

Identidad Auto soberana con Privacidad



Otto Mora
@ottomorac



**El internet se
construyó sin una
capa de identidad**

Evolución de la Identidad Digital: Centralizada, Federada, Descentralizada...

WEB 1.0 IDENTIDAD CENTRALIZADA

WEB 2.0 IDENTIDAD FEDERADA

Las plataformas crean y manejan la identidad de sus usuarios en sus servidores. El acceso a la identidad se maneja en base a cuentas con nombres de usuario y contraseñas.

Mediante el uso de proveedores de identidad, se evita la creación de identidades duplicadas para un mismo usuario, reduciendo la fricción de los usuarios en el mundo digital.

Username

Password

 Sign in with Apple

 Continue with Google

 Continue with Facebook

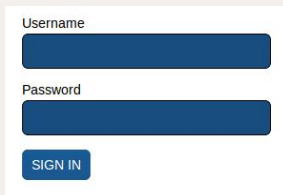
Problemática de la situación actual:

- **Mala experiencia de usuario**, las personas no tienen control sobre identidad digitales, **las plataformas controlan los datos e identidades del usuario**
- **Los datos no son portables o re-utilizables** entre plataformas.
- **Las plataformas son sujetas a hackeos:**
 - **2017 - Spambot** - 771 millones de registros expuestos. records lost. El bot expuso las claves de acceso de miles de usuarios por un problema de configuración.
 - **2018 - Aadhaar** - 1100 millones de registros expuestos. La base de datos biométrica de personas en India fue expuesta.
 - **2021 - Facebook**, hackers tuvieron acceso a 533 millones de registros de usuarios de 106 países debido a una vulnerabilidad que fue parchada en 2019.
 - **2022 - Costa Rica - Grupo Conti y Hive**. Varias entidades publicas entre ellas el Ministerio de Hacienda, Caja Costarricense del Seguro Social, entre otros se vieron afectados

Evolución de la Identidad Digital: Centralizada, Federada, Descentralizada...

WEB 1.0 IDENTIDAD CENTRALIZADA

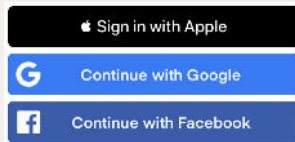
Las plataformas crean y manejan la identidad de sus usuarios en sus servidores. El acceso a la identidad se maneja en base a cuentas con nombres de usuario y contraseñas.



Formulario de inicio de sesión centralizado con campos para Username y Password, y un botón SIGN IN.

WEB 2.0 IDENTIDAD FEDERADA

Mediante el uso de proveedores de identidad, se evita la creación de identidades duplicadas para un mismo usuario, reduciendo la fricción de los usuarios en el mundo digital.



WEB 3.0 DESCENTRALIZADA Y AUTO SOBERANA

Evolución de credenciales basadas en cuentas de usuario hacia las credenciales verificables. Identidad auto soberana o *Self-Sovereign Identities (SSI)*, donde los usuarios son dueños y controlan el acceso a sus datos.



Que es la Identidad Auto soberana (SSI) y cuales son sus principios?

La **identidad Auto soberana - Self-sovereign identity (SSI)** es un enfoque de identidad digital que provee a los individuos control sobre la información que usan para demostrar quienes son a sitios web, servicios, y aplicaciones en la web.

Principles

Existence

Users must have an independent existence.

Control

Users must control their identities.

Access

Users must have access to their own data

Transparency

Systems and algorithms must be transparent.

Persistence

Identities must be long-lived.

Portability

Information and services about identity must be transportable.

Interoperability

Identities should be as widely usable as possible.

Consent

Users must agree to the use of their identity.

