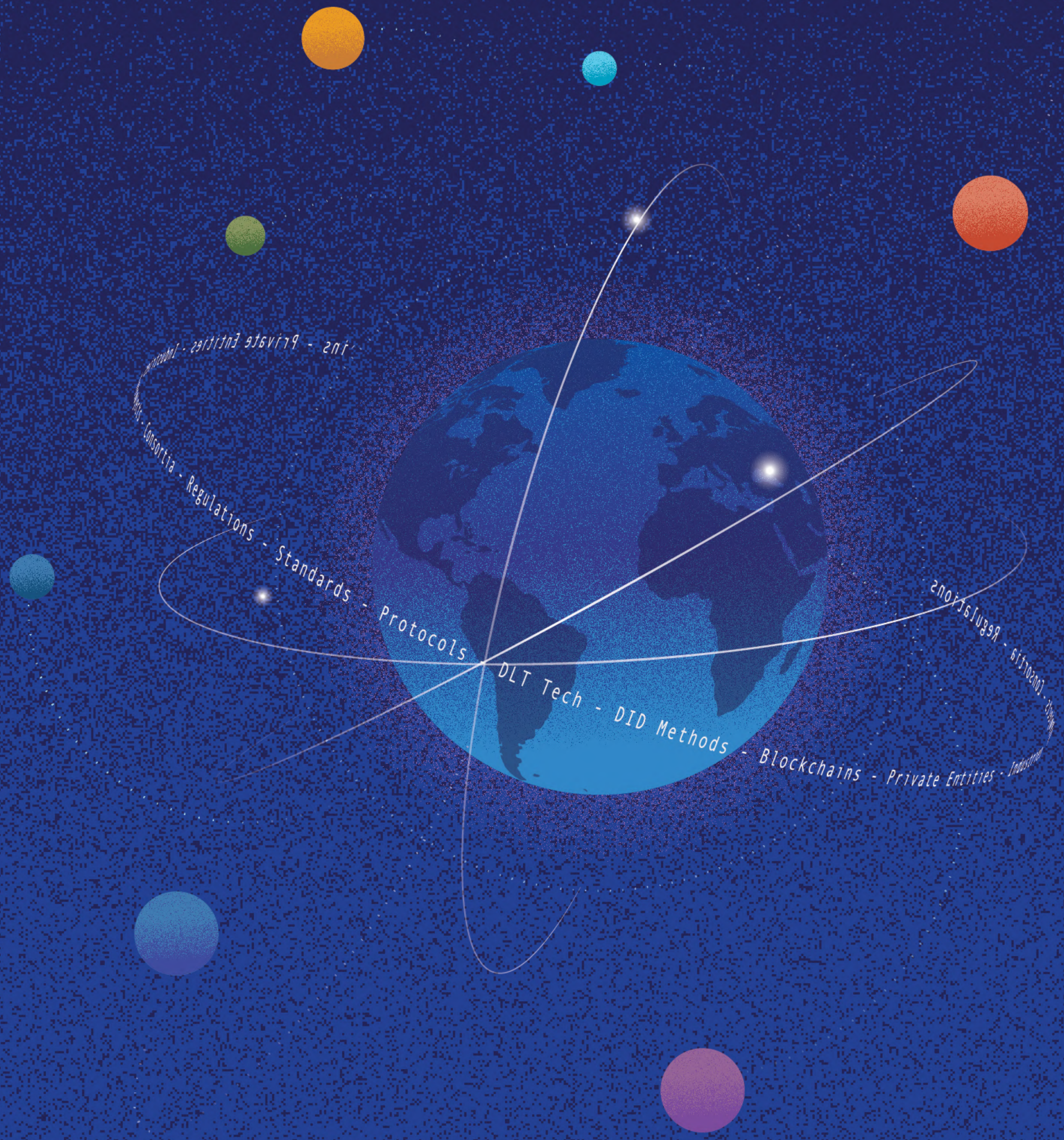
KEY STATE CAPITAL

WEB OF TRUST

SEPTEMBER 2025

WEB OF TRUST MAP

THE GLOBAL INFRASTRUCTURE OF DECENTRALIZED DIGITAL IDENTITY



ius - Private Entities - Industries
Consortia - Regulations - Standards - Protocols
DLT Tech - DID Methods - Blockchains - Private Entities - Industries
Regulations - Consortia

ID Projects - Consortia - Regulations - Standards - Protocols - DLT Tech - DID Methods - Blockchains - Private Entities - Industries

SEPTEMBER 2025

WEB OF TRUST MAP

THE GLOBAL INFRASTRUCTURE OF DECENTRALIZED DIGITAL IDENTITY

The views and opinions expressed in this report represent those of Key State Capital and do not necessarily reflect the perspectives of the individuals or organizations cited or quoted herein. The content is provided for informational purposes only and does not constitute legal, financial, or investment advice.

Lead Author: Niza González, Head of Data for the Web of Trust Map.

Co-Authors: Nicole Torres, Maria Saavedra

Editors: Ivette Cano, Nicholas Racz

Production and Design: Ivette Cano

Contact: contact@weboftrust.org

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Decentralized identity technologies have been on the rise for the past decade, yet until recently there had never been a systematic effort to map all initiatives claiming to use the technology or aligning with self-sovereign identity principles. To address this, Key State Capital initiated the Web of Trust Map research in 2022, documenting government-affiliated decentralized identity projects, consortia, collaborators, and technologies. This report, based on projects announced up to July 2023, provides an overview of the ecosystem's maturity, the dominant technologies, and the actors driving development.

Key findings show that the years 2020 and 2021 were turning points. The COVID-19 pandemic created urgent demand for contactless, secure digital credentials, leading to a wave of project announcements in 2020 and their launches in 2021. The earliest adoption occurred in education, health, and digital ID, later expanding into finance, government administration, real estate, marketing, and even creative industries. More than 40 consortia, including World Wide Web Consortium, Decentralized Identity Foundation, Linux Foundation Decentralized Trust, and Trust Over IP Foundation, are active in the space. Yet governments, particularly in Europe, North America, and Asia, remain the primary drivers of adoption through funding, regulation, and large-scale pilots.

On the verifiable data registry side, decentralized identity projects have relied on Ethereum, Sovrin, the European Blockchain Services Infrastructure Network, Polygon, and Indicio; though increasingly they are shifting toward centralized approaches such as did:web. Standards like the World Wide Web Consortium's Verifiable Credentials Data Model and Decentralized Identifiers are consistently used, while newer specifications like Open ID for Verifiable Credentials are gaining momentum. This signals a move toward more pragmatic solutions, but also a rapid shift away from the ethos of decentralized, trustless and secure infrastructures which the self-sovereign identity ecosystem focused on in the years prior.

The implications are clear: while Europe has positioned itself as the blueprint for large-scale adoption through the European Digital Identity Regulation and the forthcoming European Union Digital Identity Wallet, its example risks normalizing centralized models rather than decentralized ones. Regional disparities remain stark, with Latin America, Africa, and the Middle East lagging far behind. Private-sector business models have largely failed to materialize, leaving the ecosystem dependent on public-sector funding and regulatory mandates.

In conclusion, decentralized identity is expanding in visibility but struggling to deliver sustainable growth. The sector faces persistent challenges, lack of interoperability, uneven regional adoption, and absence of viable business models. Without renewed commitment to interoperability, innovation, and self-sovereign identity principles, the ecosystem risks consolidating into centralized, government-managed systems rather than realizing its original decentralized vision.

1. PROJECTS AND INDUSTRIES

Decentralized Identity Projects are initiatives in the Web of Trust Map that affirm the use of SSI or Decentralized Identity and have a technological deliverable available to be used by issuers, holders, and verifiers.

Projects were selected using clear criteria: they must explicitly claim to use SSI or decentralized identity principles, adopt recognized standards such as W3C DID/VC or KERI/ACDC, show at least one notable partner or user, and have a link to government or state-level activity.

30+
Industries

260+
Projects

1. PROJECTS AND INDUSTRIES

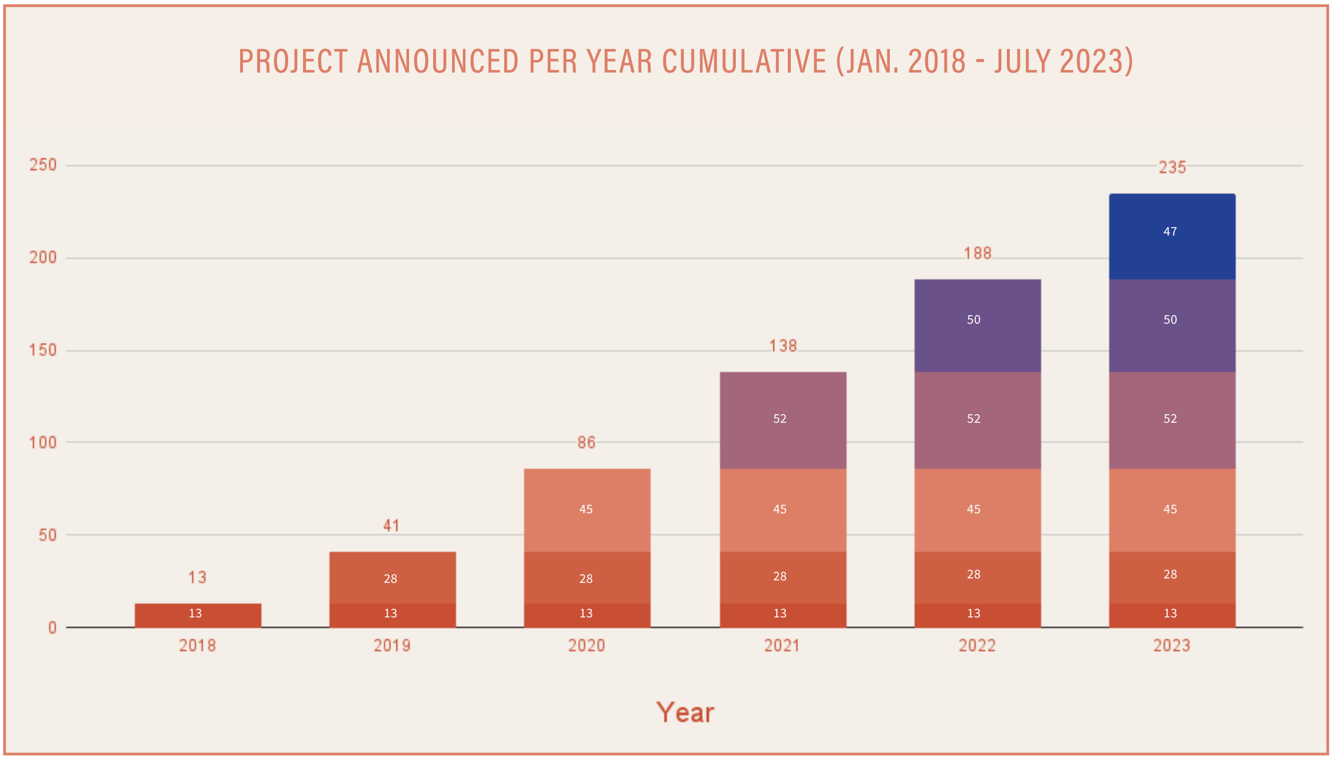
Decentralized identity has seen rapid development over the last decade, evolving from niche experimentation to more concrete applications across multiple industries. This section explores the maturity of the ecosystem through project activity and sectoral adoption. It traces the initial boom sparked by the COVID-19 pandemic, highlights key use cases that emerged in health and education, and examines how new industries have begun integrating decentralized identity technologies.

COVID-19 AS A CATALYST FOR DECENTRALIZED IDENTITY

The year 2020 experienced a significant influx of announced decentralized identity projects, totaling 45. This surge can be correlated to the COVID-19 pandemic, which led to the urgent need for contactless interactions, specifically, digital interactions. Based on this necessity, there was an acceleration in the design, development, and deployment of digital identity tools and contactless solutions. The pandemic also enabled the fast adoption of digital health certificates, such as vaccine passports or travel permits [1].

Simultaneously, governments around the world are actively pursuing their own digital identity schemes. According to the World Economic Forum, by August 2020, 165 digital or partially digital identity initiatives had been developed globally, further reflecting this widespread push towards digital solutions in response to the evolving need for contactless interactions [2].

The intense effort in developing these digital solutions and certificates for COVID-19 served as a clear example of the rapid expansion of digital identity infrastructure, explaining the increased number of project announcements aimed at meeting the demand.



Source: Web of Trust Map. See more data and insights at www.weboftrust.org

*The data presented for 2023 reflects only the period from January through July, as the research phase was concluded at that point prior to transitioning into quality control. Consequently, figures for 2023 may not be directly comparable to those of previous full years.
** A total of 34 projects did not disclose an announcement year, and several others fall outside the time range shown in the graph. These have been excluded from year-by-year comparisons.

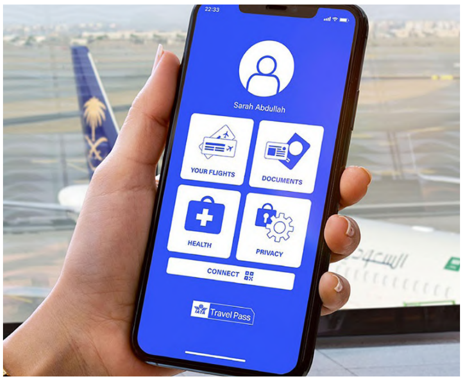
FROM ANNOUNCEMENT TO DEPLOYMENT: 2021 LAUNCHES

As institutions and developers gained a clearer understanding of the importance of secure identity and verification mechanisms, 2021 became the year when many of these announced solutions were launched or piloted. The transition from product announcements in 2020 to launches in 2021 reflects how organizations responded to an urgent need by moving quickly to develop and deploy digital identity solutions.

Several examples highlight this transition:

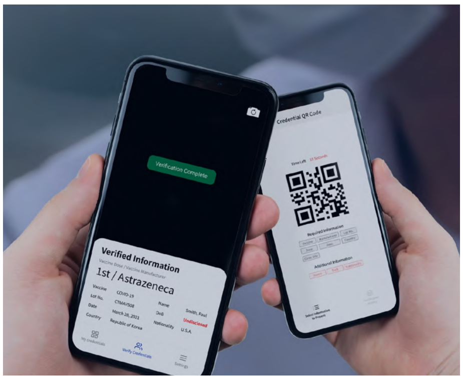
AOK PASS

Air France piloted AOK Pass, a mobile solution enabling passengers to digitize and manage their COVID-19 test results. The pilot highlighted how the airline industry sought contactless credentialing during the pandemic [3].



IATA TRAVEL PASS:

The International Air Transport Association launched the IATA Travel Pass, a mobile application developed to help travelers manage and present their verified COVID-19 test results and vaccination records. The initiative was considered due to IATA's research indicating that passengers were refusing to hand over physical documents, such as passports, phones, or boarding passes, to airport staff due to contact-related health concerns [4].



COOV

The Korean Disease Control and Prevention Agency launched COOV, a mobile app that issues COVID-19 vaccination certificates. By 2023, it was being used in 75 countries around the world [5].

These examples demonstrate how decentralized identity moved from theory to real-world deployment. While some initiatives, such as COOV, did not achieve long-term success, they marked a pivotal moment in the development of decentralized identity infrastructure. The period laid the groundwork for current and future implementations.

> *DEVON LOFFRETO, WHO ATTENDED ONLY ONE OR TWO IIWS, BUT WHOSE INFLUENCE HAS BEEN FELT EVER SINCE, SAID MOST* ***OF WHAT WE CALL IDENTITY IS "ADMINISTRATIVE," CONFERRED BY GOVERNMENT AGENCIES, EMPLOYERS, SCHOOLS, RETAILERS, AND EVERY ENTITY THAT REQUIRES US TO HAVE AN ACCOUNT.***
>
> *IN PRACTICE, MOST OF THE INDUSTRY'S WORK HAS CENTERED ON COPING WITH THIS POLY-ADMINISTRATIVE MORASS THAT IDENTITY HAS BECOME IN OUR STILL-YOUNG DIGITAL AGE. TO ME,* ***THE GREATER CHALLENGE IS MAXIMIZING PERSONAL INDEPENDENCE, SOVEREIGNTY, AND AGENCY*** *IN A DIGITAL WORLD WHERE COUNTLESS ENTITIES ARE CONSTANTLY IDENTIFYING AND CHARACTERIZING EACH OF US, OFTEN IN WAYS WORSENED BY UBIQUITOUS AND NORMALIZED SURVEILLANCE.*

DOC SEARLS, CO-FOUNDER OF COSTUMER COMMONS AND CO-ORGANIZER OF THE INTERNET IDENTITY WORSHOP

EARLY USE CASES: DIGITAL ID, HEALTH, AND EDUCATION

The earliest use cases for decentralized identity emerged in digital ID systems, with initial pilots and frameworks developed before the COVID-19 pandemic. Governments and private actors began exploring how decentralized technologies could give users more control over their identity data, improve verification processes, and enhance privacy. Initiatives like Sovrin[6] and Evernym[7] in the United States, Lissi Wallet[8] in Germany, DIDI[9] in Argentina, or Mobile ID[10] in South Korea provide an example of these types of initiatives.

