and businesses are often paying for their identity documents today already.

## Indirect Monetization

The idea behind indirect monetization is that only the parties who benefit most from reliable identity data should pay. In other words, “Verifiers” - like providers of information, products or services who request identity data from customers - pay “Issuers”.



### How it works

There are two different models for implementing indirect monetization:

- Wallet-based model, which requires the wallet to enable payment settlement.
- Registry-based model, which requires private registries to enable settlements.

#### Wallet-Based Model

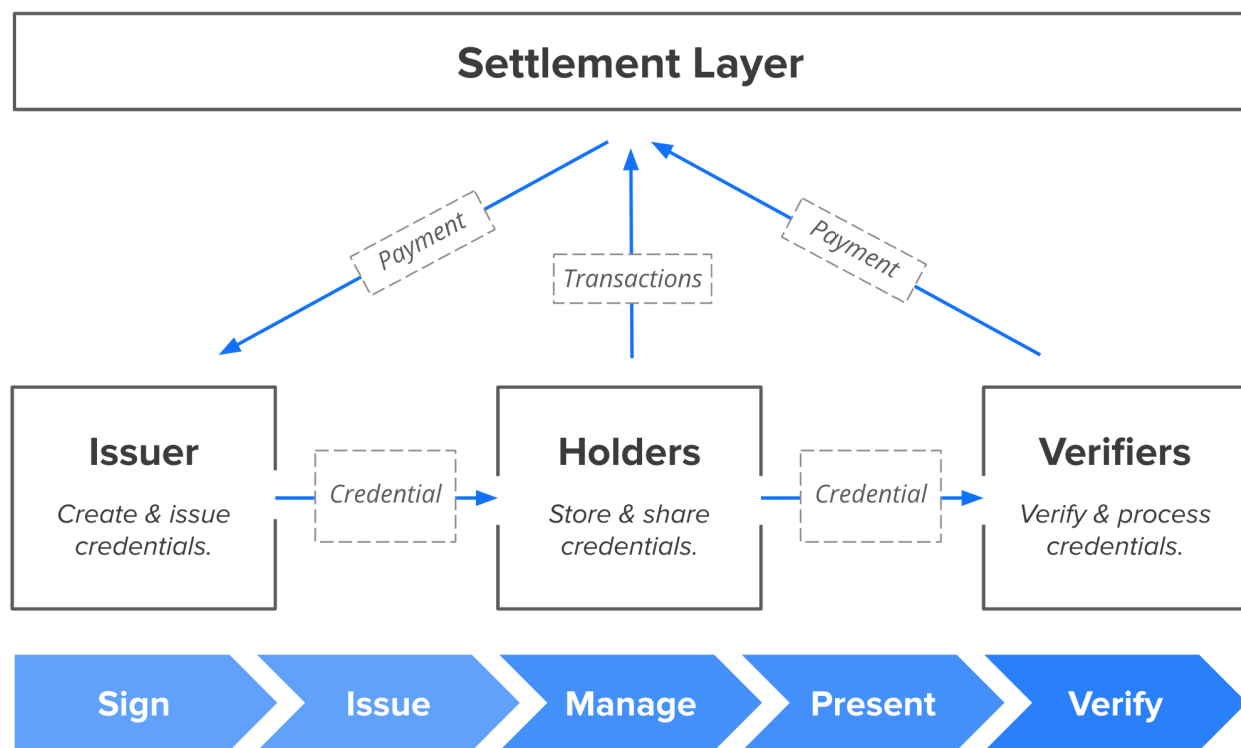
In this model, settlements are performed by a third party, which can be a legal entity (like a business) or a technology that is not controlled by a single party (like a blockchain). We can refer to this trusted third party as the “settlement layer”.

The wallet is crucial in this architecture because it provides the settlement layer with information required for executing payments, such as transaction logs. Consequently, the settlement layer must know all involved parties, particularly the “Verifiers” who are supposed to pay for reliable identity data. To enforce payments, the settlement layer must have legal contracts with “Verifiers” or collect payments in advance (held in an escrow account).

As a result, it makes sense for the settlement layer to also perform other tasks beyond enforcing payments such as attracting and onboarding stakeholders into the ecosystem, setting up governance and legal frameworks (e.g. to handle liability questions) or collecting debts.

Looking at today's banking and financial services sector, this model can be seen as an extension of open banking ecosystems that switch from centralized to user-centric identity paradigms.