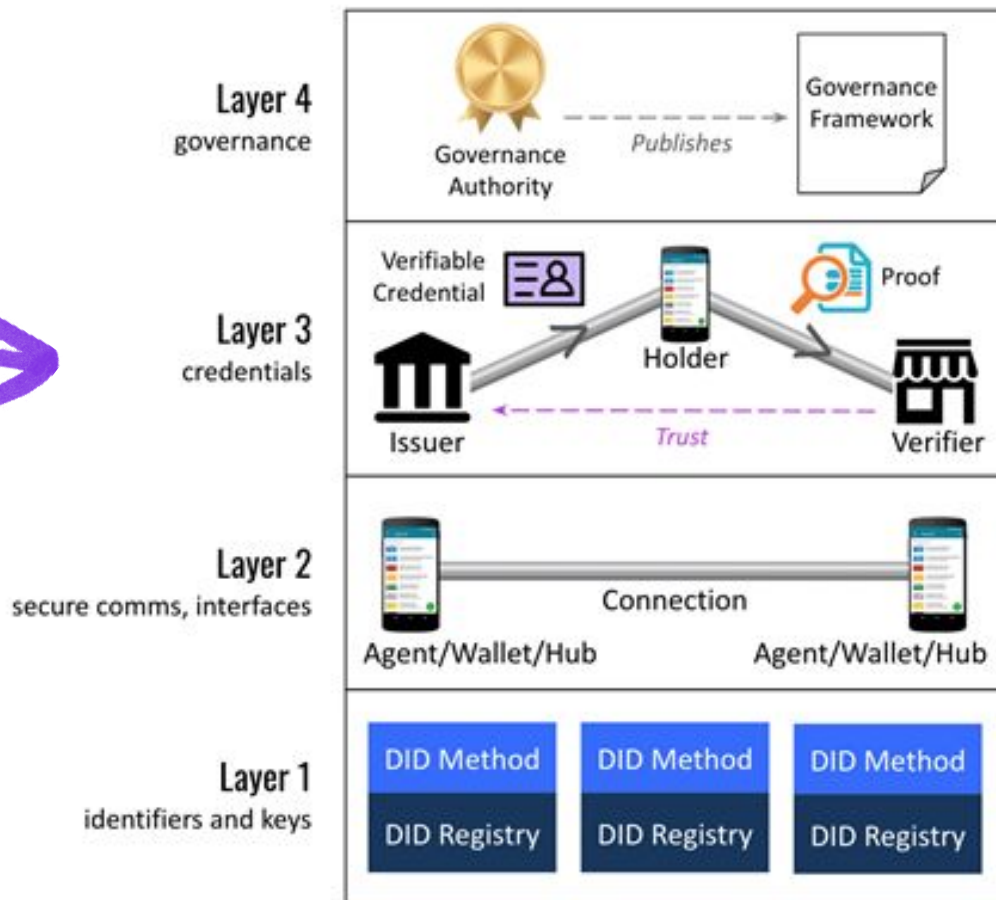
Minimisation

Disclosure of claims must be minimised.

Protection

The rights of users must be protected

Modelo de Capas de la Identidad Auto-soberana (SSI)



Actores dentro de un ecosistema SSI

La visión de SSI describe un ecosistema compuesto por 3 partes:



Emisores: entidades que emiten credenciales por ejemplo: gobiernos o instituciones educativas como universidades.

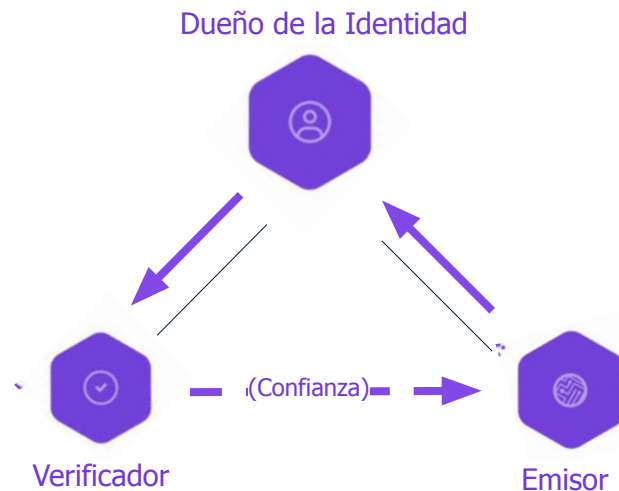


Dueño de la Identidad: persona, dispositivo o aparato que dispone de una credencial.



Verificadores: entidades interesadas en consumir o utilizar los datos de las credenciales que están en posesión del Dueño de Identidad

Este ecosistema permite que los Dueños de las Identidades tengan control sobre su información personal y puedan decidir cuales credenciales revelar a Verificadores.