However, the COVID-19 pandemic acted as a major catalyst for the adoption of decentralized identity in health and education sectors that required secure, scalable, and interoperable solutions during a global crisis. The urgent need for contactless services and cross-border credential verification rapidly accelerated the deployment of new tools.[1]

In health, projects like HPEC (a decentralized physicians' guild)[11] and BioPass (a telehealth app with decentralized medical record storage)[12] showed how decentralized identity could streamline credentialing, reduce administrative overhead, and facilitate mobility of healthcare workers.

In education, IBM Digital Credentials[13], Hyland Credentials[14], and the Digital Credentials Consortium[15] advanced the use of secure, verifiable academic credentials. These tools enabled universities to issue portable, tamper-proof diplomas and certifications, supporting both academic integrity and digital access.

These early implementations illustrated the practical value of decentralized identity, setting the stage for its expansion into other industries.

EXPANDING USE CASES ACROSS INDUSTRIES

Following initial digital ID, health and education use cases, new sectors began experimenting with decentralized identity technologies:

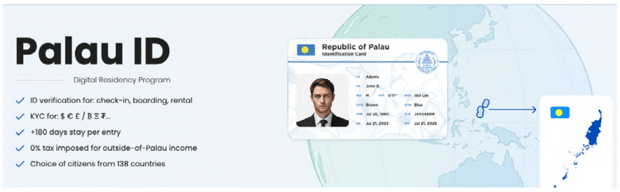
FINANCE

Decentralized identity is increasingly being applied to address fraud, data breaches, and regulatory compliance in finance. Platforms like Parameta's MyID [16] and ConnectID [17] offer verifiable credentials that support Know Your Customer (KYC) requirements while improving user experience.

Survey and advertize at the same time,
Quiz-type Ads
Quiz-type Ads is a reward-based advertisement that promotes advertisers' products by attracting user participation through surveys.
Get the Ads service detail

MARKETING

Projects like THEPOL[18] in South Korea use blockchain and decentralized identity to facilitate transparent advertising and survey mechanisms, introducing new models for audience engagement and data ownership.


Palau ID
Digital Residency Program
✓ ID verification for: check-in, boarding, rental
✓ KYC for: $ € £ / ₿ Ξ ₮...
✓ +180 days stay per entry
✓ 0% tax imposed for outside-of-Palau income
✓ Choice of citizens from 138 countries
Republic of Palau
Identification Card
Adams
John B.
M
5'11"
160 Lbs
Brown
Blue
Jul 26, 1990
JXP2489M
Jul 21, 2023
Jul 21, 2028

GOVERNMENT

Governments across various regions are incorporating decentralized identity into their public service delivery. Bhutan[19], Singapore [20], and Palau[21] have introduced citizen identity wallets or national decentralized identity systems. Local governments in Seoul[22], Buenos Aires[23], and New South Wales[24] are also leading the way.

AUTOMOTIVE

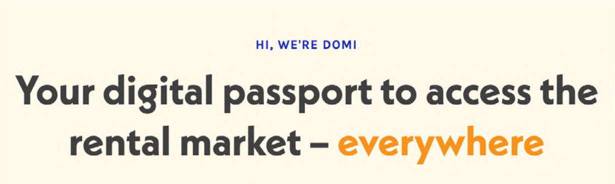
The Mobility Open Blockchain Initiative (MOBI) [25] and projects like Mobix [26] and Cardossier [27] apply decentralized identity to vehicle identity management, sustainable transportation, and digital mobility services.

> ONE REAL SIGN OF PROGRESS IN DECENTRALIZED IDENTITY IS THAT MORE PEOPLE ARE FIRST ASKING WHAT PROBLEMS ARE WE SOLVING—BEFORE JUMPING INTO DISCUSSIONS ABOUT STANDARDS. THIS SHIFT **FROM TECHNOLOGY-DRIVEN TO PROBLEM-DRIVEN THINKING** SHOWS THE SPACE IS MATURING. TECHNOLOGY SHOULD ALWAYS BE A MEANS, NOT THE GOAL.
> IT'S ENCOURAGING TO SEE NEW DECENTRALIZED IDENTITY PROJECTS EMERGE, BUT MY GOLDEN RULE REMAINS: **THE VALUE LIES IN WHETHER THEY SOLVE A MEANINGFUL PROBLEM.**

LUCY YANG, INDEPENDENT ADVISOR

> FROM OUR ADVISORY WORK ACROSS SECTORS, TWO KEY DEVELOPMENTS STAND OUT. FIRST, GOVERNMENTS ARE RAPIDLY **ISSUING DIGITAL IDENTITY CREDENTIALS TO PEOPLE**, ANSWERING THE CRITICAL 'WHO GOES FIRST?' QUESTION AND GIVING ORGANIZATIONS A CLEAR AND OFTEN MANDATED STARTING POINT.
>
> SECOND, AI IS SHATTERING THE FRAGILE DIGITAL TRUST STATUS QUO. WE STRUGGLED WITH FRAUD BEFORE AI; NOW WE FACE CEO-LEVEL EXISTENTIAL CRISES. **DIGITAL TRUST POWERED BY DECENTRALIZED IDENTITY IS NO LONGER OPTIONAL; IT'S CRITICAL.**

NICK RIS, CO-FOUNDER OF MISSION, A VENTURES CONSULTANCY FOCUSED ON DIGITAL TRUST.



HI, WE'RE DOMI

Your digital passport to access the rental market – everywhere

REAL ESTATE

Domi[28] uses verifiable credentials to streamline rental applications and tenant screening, helping landlords and tenants establish trust without paperwork.

Auracles

Introducing the missing digital foundation layer for music. A verified digital ID with an information and permissions source for music makers, services, and representatives. Founded by Imogen Heap.

CREATIVE INDUSTRIES

The Creative Passport (now Auracles)[29] provides digital identity containers for music professionals, allowing them to manage and share verified data such as works, credits, and affiliations.

cheqd

Infrastructure for Trusted Data markets

VERIFIABLE AI

Cheqd[30], Indicio Proven[31], and Privado ID[32] are pioneering projects bringing decentralized identity principles into the field of agentic AI. By embedding verifiable credentials and decentralized identifiers, these solutions enable AI agents to prove the origin, authenticity, and integrity of their actions or outputs.

ORGANIZATIONAL IDENTITY

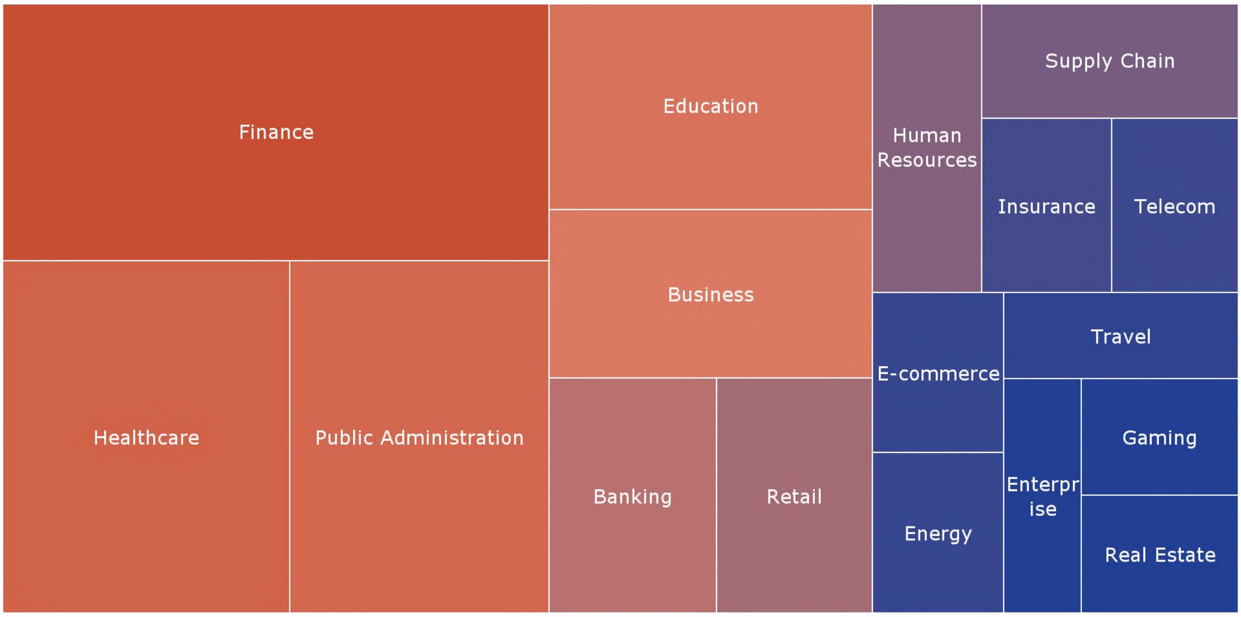
The Global Legal Entity Identifier Foundation (GLEIF) extended the global LEI system into decentralized identity by creating the verifiable Legal Entity Identifier (vLEI), built on Key Event Receipt Infrastructure (KERI) [33, 34, 35, 36, 37]. vLEIs enable verifiable authority for organizations and representatives. The vLEI is a notable outlier due to its adoption of a completely separate stack than the majority in the space.

OVERALL INDUSTRY MATURITY

While decentralized identity has expanded into multiple sectors, the maturity of adoption varies widely. Industries like health, education, finance, and government have shown more robust development due to strong demand for privacy, interoperability, and regulatory compliance. Meanwhile, sectors such as marketing, the creative industries, and real estate are still exploring their potential applications.

The progress made since 2020 reflects growing interest and experimentation, yet challenges remain, particularly around interoperability, governance, and usability. Continued investment and real-world testing will determine which sectors achieve lasting impact and which remain in pilot stages.

INDUSTRIES



Source: Web of Trust Map. See more data and insights at www.weboftrust.org

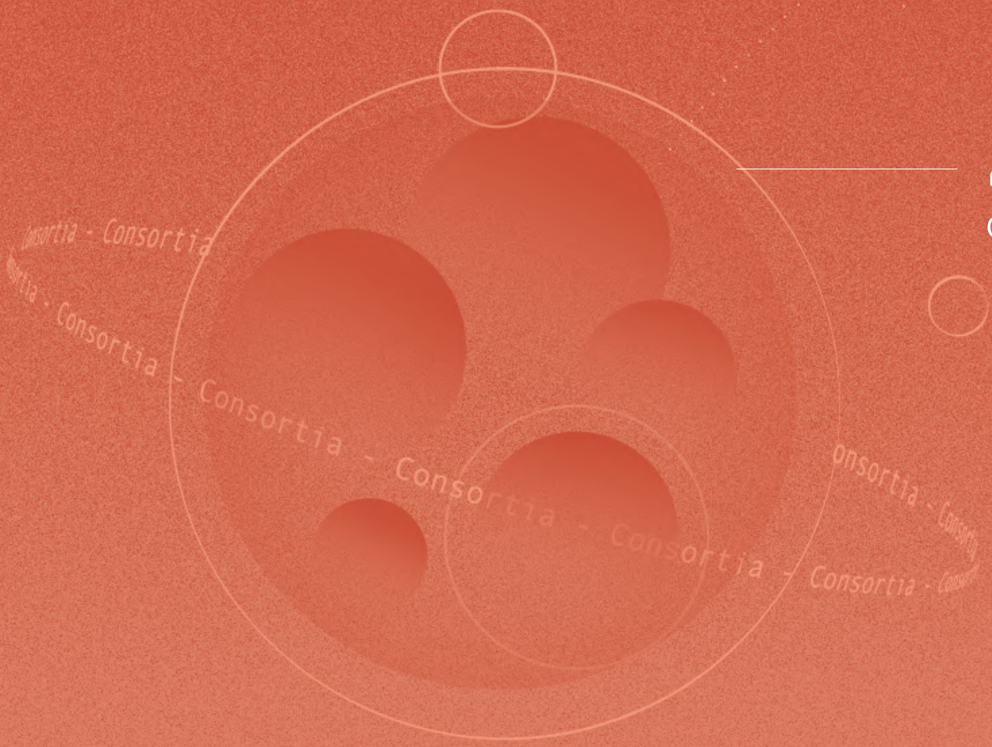
> *DECENTRALIZED IDENTITY HAS ALWAYS BEEN ABOUT MORE THAN TECHNOLOGY. IT'S ABOUT* ***RETHINKING HOW PEOPLE EXERCISE AGENCY AND FREEDOM IN A DIGITAL WORLD.*** *WHAT I FIND REMARKABLE, ESPECIALLY IN SPACES LIKE THE INTERNET IDENTITY WORKSHOP, IS HOW THE COMMUNITY CONTINUES TO PUSH THE BOUNDARIES OF WHAT'S POSSIBLE WHILE GRAPPLING WITH THE HARD QUESTIONS OF AGENCY, PRIVACY, INTEROPERABILITY, GOVERNANCE, AND TRUST.*
>
> *AS THE INDUSTRY MATURES, THE REAL CHALLENGE IS ENSURING THESE SYSTEMS WORK TOGETHER IN WAYS THAT SERVE PEOPLE FIRST AND CREATE LASTING REAL-WORLD VALUE.*

PHIL WINDLEY, FOUNDER AND ORGANIZER OF INTERNET IDENTITY WORKSHOP

2. CONSORTIA AND COLLABORATION

Consortia are associations of public or private entities featured in the Web of Trust Map that promote, use in notable ways, or maintain Self-Sovereign Identity (SSI) principles and technologies.

In more detail, they are groups that contribute significantly to advancing SSI through working groups, standards development, or other forms of industry leadership, and were selected based on notable participation, significant influence, or relevance to the SSI landscape.


Consortia - Consortia - Consortia - Consortia - Consortia - Consortia - Consortia - Consortia

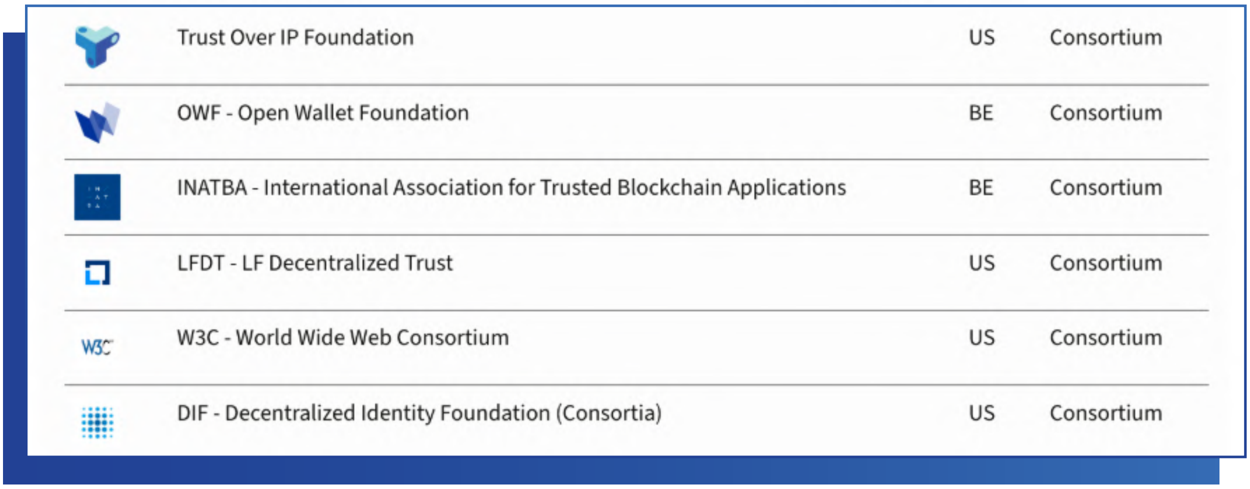
40+
Consortia

2. CONSORTIA AND COLLABORATION

Established in 2016, the Sovrin Foundation is recognized as the first consortium dedicated entirely to self-sovereign identity (SSI). As the governing body of the Sovrin Network, a public-permissioned blockchain tailored for decentralized identity, it laid the groundwork for what SSI governance could look like.

Following Sovrin's creation, dozens of consortia were either established worldwide or became involved. Such is the case of the World Wide Web Consortium (W3C), which, though established in 1994, began contributing to decentralized identity around 2016 with the proposal and subsequent launch of its Verifiable Claims - now Verifiable Credentials - Working Group.[38]

Consortia are actively developing in countries like Belgium, Switzerland, New Zealand, Germany, Canada, and South Korea, contributing to the decentralized identity ecosystem. However, the United States plays the leading role in this space. It serves as home to some of the most active and influential consortia including Trust Over IP (ToIP) Foundation and Decentralized Identity Foundation (DIF).