*Illustration of the wallet-based model:*



### Registry-Based Model

In this model, payments are also enforced by a “settlement layer” (like in the wallet-based model). However, instead of relying on wallets for enabling settlements, information that is required to verify identity data is written to a registry that is hidden behind a “paywall”. In other words, Verifiers must pay to access information without which they could not rely on data provided by “Holders”. For example, information required to evaluate

- data provenance, authenticity, integrity and authority (e.g. public keys or accreditations).
- data validity (e.g. revocation or suspension data)
- standard conformance (e.g. data models)
- machine-readability (e.g. semantic vocabulary, contexts)

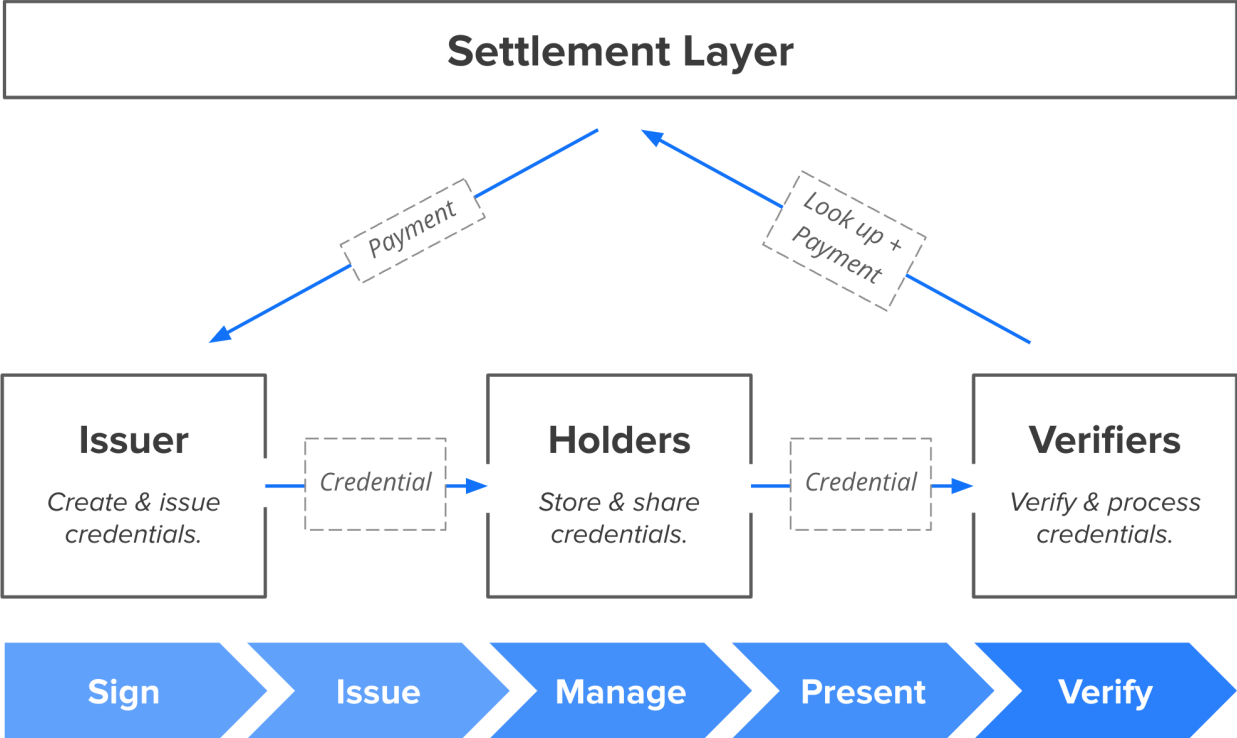
In this model, the settlement layer only needs to know “Issuers” of an ecosystem, who typically help with the creation and maintenance of the registries in order to create and maintain payment incentives. “Verifiers” must not be known in advance. They can simply pay per use, without

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

having to go through an onboarding process that includes the conclusion of legal contracts or advanced payments.

The main role of the settlement layer is to collect payments by Verifiers (for accessing information) and redistribute the payments to Issuers. As a result, this model is generally more aligned with the design of emerging decentralized ecosystems (web3).

Illustration of the registry-based model:



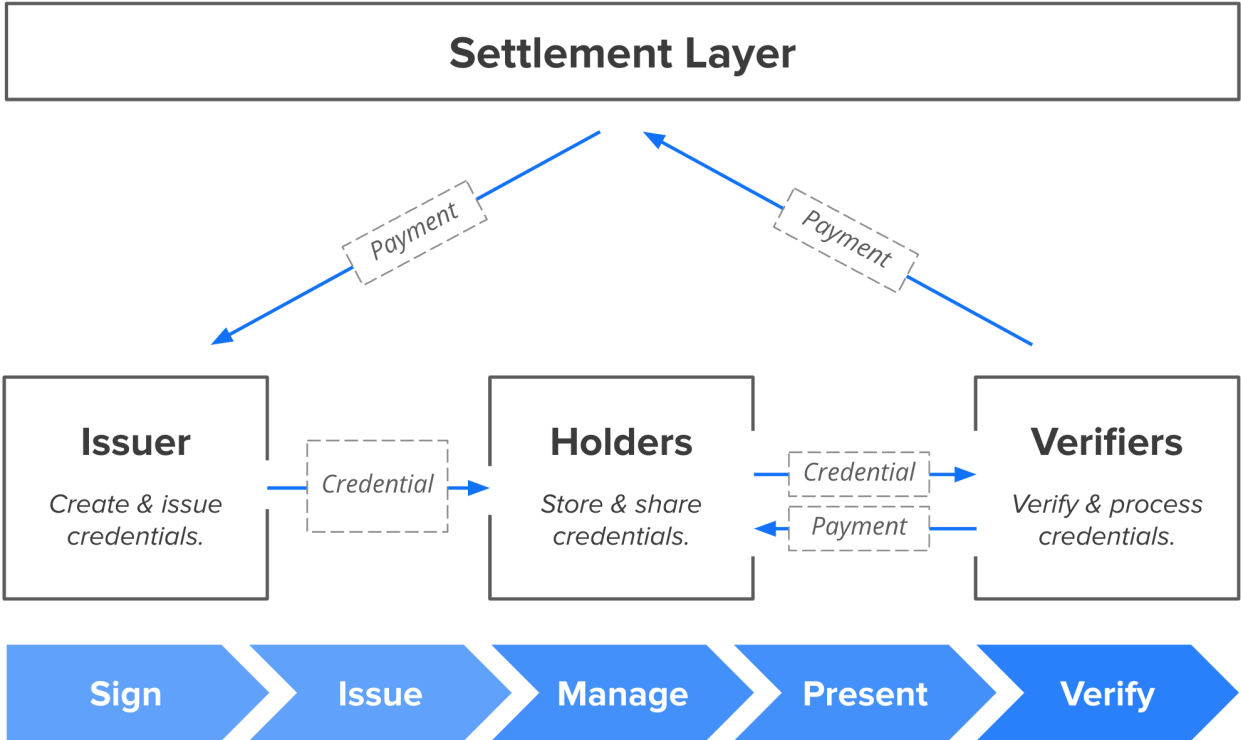
# Hybrid Model

The hybrid model, leverages ideas from direct and indirect monetization by combining

- a settlement layer for payments from “Verifiers” to “Issuers”
- peer-to-peer payments from “Verifiers” to “Holders”.

With regards to the settlement layer, both versions of the indirect monetization model (wallet- or registry-based) can be used.

*Illustration of the hybrid model:*



The main reason for adopting this hybrid model is to enable “Holders” to get financial benefits for sharing data while incentivizing Issuer’s to manage the life cycle of data because they can monetize more than once.

# Comparing Monetization Models

The following table compares the different data monetization approaches outlined in the last chapter across various dimensions in an effort to facilitate and deepen the understanding of their advantages and disadvantages:

Dimension	Direct Monetization	Indirect Monetization	Hybrid Model
How are data and payments exchanged?	Peer-to-Peer	Mediated via settlement layer	Peer-to-peer combined with settlement layer
Who can monetize data?	Issuers & Holders	Issuers (Holders only with specific implementation)	Issuers & Holders
Who pays for data?	Verifiers & Holders	Verifiers	Verifiers
How effective is the incentive structure for Issuers?	No direct incentive for maintaining credential life cycle. (Credentials are monetized once.)	Strong incentives for Issuers. (Credentials can be monetized more than once.)	Strong incentives for Issuers. (Credentials can be monetized more than once.)
How scalable is the model?	Highly scalable.	Registry-based approach is more scalable than wallet-based approach.	Registry-based approach is more scalable than wallet-based approach.
Dependencies on 3rd parties?	No inherent dependencies.	Dependency on wallet and the settlement layer.	Dependency on the settlement layer and potentially the wallet.
How private is the model?	Potentially strong privacy. (Exception: on-chain payments).	Wallet provider and/or settlement layer aggregate information.	Wallet provider and/or settlement layer aggregate information.
How secure is the model?	Potentially very secure.	Wallet providers and/or settlement layers introduce attack vectors.	Wallet providers and/or settlement layers introduce attack vectors.

# Note on Payments

Financial incentives can be created with any form of money, from FIAT (\$, €) over stable coins (USDT/C) or other “crypto currencies” (BTC, ETH) to more novel token types (NFTs). Each of these assets can potentially be used to incentivize issuers.

In all of these cases, wallets can be used to trigger such payments, for example via

- external payment service providers
- PSD2 (directly from within the wallet)
- relevant blockchains (e.g. BTC, ETH, DOT, SOL, NEAR)
- Payment protocols like the interledger protocol

Importantly, if a registry-based approach is chosen (indirect monetization, hybrid model) ecosystems that maintain the registries may introduce their own tokens and economies for identity verification (like the Velocity Network).

Moreover, you can find more detailed information about the Interledger Protocol and how to use it for peer-to-peer payments during identity data exchange flows in our whitepaper “[Decentralized Identity & Interledger Protocol](#)”.



[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](#).

Copyright © 2022 by walt.id GmbH

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