Identificadores Descentralizados (DIDs) y Credenciales verificables de la W3C

Los Identificadores Descentralizados (DID)

son identificadores globalmente únicos que permiten a individuos y organizaciones establecer su identidad en Internet de forma independiente de autoridades centralizadas. Vienen dados por un formato similar al de una URL:

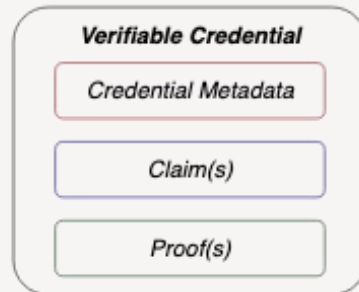
did:metodo:xyz123456789



Identificador específico del método DID

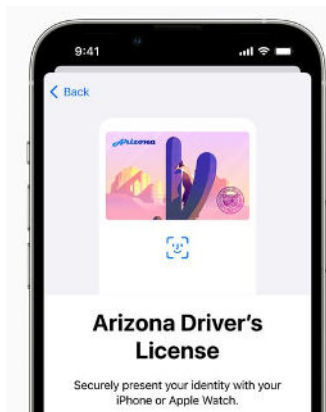
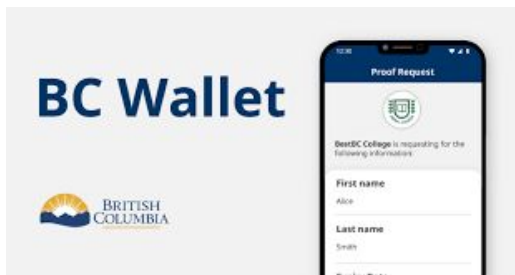
Las Credenciales Verificables son

documentos que contienen información de una forma criptográficamente segura que respete la privacidad y pueda verificarse automáticamente.



Ecosistemas SSI en Norte América y Europa

Canadá y Estados Unidos



Licencias de Conducir Digitales
(formato iso MDOC):

- Arizona
- Colorado
- California
- Maryland
- Georgia

Europa - Proyecto EUID - eIDAS2



La Comisión Europea ha lanzado un proyecto que unificará la identidad digital de todos los ciudadanos pertenecientes a la UE, mediante el reglamento eIDAS. El objetivo es cubrir carnet de conducir, certificado bancario, registro de propiedades, certificado de empadronamiento, titulación, entre otros.

Ecosistemas SSI en Latinoamérica:



Quark ID sobre zkSync

- La ciudad de Buenos Aires está emitiendo credenciales verificables para sus ciudadanos anclados sobre el Blockchain de zkSync utilizando el did method de Quark ID

Empresas de Implementación de SSI

EDENiA

(Costa Rica)

 **extrimian**

(Argentina)

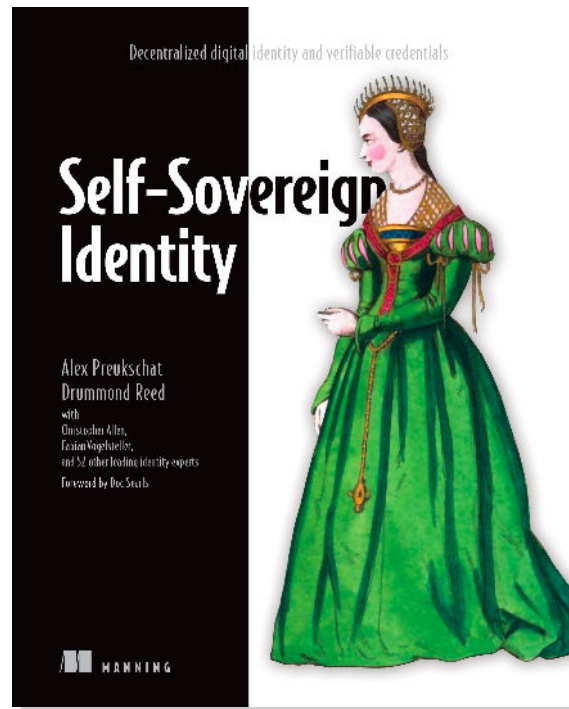
 **KayTrust**
Digital Ecosystem Platform
by NTT DATA

(Peru)