Trust Over IP Foundation	US	Consortium
OWF - Open Wallet Foundation	BE	Consortium
INATBA - International Association for Trusted Blockchain Applications	BE	Consortium
LFDT - LF Decentralized Trust	US	Consortium
W3C - World Wide Web Consortium	US	Consortium
DIF - Decentralized Identity Foundation (Consortia)	US	Consortium

Source: Web of Trust Map. See more data and insights at www.weboftrust.org

Consortia's strategic contributions in advancing decentralized identity include:

- **Standards Development:** Consortia play a central role in proposing, developing, maintaining and aligning open, interoperable technical standards. This work is primarily carried out through working groups.
- **Cross-Sector Collaboration:** Consortia bring together public and private sectors, regulators, and academia, fostering ecosystem alignment and enabling global adoption.
- **Defining trust and governance:** Decentralized identity relies not only on technology itself, but also on trust. Consortia define governance frameworks to regulate identity ecosystems, build accountability mechanisms and transparent governance models.
- Serve as a **neutral home for the collaborative development of decentralized technologies** and implementations, incubate new projects, and support network deployments.

CORE ECOSYSTEM DRIVERS

Although forty three consortia were researched and included in the Web of Trust Map, six stand out as key strategic initiatives due to their global footprint, broad connections, management of technical standards, and extensive memberships. These six consortia play a critical role in shaping the decentralized identity ecosystem, ranging from developing open-source components and enhancing interoperability to fostering collaboration across organizations.

WORLD WIDE WEB CONSORTIUM

LAUNCH: 1994
HQ: United States
MANAGING ENTITY:
World Wide Web Consortium, Inc.

OVERVIEW

The W3C[39] is the primary international standards organization for the World Wide Web. As a member-driven organization, it develops open standards and guidelines based on accessibility, internationalization, privacy, and security.

W3C brings together a diverse set of stakeholders. Notable public sector members include National Institute of Standards and Technology, the U.S. Department of Homeland Security (DHS), and Singapore's Government Technology Agency; while private sector members include Apple, Amazon, Mastercard, Danube Tech, and the Affinidi Trust Network.

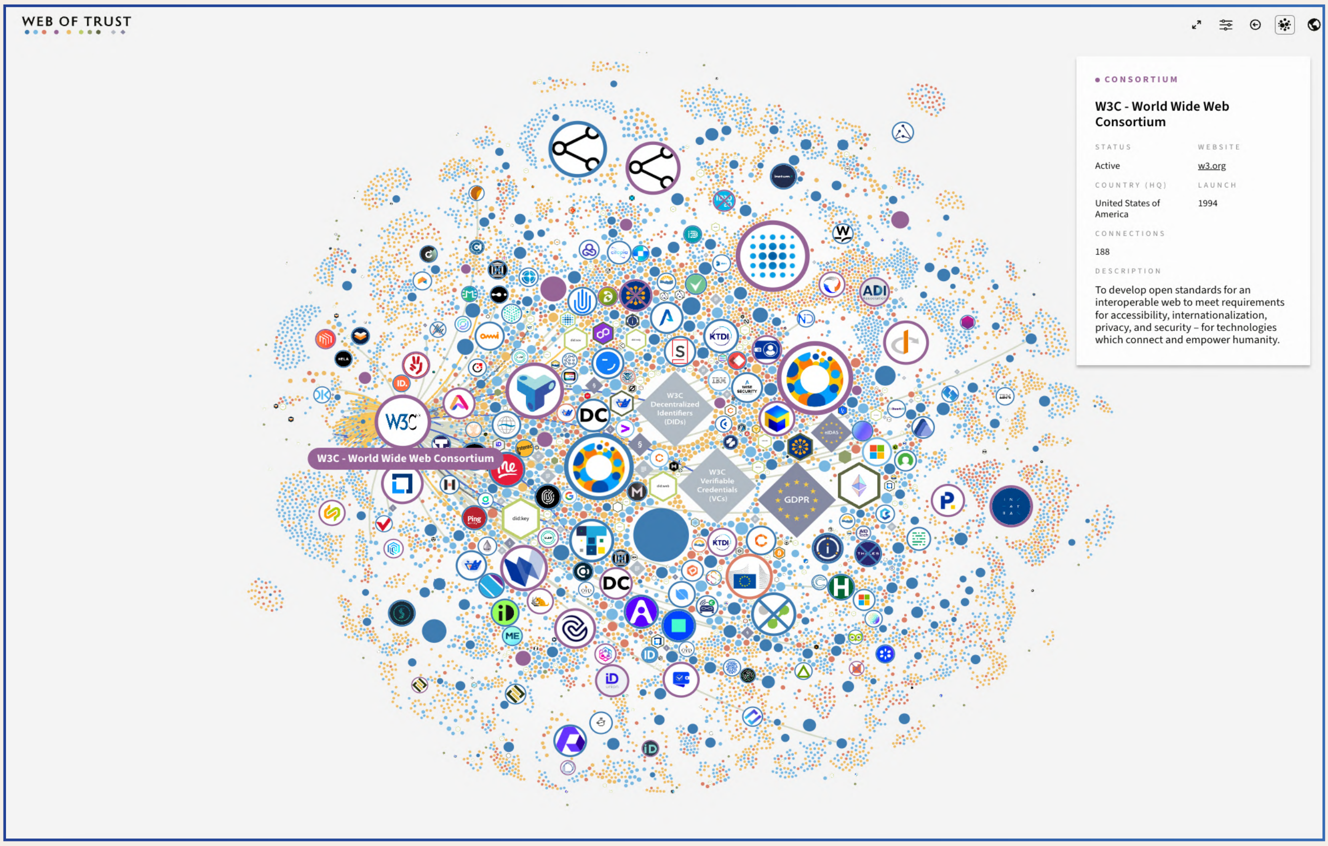
TECHNICAL & STRATEGIC HIGHLIGHTS

The organization has played a crucial role in establishing foundational digital identity standards, including Decentralized Identifiers (DID) and the Verifiable Credentials (VC) Data Model. Their widespread adoption is evident, with 172 project connections referencing DID and 205 referencing VC in the Web of Trust Map.

W3C's technical work is conducted through working groups. Key technical working groups featured in the Web of Trust Map include:

- VC Working Group - Maintains the VC Data Model specification.
- DID Working Group - Maintains the DID specification.
- Credentials Community Working Group - Focused on VC, it drafts and incubates internet specifications, prototypes, and tests implementations.
- Web Authentication Working Group - Develops the WebAuthn API for strong authentication.

WORLD WIDE WEB CONSORTIUM


WEB OF TRUST
W3C - World Wide Web Consortium
W3C Decentralized Identifiers (DIDs)
W3C Verifiable Credentials (VCs)
GDPR
did:key

● CONSORTIUM

W3C - World Wide Web Consortium

STATUS	WEBSITE
Active	w3.org

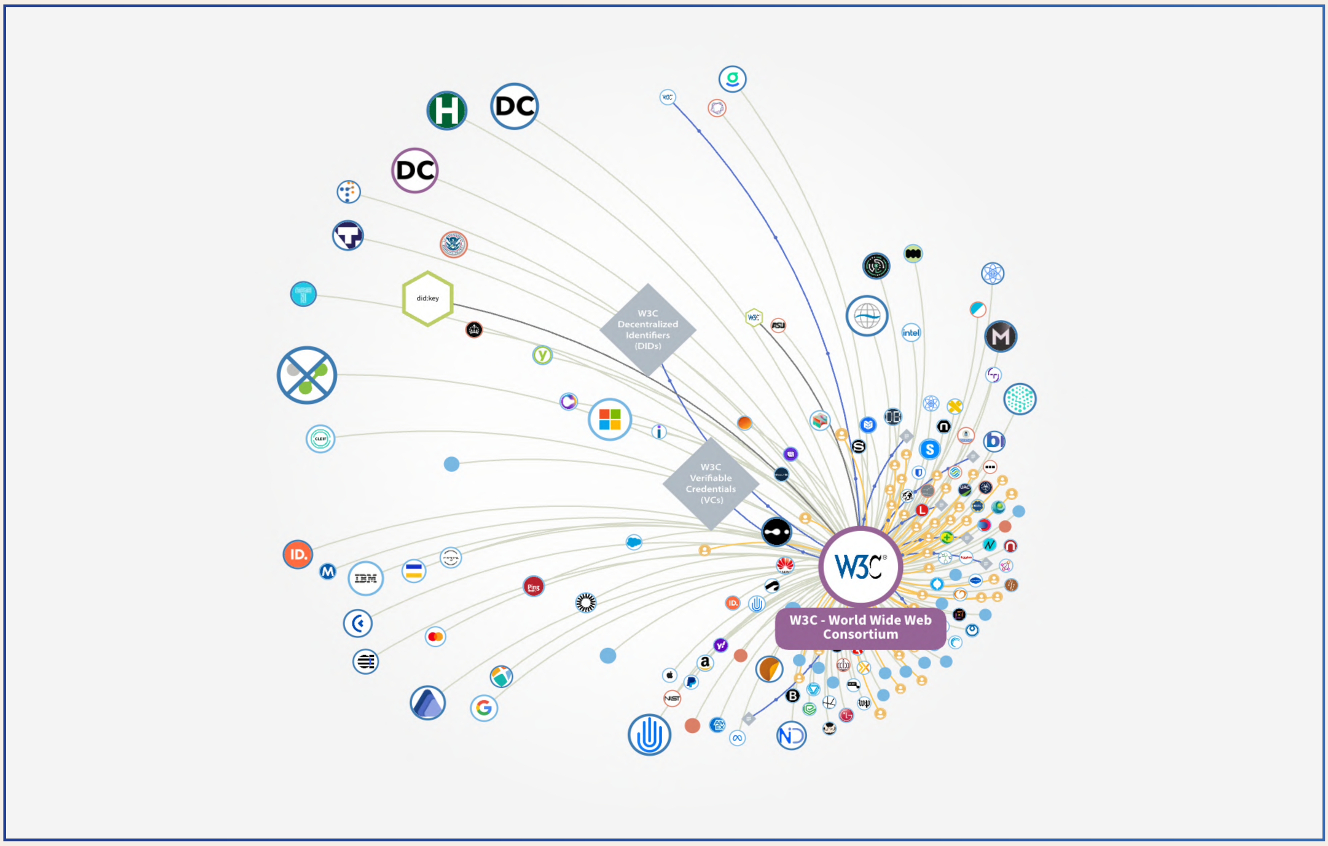
COUNTRY (HQ)	LAUNCH
United States of America	1994

CONNECTIONS

188

DESCRIPTION

To develop open standards for an interoperable web to meet requirements for accessibility, internationalization, privacy, and security – for technologies which connect and empower humanity.


W3C Decentralized Identifiers (DIDs)
W3C Verifiable Credentials (VCs)
did:key
W3C - World Wide Web Consortium

[See the full view on Web of Trust Map]

DECENTRALIZED IDENTITY FOUNDATION

DIF

LAUNCH: 2017
HQ: United States
MANAGING ENTITY: Joint Development Foundations Projects, LLC

OVERVIEW

DIF[40] is dedicated to developing open-source components and standards that support decentralized identity ecosystems. DIF serves as an important enabler in the advancement of SSI. Its work includes developing technical specifications, reference implementations, and promoting industry coordination efforts.

This consortium maintains government relations with Singapore, Canada, and Ethiopia. Its private sector members include notable participants from the ecosystem such as MATTR and SpruceID.

Technical & Strategic Highlights

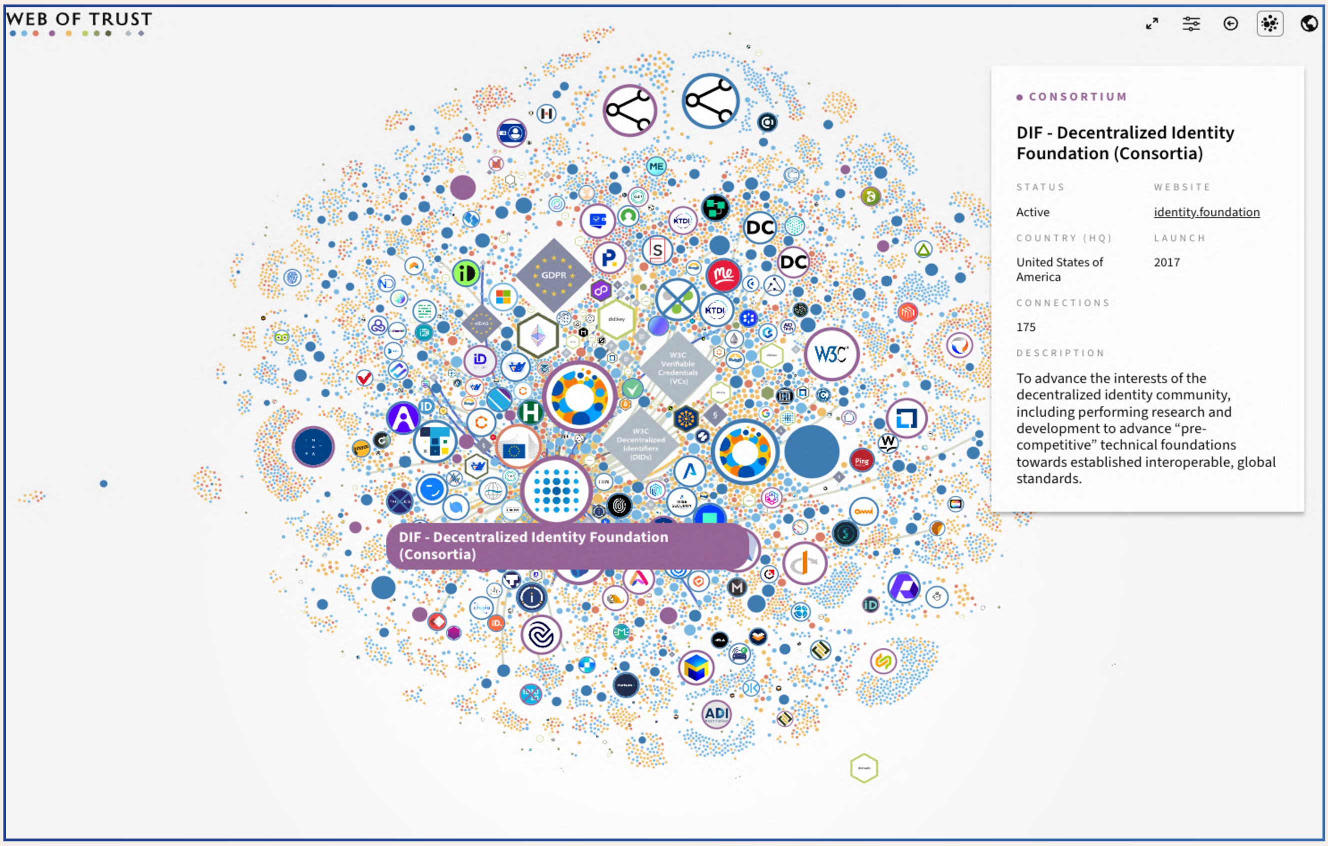
The organization leads technical collaboration on decentralized identity through working groups that develop key standards and protocols, such as DIDComm, Sidetree, and the Decentralized Web Node. DIF manages the largest number of identity-related standards/protocols (15) represented in the Web of Trust Map, highlighting its central role in the ecosystem.

Its working groups (e.g., DID Methods, DIDComm, Identifiers and Discovery, Claims and Credentials) focus on foundational components of decentralized identity, including identifiers, secure messaging, and verifiable credentials. Its Labs initiative supports the early-stage development testing, and interoperability assessment of emerging tools and frameworks, while its special interest groups drive regional coordination and industry-specific adoption.

> *THE WEB OF TRUST MAP PROVIDES MEASURABLE EVIDENCE OF DECENTRALIZED IDENTITY'S GROWTH, SHOWING HUNDREDS OF PROJECTS CONVERGING AROUND SHARED STANDARDS AND PRINCIPLES.*
>
> *AT DIF, **WE'RE EXCITED TO SEE THIS MOMENTUM EXTEND INTO TRUSTED AI AGENTS, TRAVEL EXPERIENCES, AND AUTHENTIC DIGITAL CONTENT.** THE MAP HIGHLIGHTS THE SCALE AND DIVERSITY OF WORK UNDERWAY WHILE HELPING US NAVIGATE, COORDINATE, AND BUILD TOGETHER.*

KIM HAMILTON DUFFY
EXECUTIVE DIRECTOR OF DECENTRALIZED IDENTITY FOUNDATION

DECENTRALIZED IDENTITY FOUNDATION


WEB OF TRUST
GDPR
W3C Verifiable Credentials (VCs)
W3C Decentralized Identifiers (DIDs)
DIF - Decentralized Identity Foundation (Consortia)

● CONSORTIUM

DIF - Decentralized Identity Foundation (Consortia)

STATUS: Active

WEBSITE: identity.foundation

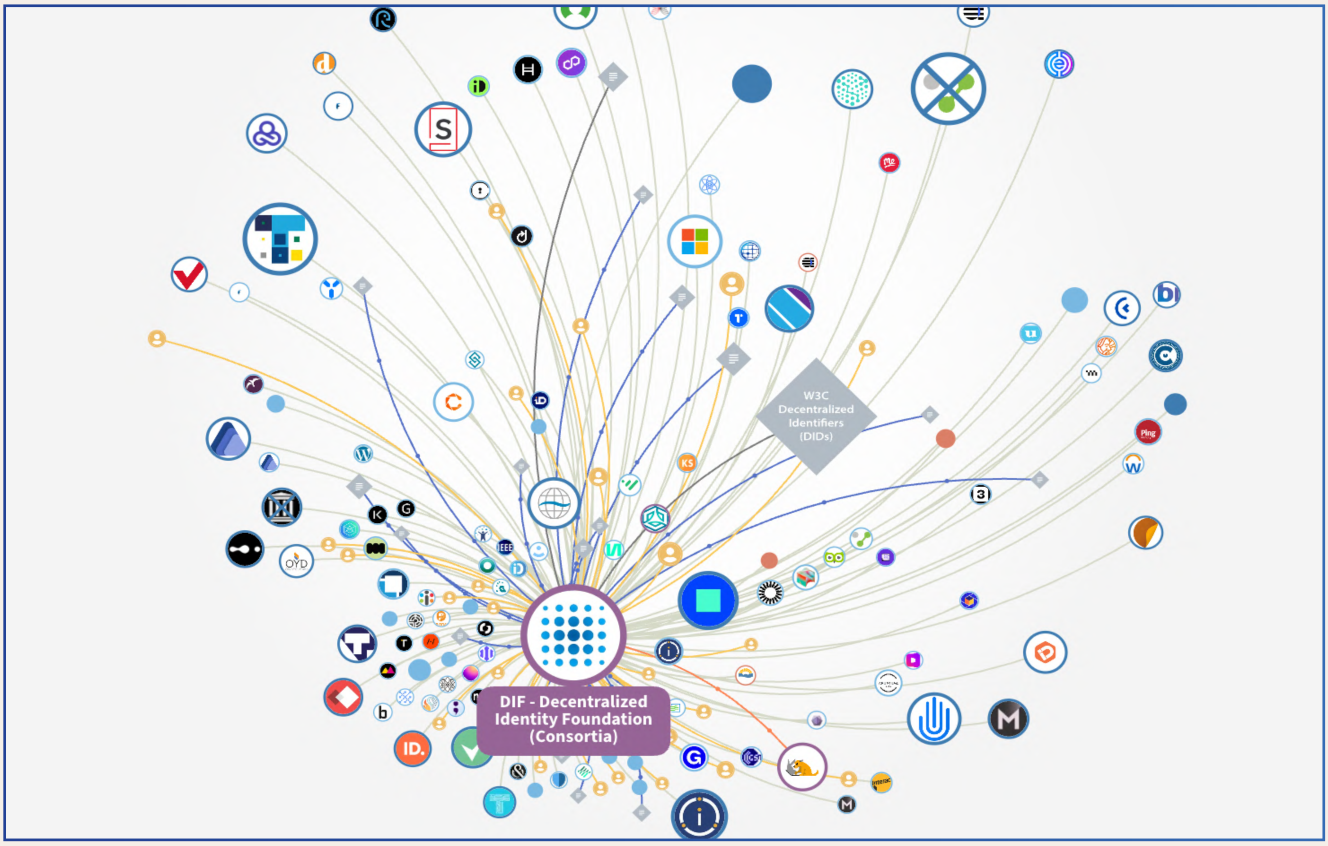
COUNTRY (HQ): United States of America

LAUNCH: 2017

CONNECTIONS: 175

DESCRIPTION

To advance the interests of the decentralized identity community, including performing research and development to advance "pre-competitive" technical foundations towards established interoperable, global standards.


W3C Decentralized Identifiers (DIDs)
DIF - Decentralized Identity Foundation (Consortia)

See the full view on Web of Trust Map

LF DECENTRALIZED TRUST

LF DECENTRALIZED TRUST

LAUNCH: 2024
HQ: United States
MANAGING ENTITY:
Linux Foundation

OVERVIEW

Linux Foundation Decentralized Trust (LFDT)[41], a recently launched initiative of the Linux Foundation, provides a neutral, open-source home for the collaborative development of decentralized technologies.

Its membership includes Brazil's public sector entity Serviço Federal de Processamento de Dados (SERPRO), along with major private sector players such as Chainlink, Deutsche Telekom, Deloitte, and Huawei Technologies.

TECHNICAL & STRATEGIC HIGHLIGHTS

LFDT advances decentralized identity by managing and developing projects across its ecosystem and providing its Labs for developers as a more accessible alternative to experiment and contribute new ideas. The foundation hosts and supports leading initiatives, including the entire Hyperledger ecosystem and ToIP, while overseeing the development and maintenance of core standards and protocols such as the AnonCreds Specification, the Indy DID Method, and the Aries protocol.

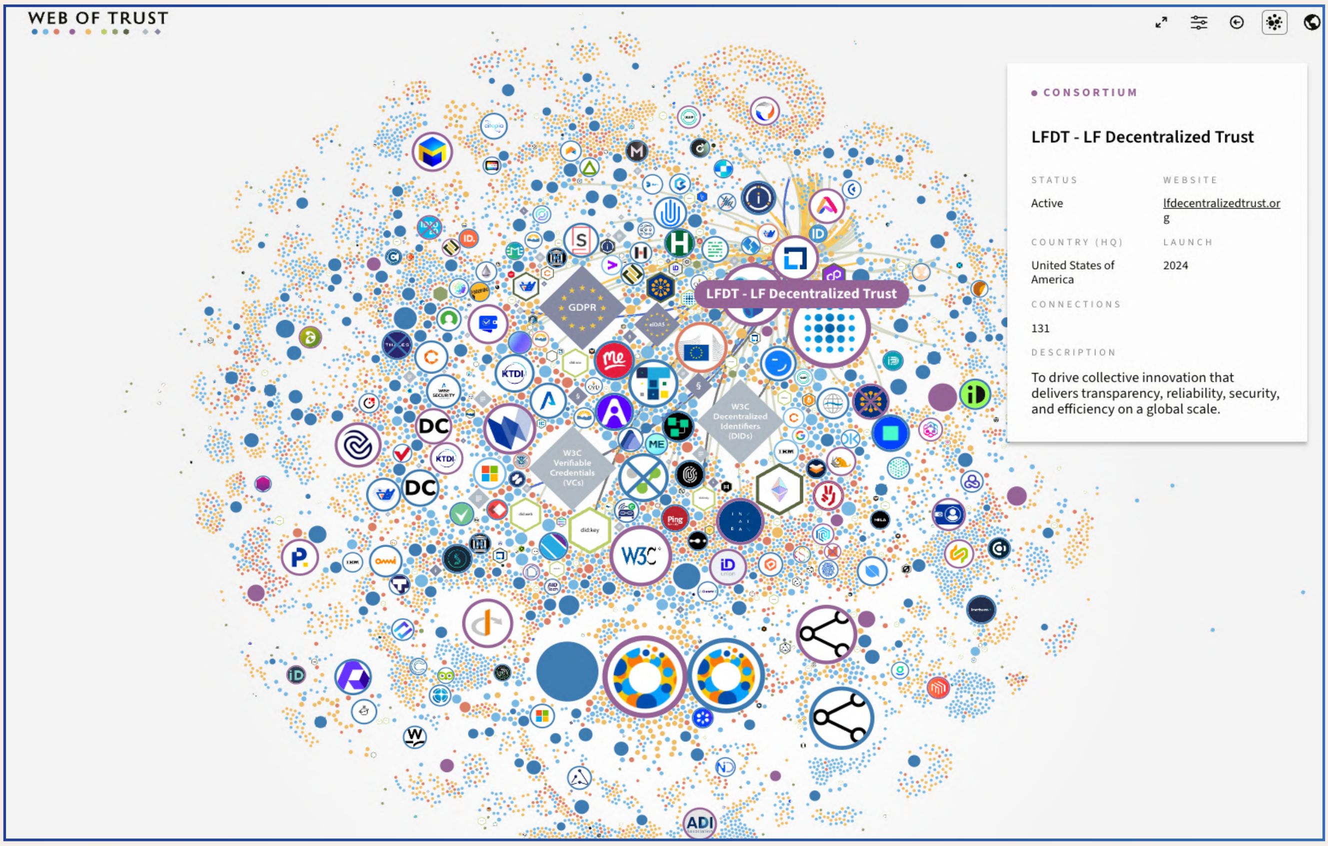
Decentralized identity projects within its scope include:

- Hyperledger AnonCreds, a privacy-preserving verifiable credential format.
- Hyperledger Indy, a suite of tools and libraries for building decentralized identity systems.
- CREDEBL, an open-source platform for managing decentralized identity and verifiable credentials.

> *DECENTRALIZED IDENTITY IS ACHIEVED THROUGH DISTRIBUTED TRUST BASED ON PORTABLE, PROVABLE, AND PROTECTED CREDENTIALS.*
>
> *THE LF DECENTRALIZED TRUST ECOSYSTEM IS TACKLING THIS ON BOTH THE CODE AND STANDARDS FRONTS. OUR COMMUNITY'S WORK IS FUELED BY THE NEED FOR TRUST LAYERS IN GOVERNMENT, FINANCE, TRADE, TRAVEL, AND MORE, INCLUDING A GROWING URGENCY FOR NEW BREEDS OF AUTHENTICATION IN THE AGE OF AI.*

DANIELA BARBOSA, GENERAL MANAGER OF DECENTRALIZED TECHNOLOGIES AT THE LINUX FOUNDATION AND EXECUTIVE DIRECTOR OF LF DECENTRALIZED TRUST

LF DECENTRALIZED TRUST


WEB OF TRUST
GDPR
W3C Decentralized Identifiers (DIDs)
W3C Verifiable Credentials (VCs)
did:key
LFDT - LF Decentralized Trust

● CONSORTIUM

LFDT - LF Decentralized Trust

STATUS
Active

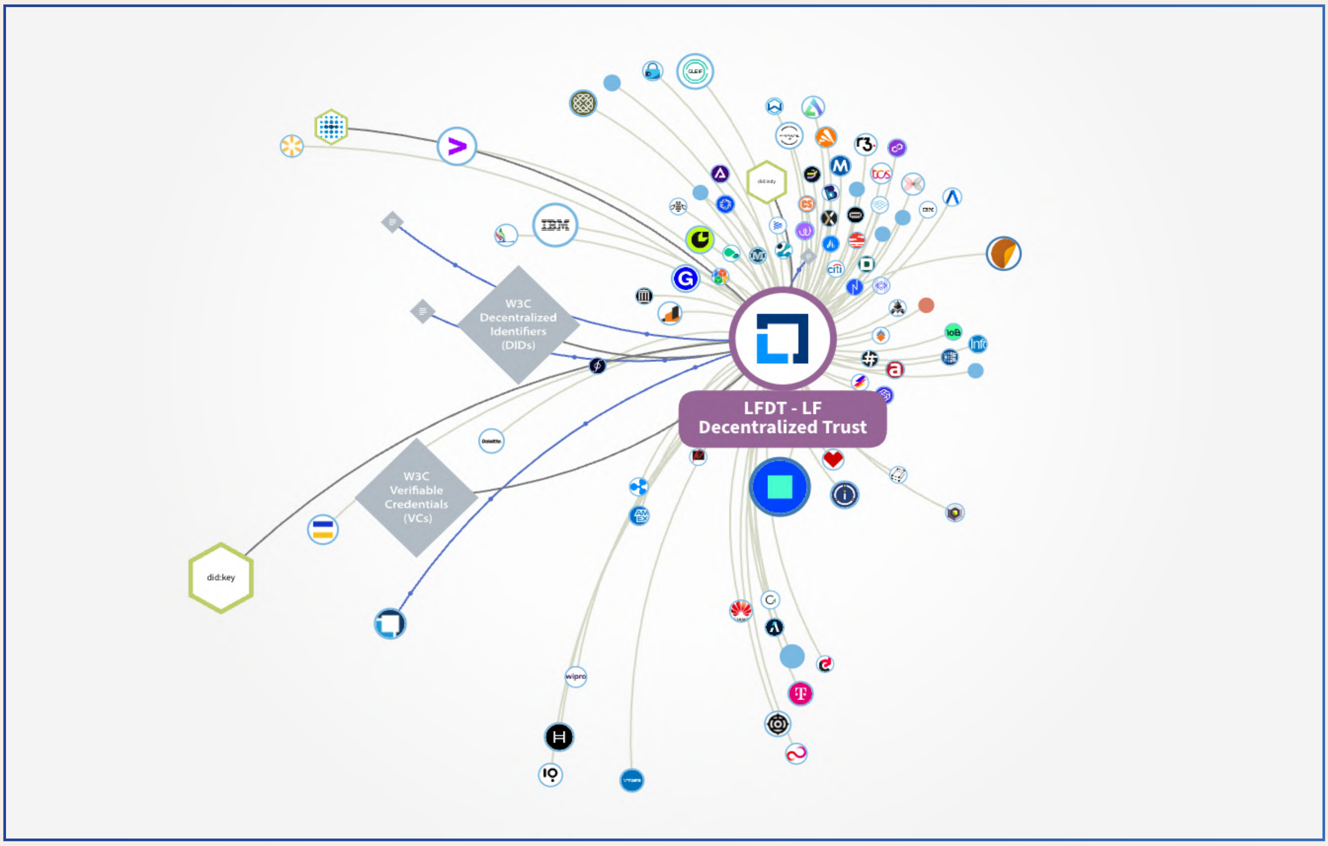
WEBSITE
lfdecentralizedtrust.org

COUNTRY (HQ)
United States of America

LAUNCH
2024

CONNECTIONS
131

DESCRIPTION
To drive collective innovation that delivers transparency, reliability, security, and efficiency on a global scale.


LFDT - LF Decentralized Trust
W3C Decentralized Identifiers (DIDs)
W3C Verifiable Credentials (VCs)
did:key
IBM

See the full view on Web of Trust Map

OPEN WALLET FOUNDATION

OpenWallet FOUNDATION

LAUNCH: 2023
HQ: Belgium
MANAGING ENTITY:
Linux Foundation Europe

OVERVIEW

The Open Wallet Foundation (OWF)[42] was launched to develop open-source software components for digital wallet technology. Members from the public sector include Swisscom Ltd, the World Bank Group, the Government of the Autonomous City of Buenos Aires, Bhutan's Government Technology Agency, and Mexico's Secretary of Innovation and Open Government. Other notable members from the private sector include Accenture, Google, Gen, Visa, and the Digital Identity and Data Sovereignty Association (DIDAS).

TECHNICAL & STRATEGIC HIGHLIGHTS

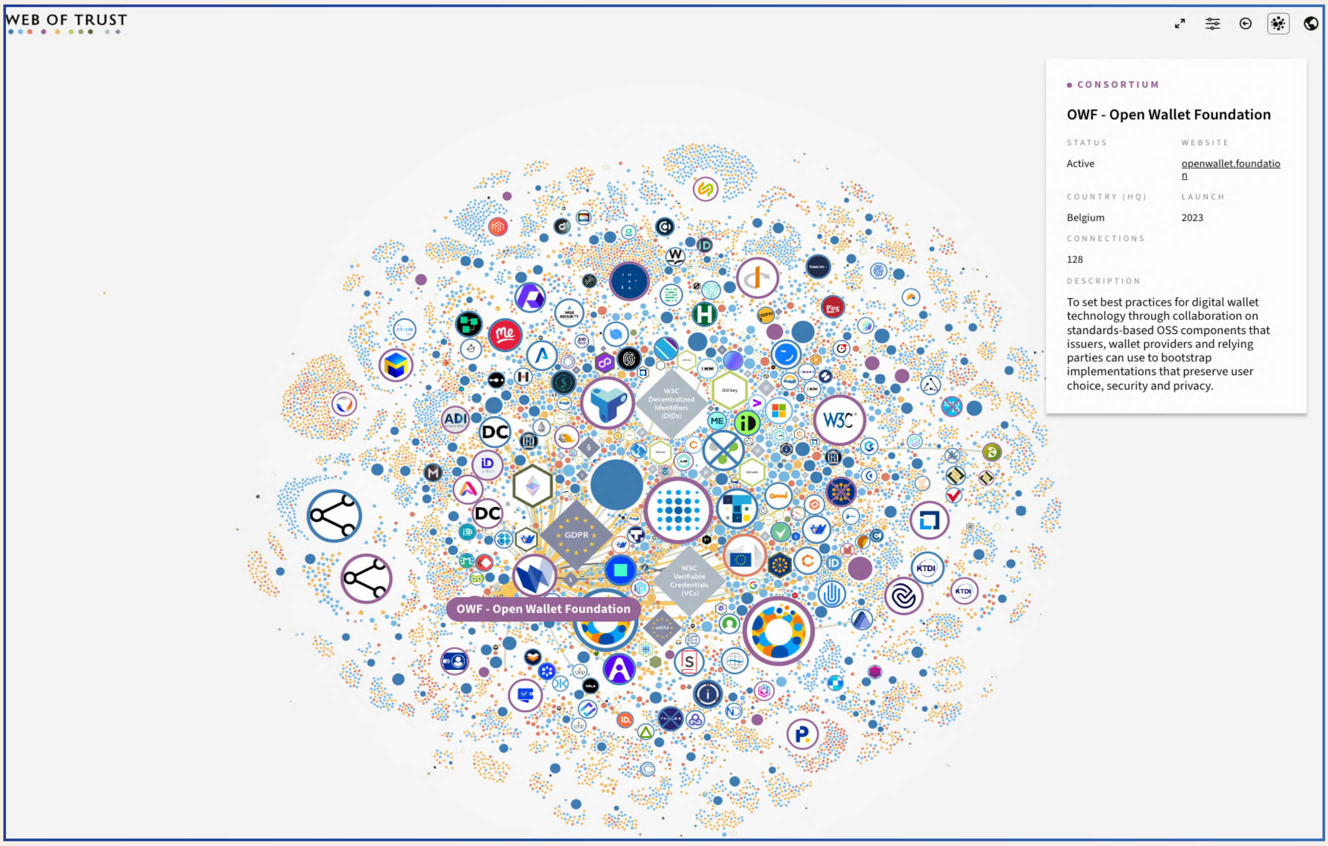
The OWF serves as a neutral hub for open-source projects aimed at building interoperable digital wallets. Its portfolio includes initiatives at both the Growth and Labs stages, with notable projects such as Credo (formerly Hyperledger Aries Framework Javascript), a framework for SSI solutions. OWF's technical priorities center on supporting W3C VC and other key identity standards, with a strong emphasis on interoperability across wallet solutions. To advance this mission, the foundation actively collaborates with consortia such as ToIP, DIF, and the OpenID Foundation.