Literatura Recomendada: para aprender más sobre Identidad Auto Soberana

Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials

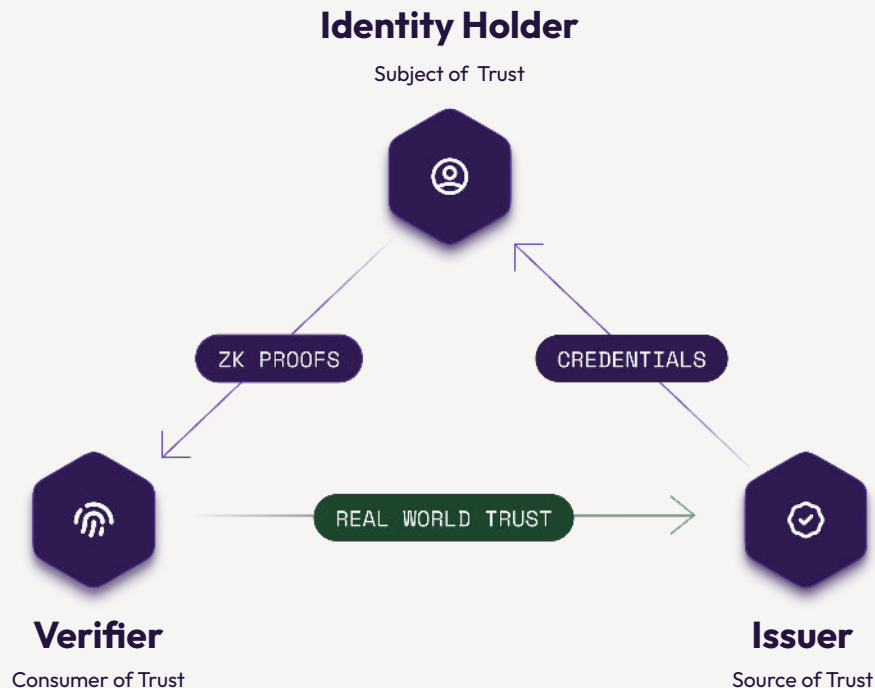
Por Alex Preukschat y Drummond Reed



Identidad
Auto soberana
con Privacidad

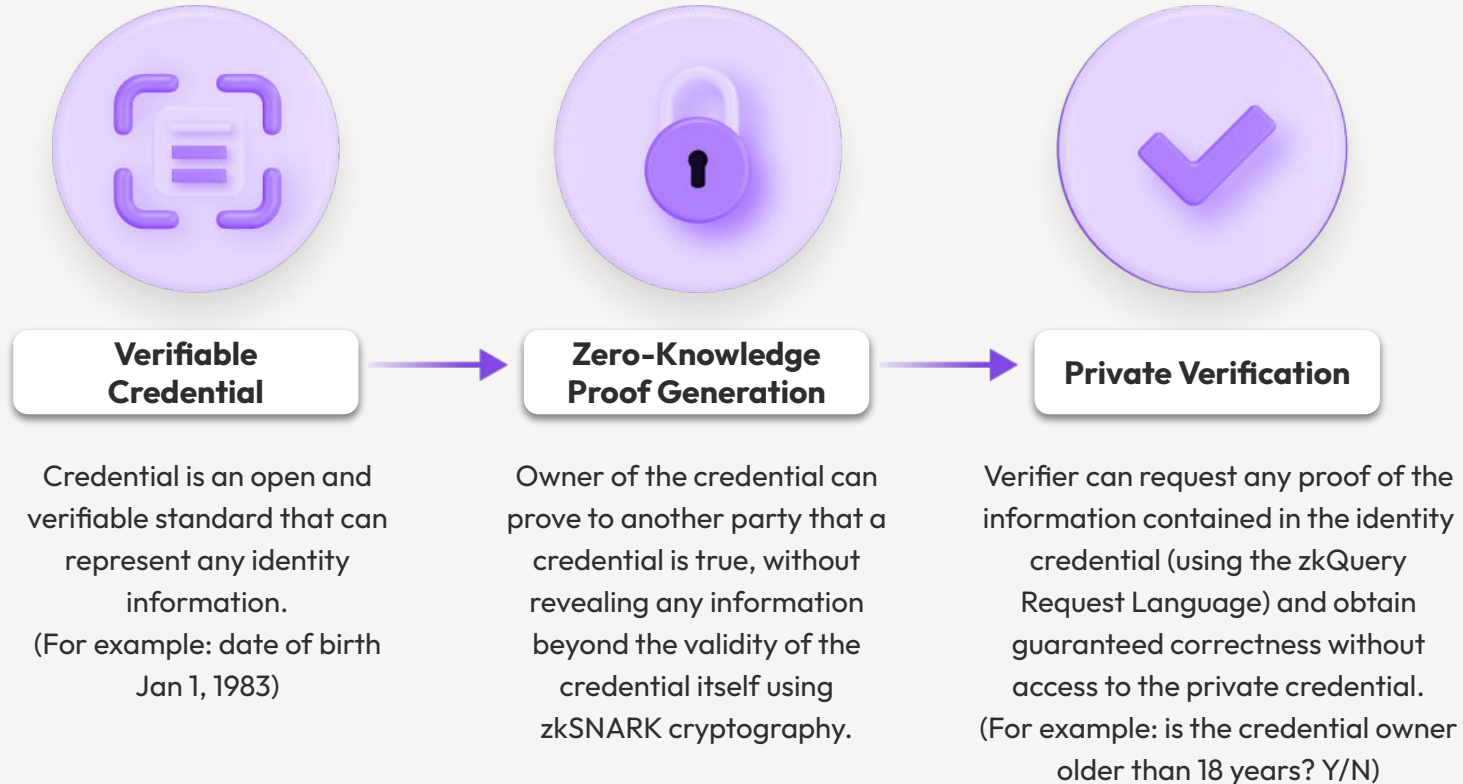


Actores dentro de un Ecosistema SSI con privacidad



Verifiable Presentations leveraging ZK Proofs

Polygon ID is based on the **user-centered** proving system to make all interactions **Private by default**



Main features of Polygon ID?



ZK Technology

Enables users to verify details of credentials they've received without necessarily disclosing personal information.



ZK Query Language

Provides a simple way for developers to design customized authentication requirements based on user's credentials.

[\(link\)](#)



Open Source and Decentralized

All tools within the Polygon ID identity infrastructure are open-source and can be self-hosted in furtherance of decentralization.



Interoperability

Compatible with W3C's Decentralized Identity (DID) and Verifiable Credentials (VC) standards.



On-Chain Verification

Users can authenticate user credentials stored in their wallets and verifiers can validate the authenticity of those credentials on-chain.