OWF also hosts and coordinates events such as the Global Digital Collaboration, first held in Geneva on July 1-2, 2025. The inaugural event brought together more than a thousand participants from both the public and private sectors, featuring dozens of discussions and presentations.

> *WE WERE ONE OF 50 ORGANIZERS OF THE GLOBAL DIGITAL COLLABORATION, INCLUDING MANY OF THE MOST IMPORTANT INTERGOVERNMENTAL, STANDARDS, AND OPEN SOURCE ORGANIZATIONS.*
>
> *I HOPE IT [GLOBAL DIGITAL COLLABORATION] BECOMES THE BEST PLACE FOR ALL OF US TO COME TOGETHER, **LEARN FROM EACH OTHER, IDENTIFY GAPS AND OVERLAPS IN OUR INITIATIVES, AND BETTER COORDINATE STANDARDS, CODE, AND POLICY.***

DANIEL GOLDSCHEIDER, FOUNDER AND EXECUTIVE DIRECTOR OF OPENWALLET FOUNDATION.

OPEN WALLET FOUNDATION


WEB OF TRUST
W3C Decentralized Identifiers (DIDs)
GDPR
W3C Verifiable Credentials (VCs)
OWF - Open Wallet Foundation
W3C
KTDI

● CONSORTIUM

OWF - Open Wallet Foundation

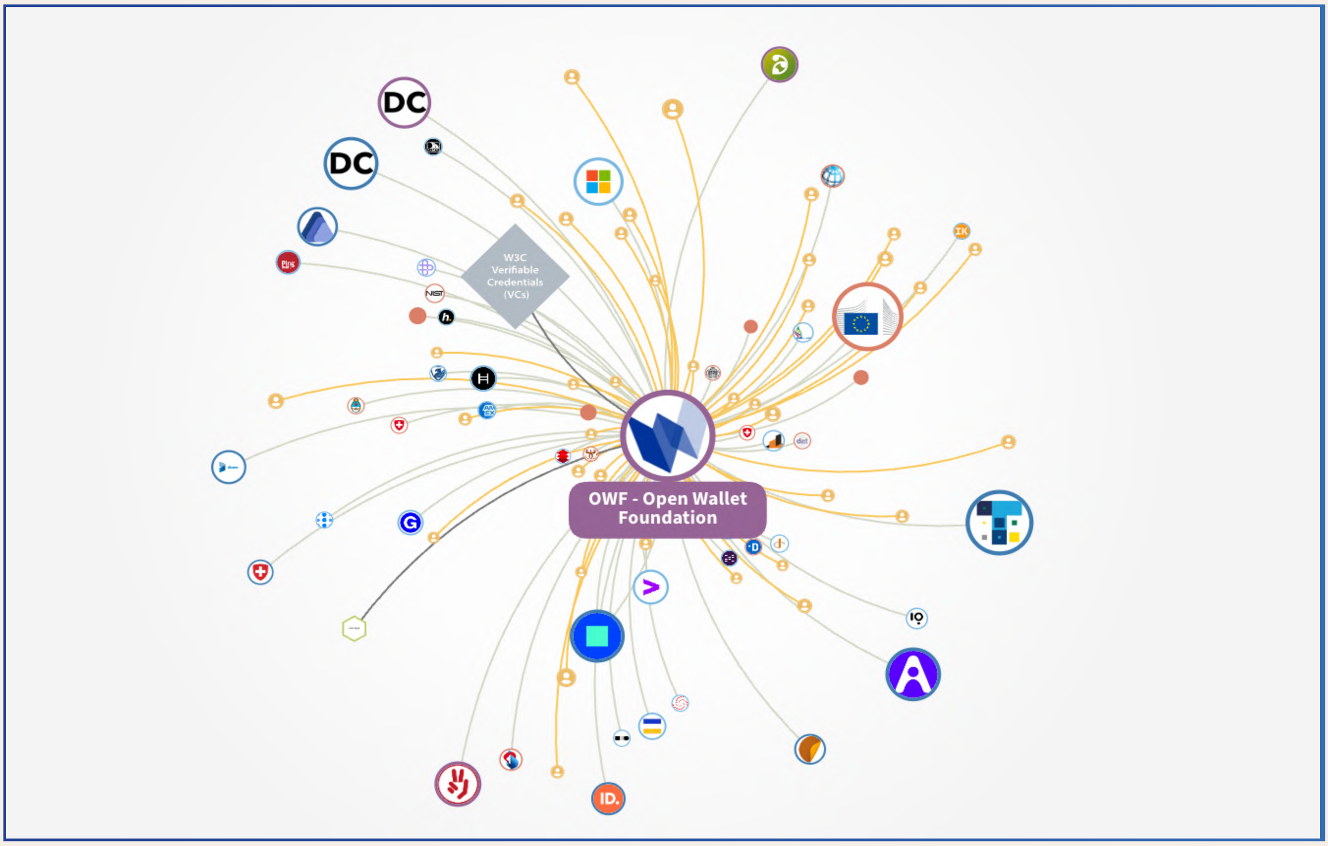
STATUS	WEBSITE
Active	openwallet.foundation
COUNTRY (HQ)	**LAUNCH**
Belgium	2023

CONNECTIONS

128

DESCRIPTION

To set best practices for digital wallet technology through collaboration on standards-based OSS components that issuers, wallet providers and relying parties can use to bootstrap implementations that preserve user choice, security and privacy.


W3C Verifiable Credentials (VCs)
OWF - Open Wallet Foundation
DC
DC
ID.

See the full view on Web of Trust Map

TRUST OVER IP FOUNDATION

TRUST Over IP FOUNDATION

LAUNCH: 2020
HQ: United States
MANAGING ENTITY:
Joint Development Foundations Projects, LLC.

OVERVIEW

ToIP[43] was launched to develop an architecture for Internet-scale digital trust. In September 2024, the Foundation became the first standards project hosted within the newly established LFDT umbrella.

ToIP has grown to include over 300 member organizations, reflecting its strong influence in the decentralized identity ecosystem. Among its top public members are the Government of Western Australia and the International Americas Development Bank. Leading private sector members include NEC Corporation, IBM Watson Health, Adobe and GLEIF, underscoring ToIP's broad industry reach and impact.

TECHNICAL & STRATEGIC HIGHLIGHTS

The foundation's core architectural focus is the development of the ToIP Stack, a four-layer architecture for decentralized digital trust infrastructure. This features, most importantly, the concept of a governance framework, overseeing the implementation and management of credential ecosystems across vertical applications and horizontal spanning layers.

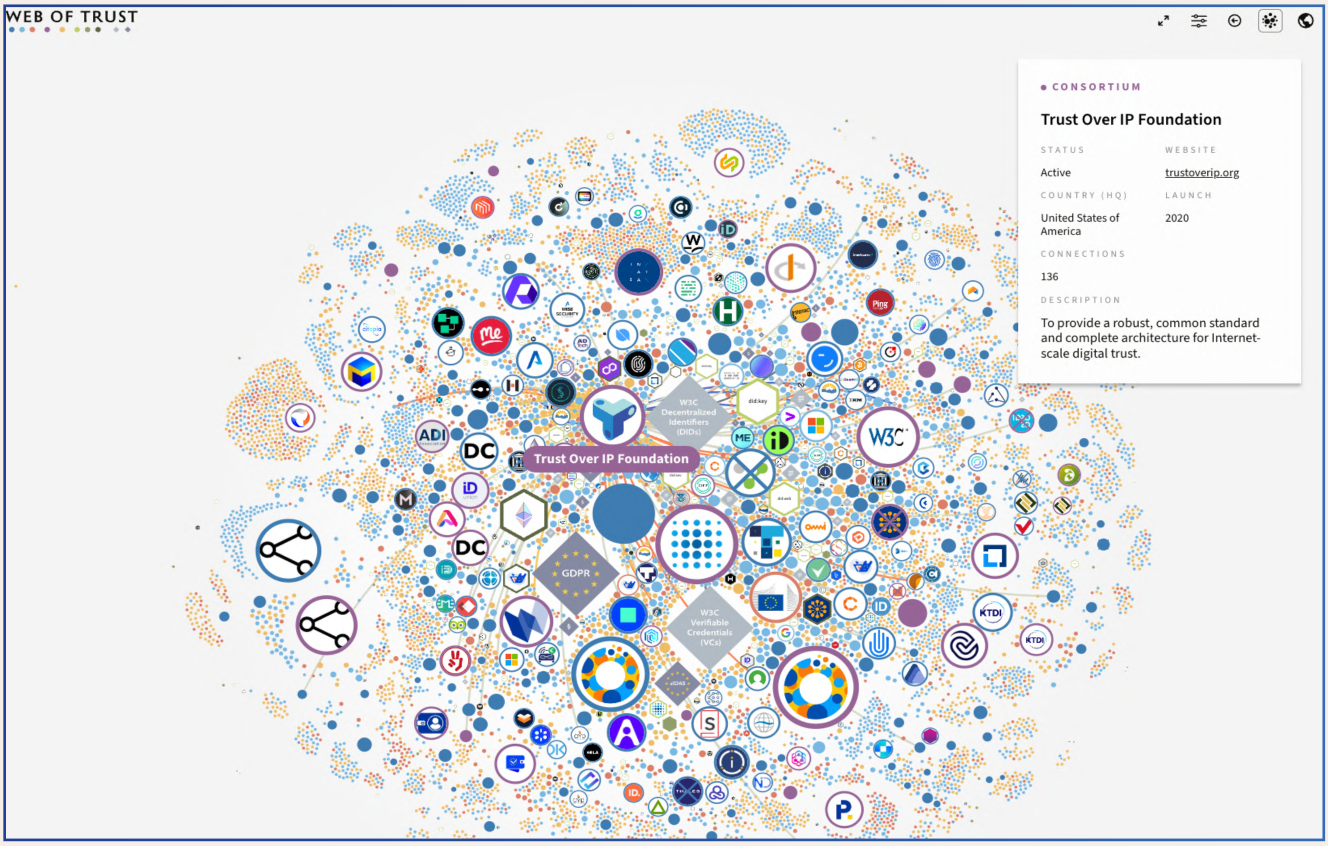
ToIP maintains key specifications like Key Event Receipt Infrastructure (KERI) for secure key management and Authentic Chained Data Containers (ACDC) for verifiable data exchange[36, 44]. Notable specifications developed by the organization include:

- Trust Spanning Protocol, for establishing trust relationships.
- Trust Registry Query Protocol, for ecosystem queries.
- W3C DID method implementations, such as did:webs and did:x509.

> *AFTER FIVE YEARS OF LAYING THE FOUNDATIONS AT TRUST OVER IP (TOIP) AND OTHER STANDARDS BODIES, **WE ARE NEARING AN INFLECTION POINT FOR DECENTRALIZED DIGITAL TRUST INFRASTRUCTURE.** PROJECTS ARE NOW EMERGING TO ENABLE BREAKTHROUGH FEATURES AT SCALE.*
>
> *THE **FIRST PERSON PROJECT** IS A GOOD EXAMPLE: IT AIMS TO COMBINE STANDARDS FROM TOIP, LF DECENTRALIZED TRUST, DIF, OWF, AYRA, W3C AND MANY OTHER PROJECTS IN THE WEB OF TRUST MAP TO FINALLY DELIVER A UNIVERSAL PRIVACY-PRESERVING PROOF OF PERSONHOOD—A CRITICAL NEW ELEMENT OF CYBERSECURITY INFRASTRUCTURE IN THE AGE OF AI.*

DRUMMOND REED, FOUNDER OF THE OPEN WALLET FOUNDATION, TRUST OVER IP, AYRA FORUM, AND THE FIRST PERSON PROJECT

TRUST OVER IP FOUNDATION


WEB OF TRUST
Trust Over IP Foundation
W3C Decentralized Identifiers (DIDs)
W3C Verifiable Credentials (VCs)
GDPR
W3C

● CONSORTIUM

Trust Over IP Foundation

STATUS	WEBSITE
Active	trustoverip.org

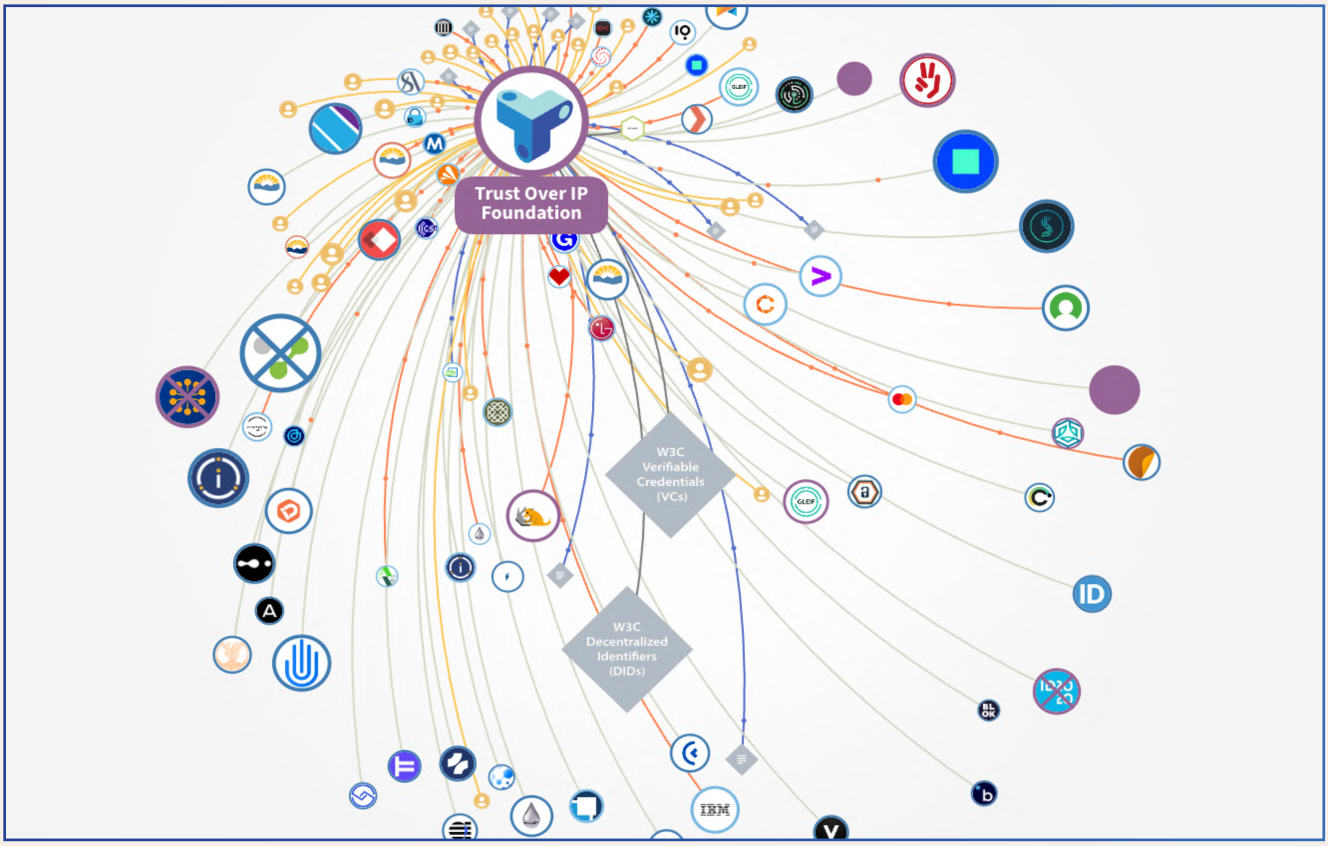
COUNTRY (HQ)	LAUNCH
United States of America	2020

CONNECTIONS

136

DESCRIPTION

To provide a robust, common standard and complete architecture for Internet-scale digital trust.