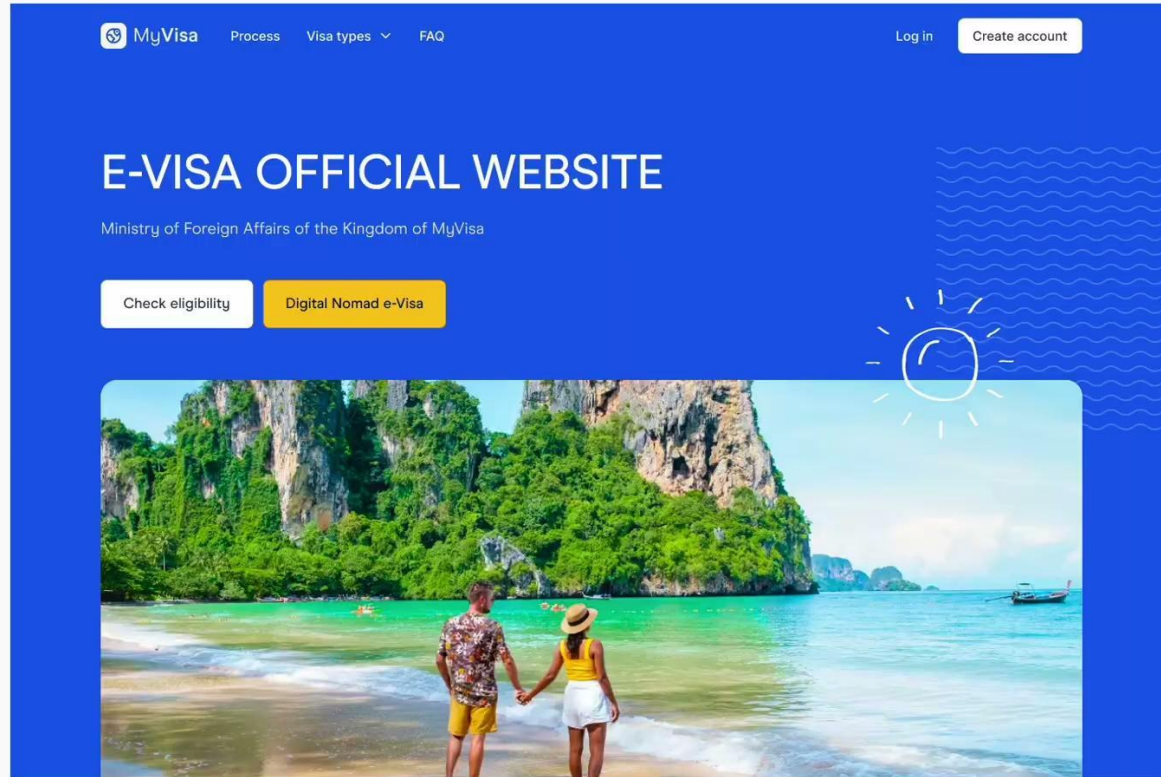
i

While a key feature of Polygon ID is its use of ZK technology, users can also disclose their identity data to verifiers through selective disclosure. Selective disclosure allows users to choose which specific pieces of their data they wish to share with verifiers allowing users to “selectively disclose” that data.

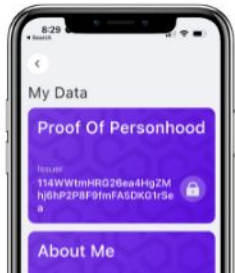
Demo Video (ID Creation)



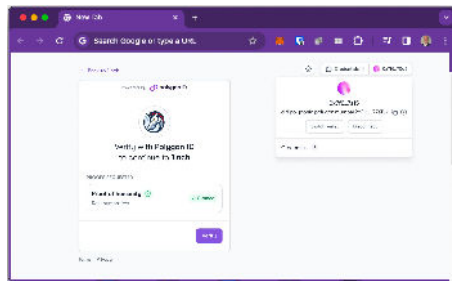
Demo Video (Digital Nomad visa)



Polygon ID Ecosystem



Polygon ID Mobile App



Polygon ID Web Wallet

The Polygon ID app (Available for [Android](#), and [iOS](#)) is a reference application. Also we have a Polygon ID web wallet currently under development to remove the app download requirement.

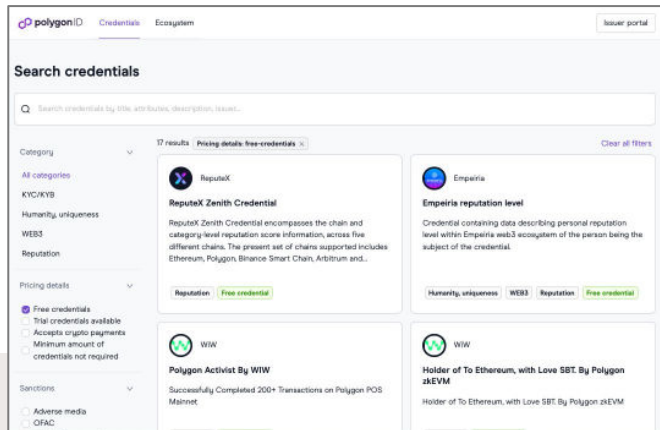
Our long term vision is to get adoption from a broad range of web3 and web2 wallets.

To that end, we have made available a [flutter based SDK](#) and a [Javascript SDK](#) for wallet providers that wish to integrate Polygon ID.