Trust Over IP Foundation
W3C Verifiable Credentials (VCs)
W3C Decentralized Identifiers (DIDs)
IBM

See the full view on Web of Trust Map

INTERNATIONAL ASSOCIATION FOR TRUSTED BLOCKCHAIN APPLICATIONS

INATBA
International Association
for Trusted Blockchain Applications

LAUNCH: 2019
HQ: Belgium
MANAGING ENTITY:
International Association for Trusted
Blockchain Applications, AISBL

OVERVIEW

The International Association for Trusted Blockchain Applications (INATBA)[45] is a global forum established with the backing of the European Commission to foster collaboration between blockchain industry stakeholders and policymakers.

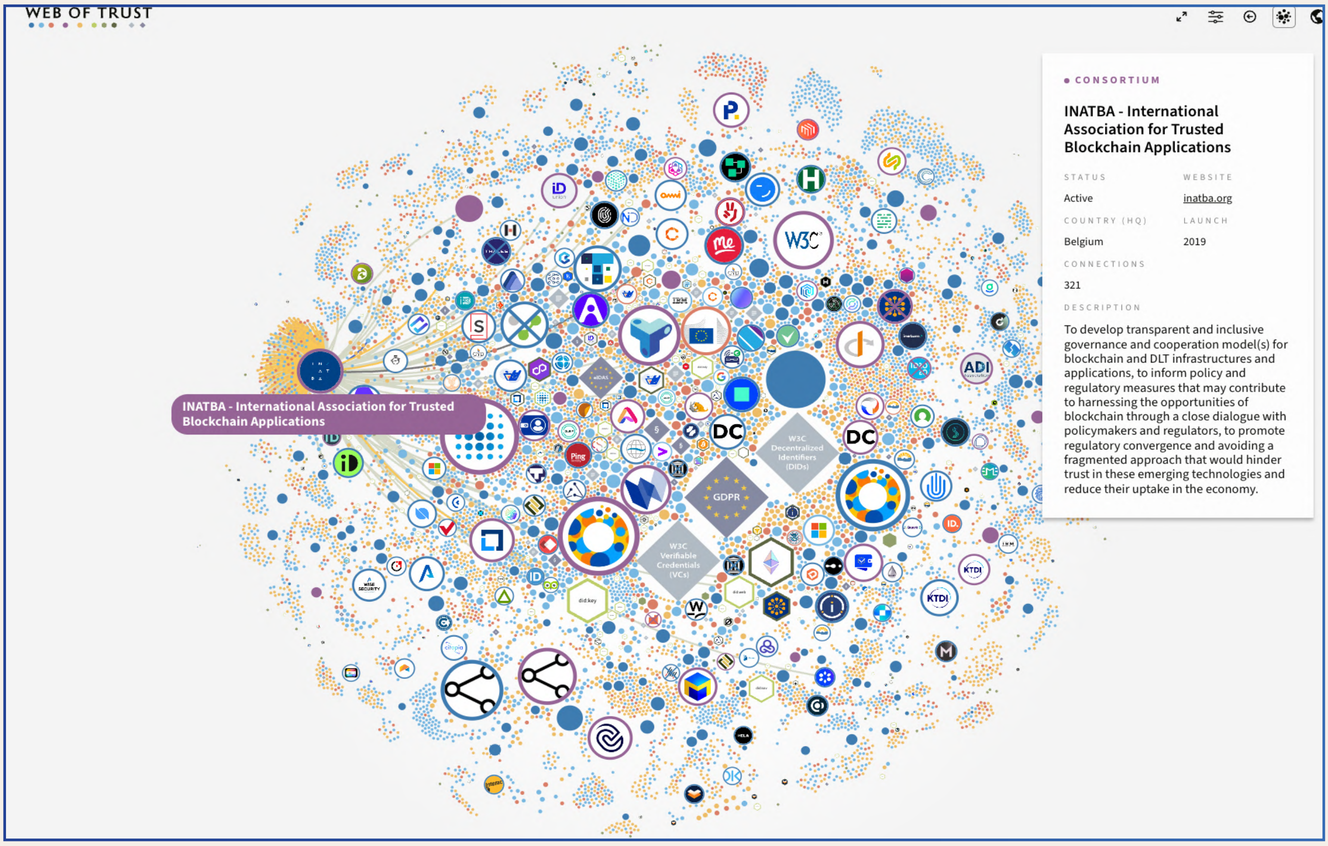
This organization has the most relations in the Web of Trust Map, with 212 connections across affiliated entities, government relations, and public and private members. Its public sector members include the European Commission, the Government of Canada, Japan's Cabinet Secretariat, as well as numerous public universities. Among its private sector members are key organizations such as IBM United Kingdom, BBVA, Cardano, and Cheqd.

TECHNICAL & STRATEGIC HIGHLIGHTS

INATBA advances decentralized digital identity through working groups and task forces focused on standardization, interoperability, and regulatory alignment. The Web of Trust Map features those contributing to SSI standardization through their efforts, such as:

- **Identity Working Group:** Promotes trust and interoperability in decentralized identity systems and SSI services, and engages with European Union (EU) policy on the Electronic Identification, Authentication and Trust Services (eIDAS) and the EU Digital Identity framework.
- **Digital Credentials Task Force:** Develops recommendations to advance cross-border interoperability and mutual recognition of digital credentials.
- **Privacy Working Group:** Focuses on data protection, privacy-preserving technologies (e.g. zero-knowledge proofs), data sovereignty, and regulatory engagement.

INTERNATIONAL ASSOCIATION FOR TRUSTED BLOCKCHAIN APPLICATIONS


WEB OF TRUST
INATBA - International Association for Trusted Blockchain Applications
W3C
GDPR
W3C Decentralized Identifiers (DIDs)
W3C Verifiable Credentials (VCs)
DC
ADI
KTDI
did:key

● CONSORTIUM

INATBA - International Association for Trusted Blockchain Applications

STATUS
Active

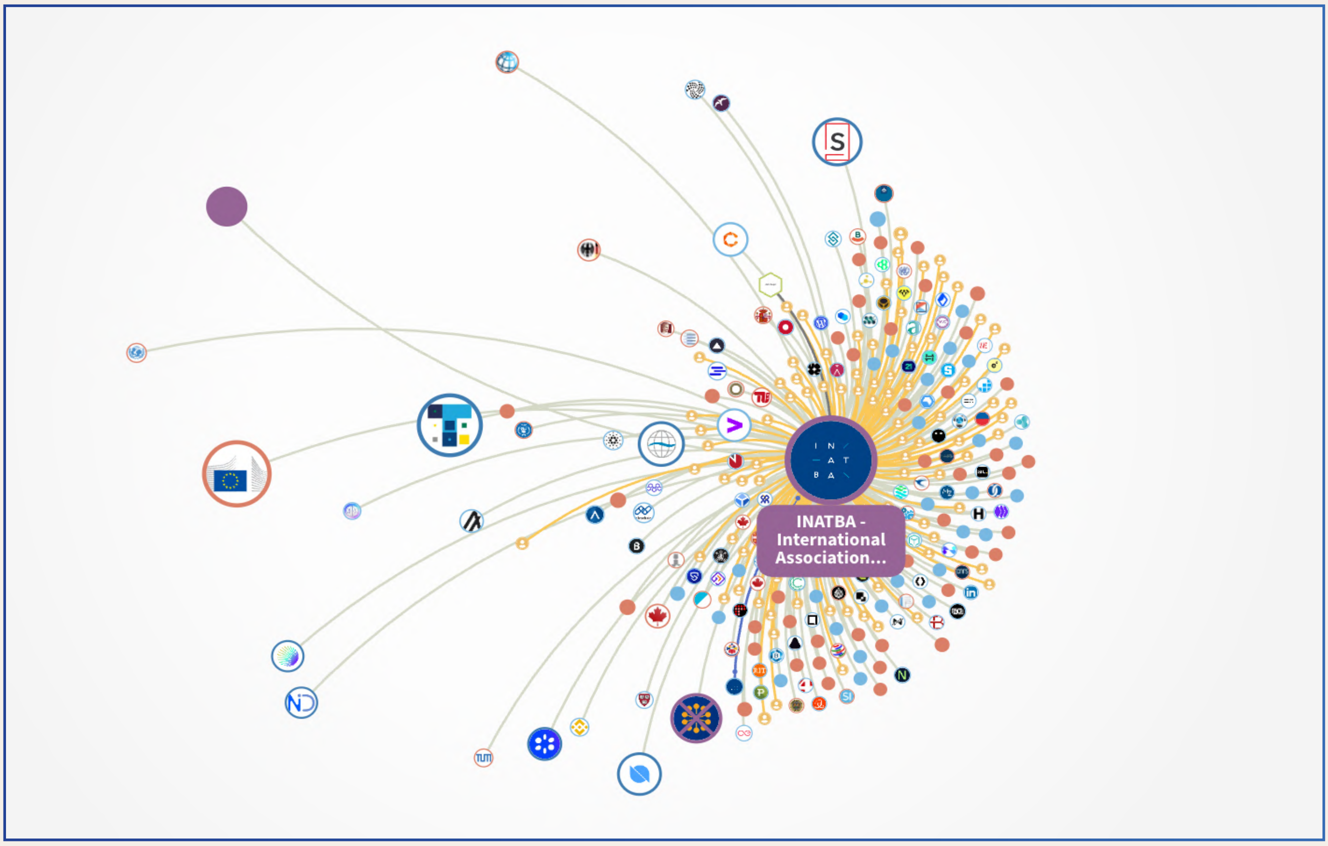
WEBSITE
inatba.org

COUNTRY (HQ)
Belgium

LAUNCH
2019

CONNECTIONS
321

DESCRIPTION
To develop transparent and inclusive governance and cooperation model(s) for blockchain and DLT infrastructures and applications, to inform policy and regulatory measures that may contribute to harnessing the opportunities of blockchain through a close dialogue with policymakers and regulators, to promote regulatory convergence and avoiding a fragmented approach that would hinder trust in these emerging technologies and reduce their uptake in the economy.



[See the full view on Web of Trust Map](#)

SPECIALIZED INITIATIVES

In addition to the core ecosystem drivers, several consortia play a meaningful role in advancing the decentralized identity landscape. While smaller in size or narrower in scope, they demonstrate strong regional leadership, technical specialization, and targeted advancements that contribute to the ecosystem's growth and diversity.

AYRA ASSOCIATION

LAUNCH: 2025
HQ: Switzerland
MANAGING ENTITY: Ayra Association

As one of the most recently launched consortia, the Ayra Association (formerly known as the Global Acceptance Network)[46] is dedicated to developing an interconnected ecosystem for digital trust. Acting as a neutral facilitator, the organization addresses scalability challenges related to verifiable data and digital trust infrastructure.

OPENID FOUNDATION

LAUNCH: 2007
HQ: United States
MANAGING ENTITY: OpenID Foundation

The OpenID Foundation[47] is a global standardization body known for developing widely adopted identity standards such as OpenID Connect. The Web of Trust Map features the foundation's Connect Working Group, which develops the OID4VC suite. This suite includes three core specifications for self-sovereign authentication and the issuance and presentation of verifiable credentials. Alongside the OID4VC suite, the Web of Trust Map highlights 10 other standards and protocols under the initiative's management.

> *THE EUDI WALLET'S SELECTION OF OID4VCI, OID4VP, AND HAIP CREATES DEPLOYMENT ACROSS ALL EU MEMBER STATES BY YEAR-END, GIVING EVERY EUROPEAN ACCESS TO WALLETS BUILT ON OIDF SPECIFICATIONS. THIS TECHNICAL CHOICE IS DRIVING ADOPTION BEYOND EUROPE. SWITZERLAND, AND CALIFORNIA'S DMV HAVE DEPLOYED THESE SPECIFICATIONS, WHILE MOSIP OFFERS THEM GLOBALLY.*
>
> *WE ALSO EXPECT THAT OTHER BORDERING COUNTRIES LIKE THE WESTERN BALKANS COULD ALSO FOLLOW THE EUDI WALLET PATH. THE EU'S DECISION IS CREATING THE NETWORK EFFECTS NEEDED FOR TRUE INTEROPERABILITY, AS RELYING PARTIES NATURALLY WANT TO INTEGRATE WITH THIS SUBSTANTIAL AND GROWING USER BASE.*

GAIL HODGES - EXECUTIVE DIRECTOR AT THE OPENID FOUNDATION

DIGITAL IDENTITY AND DATA SOVEREIGNTY ASSOCIATION

LAUNCH: 2020
HQ: Switzerland
MANAGING ENTITY: Digital Identity and Data Sovereignty Association (DIDAS)

DIDAS[48] is a Swiss non-profit organization founded to advance the adoption and development of SSI in Switzerland. DIDAS maintains active working groups across a range of sectors, including health, mobility, financial services, logistics, supply chain management, and e-commerce. DIDAS works closely with longtime Internet Identity Workshop (IIW) facilitators and the local partner Trust Square to enable the Digital Identity unConference Europe (DICE).

DIGITAL ID AND AUTHENTICATION COUNCIL OF CANADA

LAUNCH DATE: 2012
HQ: Canada
MANAGING ENTITY: Digital ID and Authentication Council of Canada (DIACC)

DIACC[49] is a non-profit consortium established following the need for stronger digital identity and authentication systems[50]. The Pan-Canadian Trust Framework is central to DIACC's work. It provides a structured set of rules, standards, and guidance to ensure secure, privacy-preserving, and user-centric digital identity and credential services. To support adoption and trust, DIACC offers a certification program that provides independent third-party assessments to verify compliance with the Pan-Canadian Trust Framework requirements.

> *"OUR BIGGEST ACCOMPLISHMENT HAS BEEN **CREATING THE PAN-CANADIAN TRUST FRAMEWORK, A MADE-IN-CANADA SET OF AUDITABLE GUIDELINES THAT IS BOTH GLOBALLY RELEVANT AND LOCALLY GROUNDED.** IT'S THE FOUNDATION THAT ENABLES DIFFERENT ORGANIZATIONS AND GOVERNMENTS TO COLLABORATE WITH CONFIDENCE BY MITIGATING RISKS AND REDUCING LIABILITIES.*
>
> *BEYOND THE FRAMEWORK ITSELF, OUR ABILITY TO BRING STAKEHOLDERS FROM DIVERSE SECTORS TO THE SAME TABLE, TO DRIVE ADOPTION AND ALIGN ON SHARED VALUES, IS WHAT MAKES DIACC A UNIQUE STRATEGIC ALLIANCE AND A TRUSTED LEADER IN MODERN DIGITAL TRUST AND IDENTITY VERIFICATION."*

JONI BRENNAN, PRESIDENT AT DIACC

EUROPE'S LARGE-SCALE PILOTS

The EU began the implementation of four Large-Scale Pilots in April 2023 to test the European Digital Identity (EUDI) Wallet under the Digital Europe Programme. These pilots, funded by the European Commission, aimed to validate the EUDI Wallet in real-world settings, ensuring compliance with eIDAS 2.0 technical specifications, cross-border interoperability, and user-centric digital identity solutions.

Structured as public-private consortia, the pilots brought together over 350 organizations across 27 EU member states, Norway, Iceland, and Ukraine. Laying the groundwork for its widespread deployment across the EU, they tested the wallet across 11 key use cases.

This first set of pilots is scheduled to conclude in 2025[51], although some, such as the Digital Credentials for Europe (DC4EU) Consortium, have already been completed, paving the way for a new set of Large-Scale Pilots being defined by the European Commission.

POTENTIAL[52]

LAUNCH: 2022
HQ: France
COUNTRIES INVOLVED: 19 EU members states + Ukraine[53]
MEMBERS: Public (96), Private (66)
USE CASES: eGov services, Bank Account Opening, SIM Card Registration, Mobile Driving License, Qualified eSignature, ePrescription

EU DIGITAL IDENTITY WALLET CONSORTIUM - EWC [54]

LAUNCH: 2022
HQ: Sweden
COUNTRIES INVOLVED: all 27 EU member states and partners from other countries[55]
MEMBERS: Public (22), Private (49)
USE CASES: Travel, payments and legal persons. Focused on Digital Travel Credentials.