Wallet providers Integrating Polygon ID

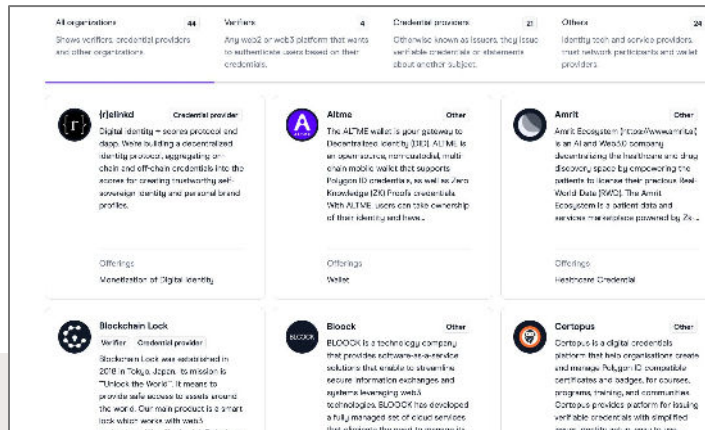


Polygon ID: Marketplace & Ecosystem



Credentials Marketplace:

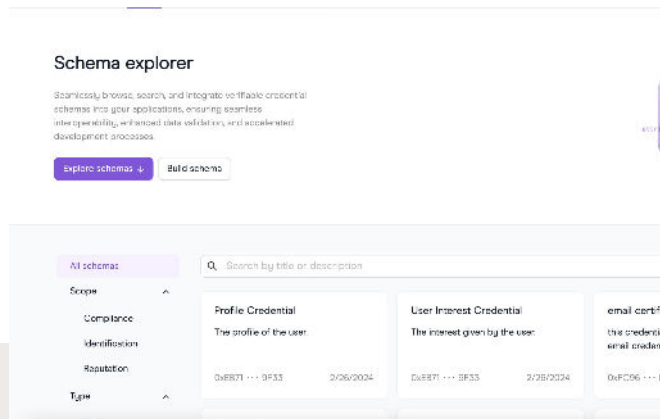
You can leverage both free and paid credentials from the [Polygon ID marketplace](#) in your use case. We have several KYC providers (Civic, Nexera ID, Netki, Synaps), as well as Gaming and Web3 Credentials (Clique, Reclaim, WIW, Reputex) among others.



Ecosystem:

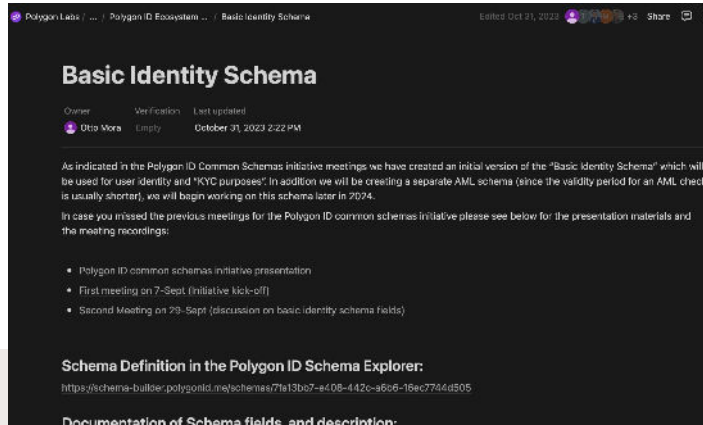
In our [ecosystem page](#) you can see all the available credentials issuers, wallet providers, systems implementers, and SaaS providers working with our technology.

Polygon ID: Credential Schema Tools



Schema Explorer and Builder

With the Schema Explorer tool you can browse JSON-LD schemas created by others. You can also use fork these schemas using our online builder tool and publish them on IPFS.



Polygon ID Common Schemas:

We launched this initiative in recognition of the need for re-usable credentials and preventing credential schema fragmentation. Our first schema launched last year under this initiative was the “[basic identity schema](#)”, which we developed with several of our KYC vendors and can be leveraged for re-usable KYC.

Who is using Polygon ID today?



[HSBC is using Polygon ID](#) for customer data portability across subsidiaries, they recently completed a POC and will be launching a product later this year.

Digishares an asset tokenization platform in Europe is [building their identity tokenization framework](#) with Polygon ID.

[Guild.xyz](#) enables online communities to manage their discord chat rooms using Polygon ID.

A major European bank recently completed a POC and will publish a report with the results of this POC. 4 other banks are building production pilots with Polygon ID including 2 in Asia, one in Europe, and one in Latin America.

Muchas Gracias!



Docs and Tutorials Hub
<https://devs.polygonid.com/>



Contact us here!

id-bd@polygon.technology



Otto Mora

Polygon ID, Americas

@ottomorac

omora@polygon.technology