NOBID CONSORTIUM [56]

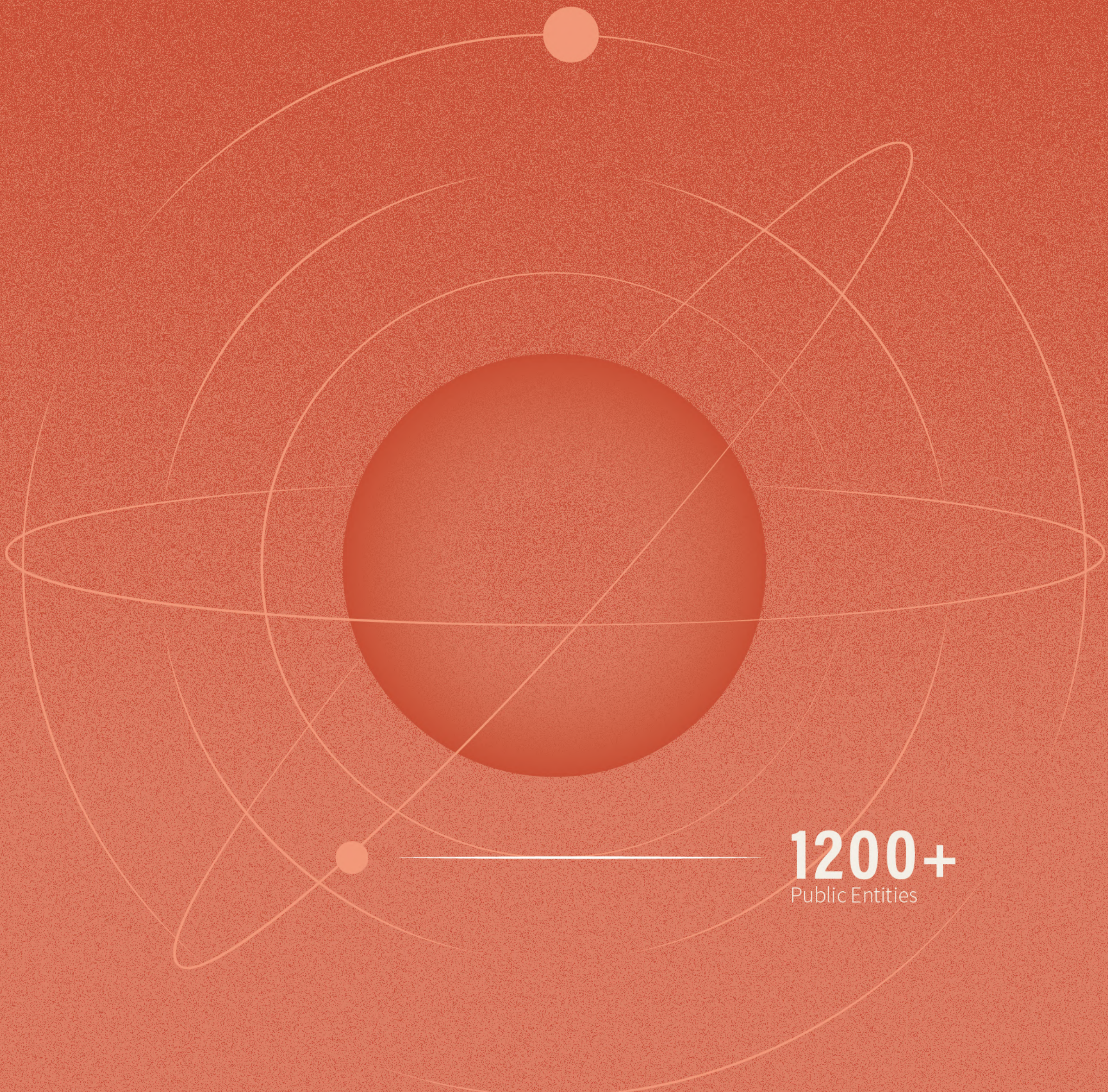
LAUNCH: 2023
HQ: Norway
COUNTRIES INVOLVED: Nordic and Baltic countries, together with Italy and Germany Island, Norway, Denmark, Latvia [57]
MEMBERS: Public (9), Private (16)
USE CASE: Payments for domestic and cross border usage

DIGITAL CREDENTIALS FOR EUROPE CONSORTIUM- DC4EU[58]

LAUNCH: 2023
HQ: Spain
COUNTRIES INVOLVED: 22 EU member states plus Norway, Ukraine and Switzerland[59]
MEMBERS: Public (52), Private (22)
USE CASE: Education and social security

3. GOVERNMENT INVOLVEMENT

Governments are central actors in the decentralized identity ecosystem, serving simultaneously as enablers, adopters, and funders of emerging technologies. Their participation provides legitimacy and trust, facilitates large-scale deployment, and ensures alignment with regulatory and policy frameworks. In fact, government affiliation was a core inclusion criterion for the Web of Trust Map, meaning that nearly all mapped projects maintain some form of governmental connection.



1200+
Public Entities

3. GOVERNMENT INVOLVEMENT

Governments act as key enablers, adopters, and funders of decentralized identity technologies, providing the trust and support necessary for large-scale implementations.

As part of the inclusion criteria for the Web of Trust Map, government affiliation was required for a project to be included. Therefore, the majority of the projects on the map, with a few exceptions, have some form of government relations.

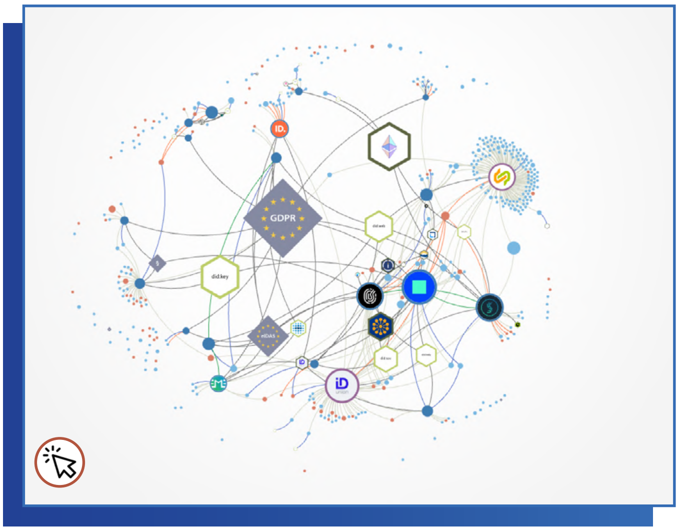
Government involvement in the decentralized identity ecosystem can result in:

- **Legitimacy and trust:** Helps legitimize decentralized identity technologies for the public and other institutions.
- **Enabling widespread adoption:** With their infrastructure, reach, and authority, governments can more easily deploy identity solutions to large populations, driving adoption beyond limited pilots or specific industries. This can also encourage private sector adoption.
- **Policy alignment and standarization:** Ensure compliance with laws and privacy regulations (e.g., General Data Protection Regulation - GDPR) while also setting common standards that enable interoperability across jurisdictions, as seen with the European Blockchain Services Infrastructure (EBSI) and EUDI Wallets initiatives.
- **Public service modernization:** Can improve access to and delivery of digital government services.

Various countries and regions have adopted decentralized identity approaches through pilots, funding, or large-scale projects. The governments with the most significant involvement in the current decentralized identity ecosystem include Germany, Canada, the European Union, the United States, and South Korea.

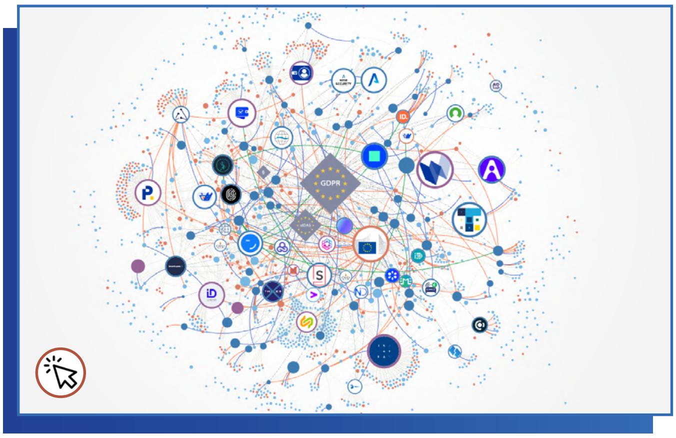
Top Goverments involved in Decentralized Identity	Number of decentralized identity projects being supported
European Commission	122
European Blockchain Service Infrastructure (EBSI)	23
Government of British Columbia	19
U.S. Department of Homeland Security	18
Government of Canada	16
(German) Federal Ministry for Economic Affairs and Climate Action	15
(Canada) Government of Ontario	14
Korea Internet and Security Agency	8
(South Korean) Ministry of Science and ICT	8
(German) Bundesagentur für Sprunginnovationen GMBH	7
(German) Bundesdruckerei Gruppe GMBH	7
(German) Federal Ministry of Education and Research	6

GERMANY



Since 2020, Germany has been a pioneer in the decentralized identity ecosystem, initially through the funding of the IDunion network, an initiative supported by the Federal Ministry of Economics and Energy (BMWi), now known as the Federal Ministry for Economic Affairs and Climate Action (BMWK)[60]. Since then, various government agencies have also become increasingly involved, including the Bundesagentur für Sprunginnovationen (SPRIND)[61], the Bundesdruckerei Gruppe (Federal Printing Office Group)[62], and the Federal Ministry of Education and Research[63]. These agencies have demonstrated their commitment to the current ecosystem through funding, project incubation, or active participation.

EUROPEAN UNION



The European Commission[64] has demonstrated the most significant involvement in the decentralized identity ecosystem through its funding initiatives, pilots, incubation programs, and large-scale adoption initiatives. This includes EBSI[65], designed to enable cross-border interoperability, and the legislative framework eIDAS 2.0[66], which promotes digital identity adoption across the EU. While eIDAS 2.0 considered blockchain as a verifiable data registry, it ultimately remains technology-neutral, allowing multiple approaches to the implementation. The current trend in 2025 is a move towards web2-based solutions for eIDAS 2.0, with the initial focus on decentralized ledgers becoming less relevant for the European Commission-funded initiatives. Regardless, by combining funding, a supportive legal framework, and an operational blockchain infrastructure, Europe has set a strong precedent for advancing decentralized identity at a regional level.

> *THE EU DIGITAL IDENTITY WALLET CONSORTIUM WAS A GREAT BUILDING BLOCK FOR THE EUDI WALLET ECOSYSTEM. MANY OF THE LEARNINGS AND WORK WILL BE USED,* ***SERVING AS THE FOUNDATION FOR THE NEXT GENERATION OF LARGE-SCALE PILOTS,*** *PARTICULARLY IN THE WE BUILD CONSORTIUM. IN THE LONG TERM, I BELIEVE THE BUSINESS WALLET - LIKELY TO BECOME HIGHLY IMPORTANT - WILL BE THE REAL LEGACY.*
>
> *THE DECENTRALIZED IDENTITY SPACE WILL KEEP PUSHING THE BOUNDARIES OF WHAT WE WORK WITH AND DIGITAL IDENTITY. HOWEVER, THERE WILL ALSO BE SOME DISAPPOINTMENT, AS* ***THE REAL DECENTRALIZATION THAT SOME OF THE MOST ENGAGED PEOPLE HOPE FOR IS NOT MATERIALIZING, NEITHER IN THE EU NOR IN OTHER ADVANCED REGIONS SUCH AS INDIA OR SINGAPORE.***

DAVID MAGÅRD, COORDINATOR FOR EWC - EU DIGITAL IDENTITY WALLET CONSORTIUM.

CANADA

The Government of Canada has been active in the adoption of decentralized identity since 2018 through the Known Traveller Digital Identity pilot, an initiative of the World Economic Forum[67]. Since then, the Government of Canada has been involved in other private initiatives such as Blockcerts, Oliu, INATBA, among others[68,69,70].

The Government of British Columbia[71] is particularly notable for its high level of involvement in projects included in the Web of Trust Map, with more than 10 connections related to funding and affiliations. It is also pursuing its own government-led initiatives, including BC Wallet[72], a mobile wallet application that enables users to receive, store, and present verifiable credentials, and OrgBook BC[73], a public digital directory service providing verified information about organizations registered in the province.

Another government-led initiative is Ontario's Digital ID[74], which aims to provide citizens with a secure, privacy-preserving way to prove their identity both online and in person. In addition to this program, the Government of Ontario[75] is also involved in various other decentralized identity projects.

> *CANADA HAS TAKEN A THOUGHTFUL AND COLLABORATIVE APPROACH TO DECENTRALIZED IDENTITY BY SUPPORTING A WIDE RANGE OF PROJECTS AND VOICES. CANADIANS HAVE INVESTED IN TESTING, LEARNING, AND BUILDING TRUST ACROSS MULTIPLE TECHNOLOGY STACKS.*
>
> *THIS DIVERSE APPROACH HELPS ENSURE THAT **DECENTRALIZED IDENTITY REFLECTS THE NEEDS OF PEOPLE, BUSINESSES, AND GOVERNMENTS.** IT'S ABOUT FINDING BALANCE BETWEEN INNOVATION AND PRACTICALITY, SO THAT IDENTITY SOLUTIONS ARE SECURE, INCLUSIVE, AND BUILT FOR THE LONG TERM.*

JONI BRENNA, PRESIDENT OF THE DIGITAL ID & AUTHENTICATION COUNCIL OF CANADA (DIACC)

SOUTH KOREA

South Korea has been actively involved in SSI through the Korea Internet & Security Agency[76] and the Ministry of Science and ICT[77], which have the most amount of involvement in the space through various partnerships in the Web of Trust Map. These two agencies back the Initial DID Alliance[78], which is one of the consortia present in the country focusing on SSI use cases. These two agencies have involvement with Seoul Wallet[22], B Pass[79], Initial[80], and Wepublic Wallet[81]; demonstrating a high level of engagement and leadership in shaping South Korea's decentralized identity landscape.

UNITED STATES

Since 2016, the DHS has funded research and development in cybersecurity technologies, including digital identity credentials[82]. DHS has provided funding to at least five projects focused on SSI and related technologies. It has worked with companies such as SecureKey, Transmute, and Danube Tech, among others[83].

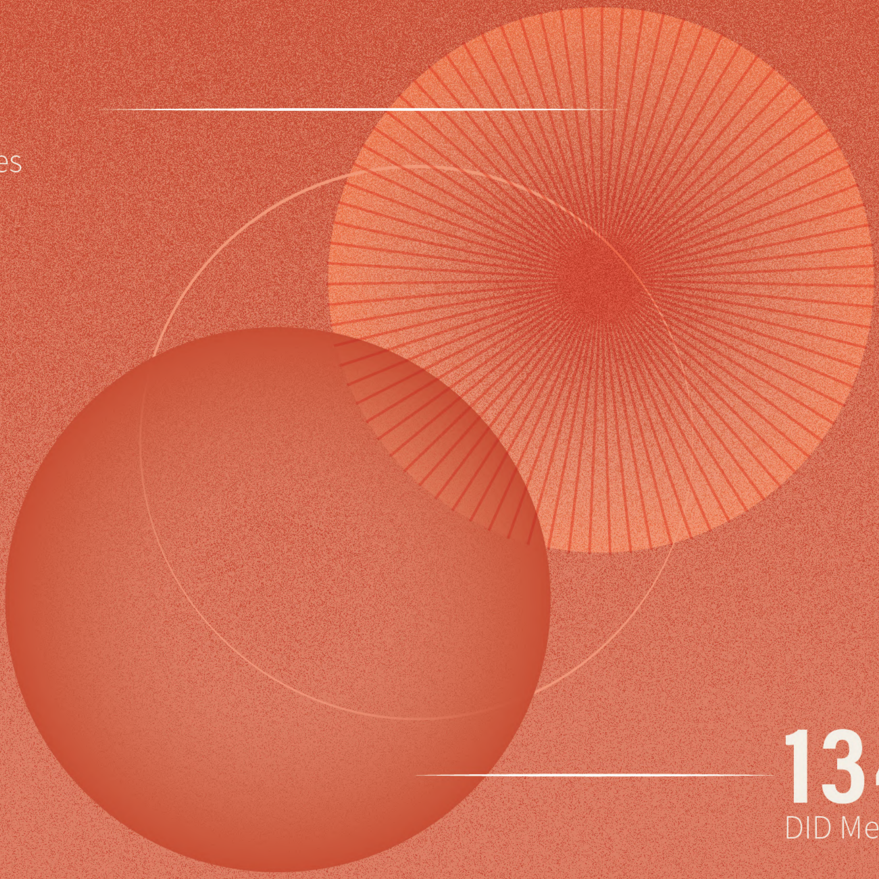
In parallel, DHS has participated in W3C, specifically within the VC Working Group, contributing to the development of technical standards for decentralized identity systems[84].

> *THE BIGGEST BARRIERS HAVE BEEN ADOPTION BY LARGE TRUSTED INSTITUTIONS, LIKE GOVERNMENT.* ***WITHOUT TRUSTED INSTITUTIONS STANDING BEHIND ISSUED CREDENTIALS IT'S HARD TO TRUST A NEW THING LIKE THIS, AND TO TRUST CREDENTIALS.***
>
> *MOST GOVERNMENT-LED INITIATIVES ARE* ***PERVERTING THE DECENTRALIZED MODEL IN ONE WAY OR ANOTHER SO THAT IT'S STILL MOSTLY CENTRALIZED.*** *THIS HAS OCCURRED BECAUSE OF THE PRIVATE SECTOR ADVISORS LEADING GOVERNMENT ACTORS TO ADOPT MODELS FAVORABLE TO THEIR CURRENT BUSINESSES, WHICH IS UNFORTUNATE.*
>
> *I AM PARTICULARLY INTERESTED IN WHAT THE U.S. STATE OF UTAH IS DOING WITH SEDI: STATE-ENDORSED DECENTRALIZED IDENTITY. IT BRINGS* ***THE POWER OF GOVERNMENT WHILE STILL RESPECTING THE PRIVACY AND AUTONOMY OF INDIVIDUALS IN A BALANCED WAY.***

TIMOTHY RUFF, PRINCIPAL AT DIGITAL TRUST VENTURE PARTNERS

4. TECHNICAL INFRASTRUCTURE

Every digital identity system rests on a backbone of technologies like blockchains, DID methods, and interoperability standards. These specifications determine whether systems can scale, whether users stay in control, and whether projects can be compatible. The Web of Trust Map shows what the ecosystem's technical foundations are and what it means for the future.



140
DLT Instances

134
DID Methods

4. TECHNICAL INFRASTRUCTURE

As decentralized identity systems evolve, understanding the technical infrastructure supporting these projects is crucial to ensure technological compatibility, avoid vendor lock-in, and align for future scalable architectures. Though decentralized identity is in a maturing stage, aligning technical efforts is essential to ensure its sustainability. Widely adopted standards reduce fragmentation, support integration across systems, and enable broader use of digital credentials across jurisdictions and sectors [85].

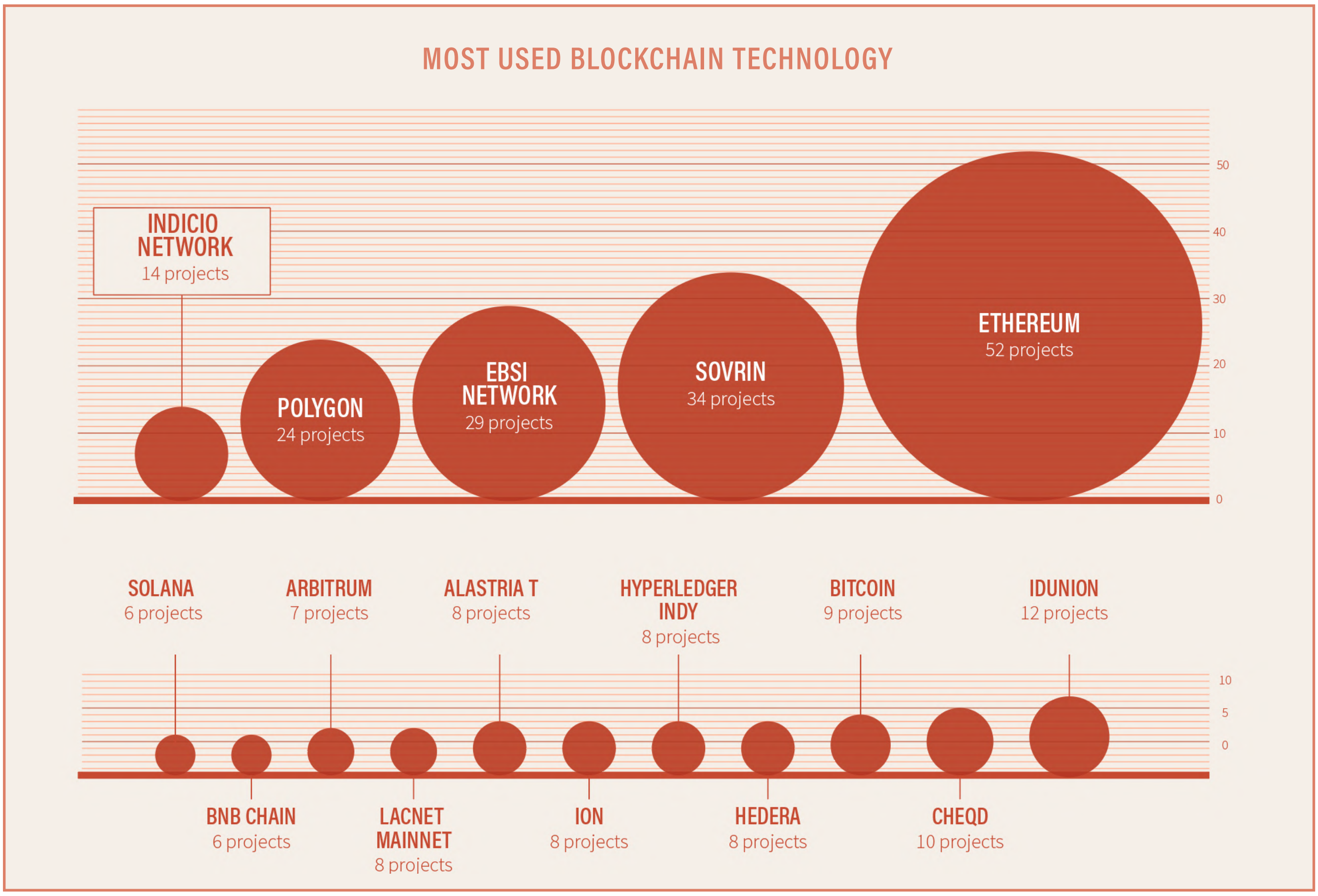
The Web of Trust Map captures a snapshot of the current technical landscape by documenting the use of distributed ledger technologies across mapped projects. It also records a project's claim to enable key features such as credential import/export, zero-knowledge proofs, or local credential storage, all relevant for privacy, usability, and portability.

BLOCKCHAIN AND LEDGER TECHNOLOGY

Among the decentralized identity projects mapped, several blockchain networks appear repeatedly as the foundational infrastructure for anchoring identifiers, issuing credentials, or ensuring data integrity. The five most commonly used blockchains and ledgers in the Web of Trust Map are:

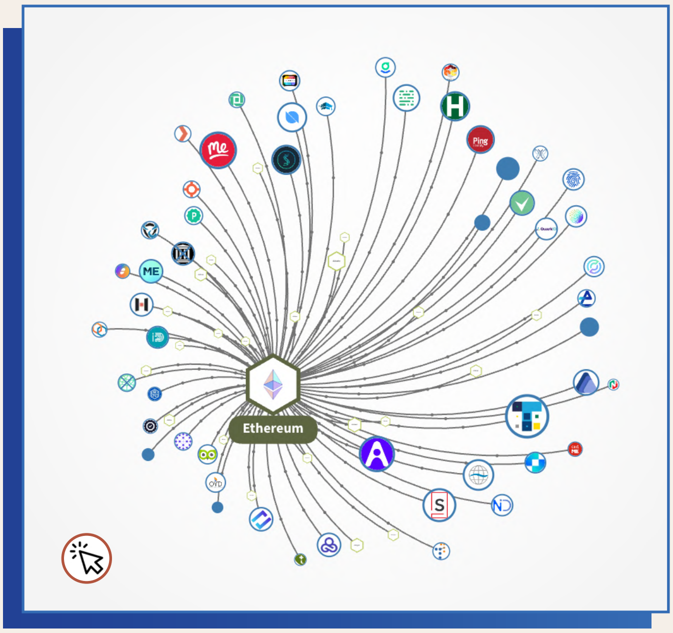
- **Ethereum:** 52 projects
- **Sovrin:** 34 projects
- **EBSI Network:** 29 projects
- **Polygon:** 24 projects
- **Indicio Network:** 14 projects

Each of these networks offers different trade-offs in terms of governance, scalability, privacy, and alignment to standards.



Source: Web of Trust Map. See more data and insights at www.weboftrust.org

ETHEREUM



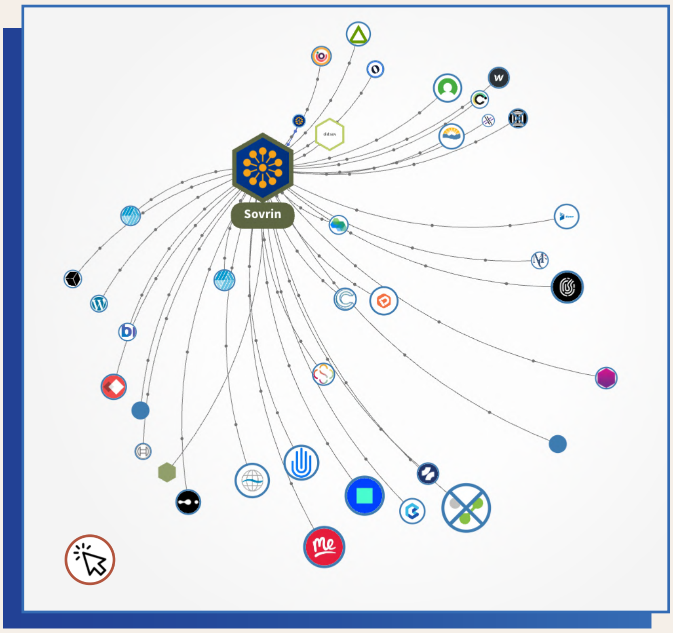
Ethereum[86] is one of the most widely adopted general-purpose blockchains, with 52 projects in the Web of Trust Map relying on it. It is also used by more than 25 DID methods, including did:ethr, did:gatc, did:iden3, and others.

This blockchain is a popular choice for decentralized identity solutions due to its smart contract functionality, security, and decentralized architecture. Developers benefit from its large ecosystem and extensive support for DID methods, making it a flexible and trusted platform for building identity systems [87].

Beyond decentralized identity, Ethereum also plays a foundational role in the broader Web3 ecosystem, supporting decentralized finance (DeFi), non-fungible tokens (NFT), and decentralized applications (dApps).

This widespread adoption has created strong developer communities, reusable infrastructure, and interoperability layers that decentralized identity projects can leverage. The overlap between Web3 and identity innovation has further reinforced Ethereum's position as a cornerstone technology for building user-controlled, verifiable digital identities.

SOVRIN

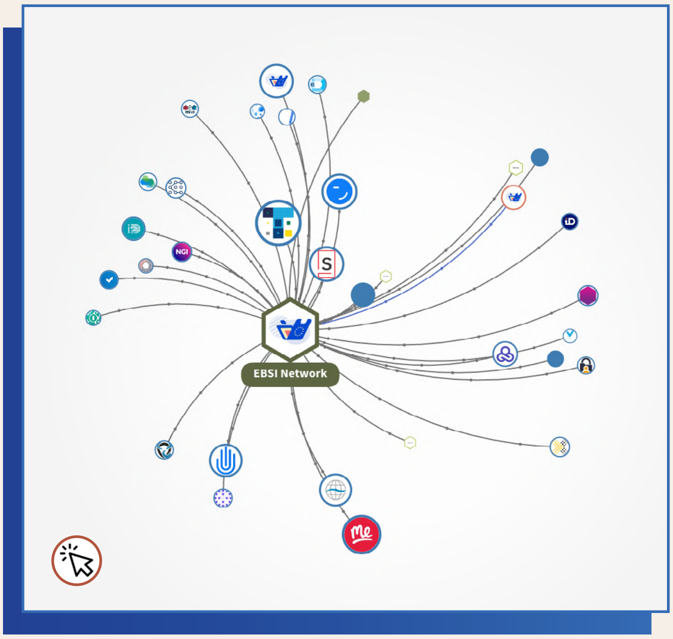


Sovrin[88] was a permissioned ledger purpose-built for digital identity use cases, based on Hyperledger Indy. It was specifically designed to support privacy-preserving credential issuance, selective disclosure, and decentralized key management. Projects using Sovrin relied on the did:sov method, which allowed for anchoring Decentralized Identifiers directly to the ledger.

Sovrin operated under a defined governance framework, with roles distributed across stewards, trustees, and other participants, making it particularly suitable for public sector deployments where trust, oversight, and compliance were critical[89]. Sovrin was also the first instance of Hyperledger Indy[90], setting a precedent for later networks such as IDunion and Indicio, which also built on the Indy ledger.

While the Sovrin Foundation has announced the shutdown of its mainnet ledger[91], its historical role remains significant. Sovrin was one of the earliest and most widely adopted networks in the SSI space, and its strong presence in the Web of Trust Map reflects the foundational role it played in shaping early SSI infrastructure and governance models.

EBSI NETWORK

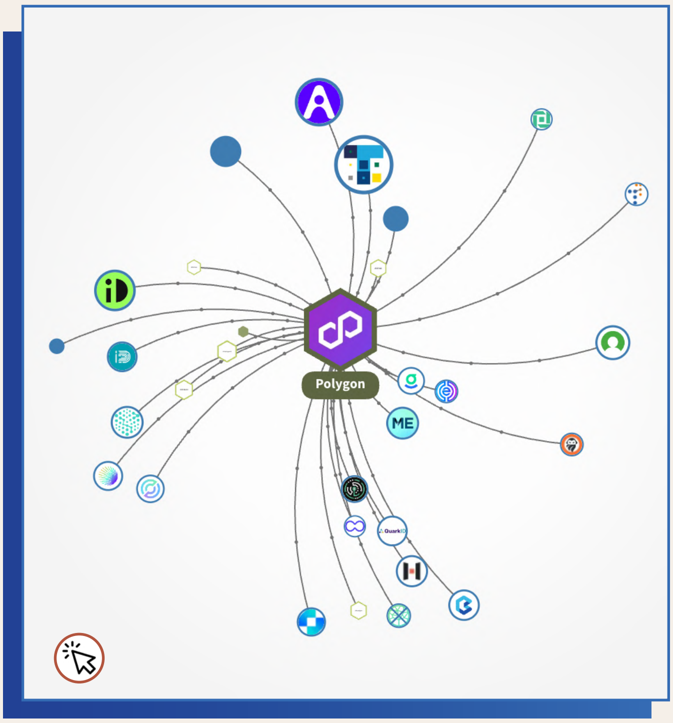


EBSI[92] is one of the most widely used ledgers in the Web of Trust Map, with 29 projects building on it. Developed by the European Commission and the European Blockchain Partnership, EBSI is a permissioned network designed to support cross-border public services and align with the EU's digital identity vision. Its strong presence in the map reflects the growing adoption of EU-backed standards and the central role of public sector initiatives in driving decentralized identity forward.

EBSI offers public read access, allowing anyone to view ledger data freely, while write permissions are limited to authorized participants. Only designated node operators (public institutions from EU member states, Norway, or Liechtenstein) can join the network through a formal onboarding process.

The system is built on Hyperledger Besu, an enterprise-ready Ethereum client designed for both public and private permissioned blockchains. As an Ethereum Virtual Machine compatible network, EBSI can also run smart contracts written in Solidity, enabling decentralized applications within a controlled and regulated environment.

POLYGON

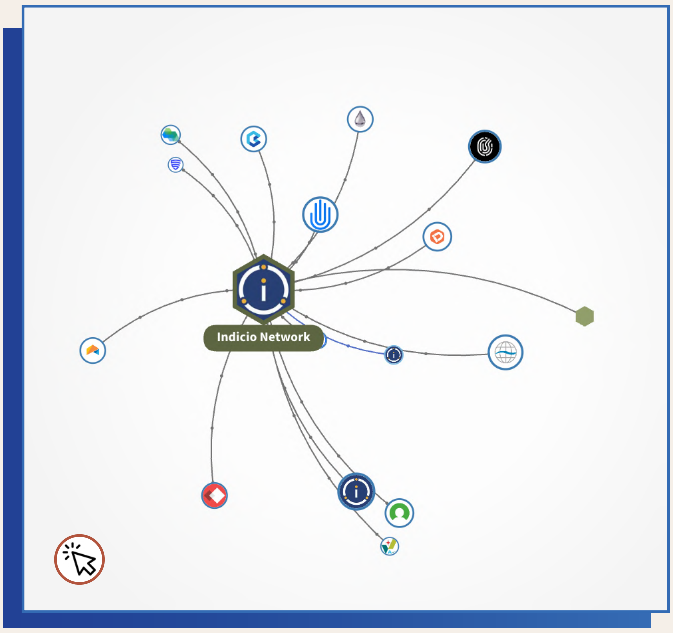


Polygon[93] is the fourth most adopted ledger in the Web of Trust Map, used by 24 projects, making it one of the most prominent Ethereum-compatible networks in the dataset.

As a scalable Layer 2 solution, Polygon offers lower transaction costs and faster processing than Ethereum, while maintaining compatibility with the Ethereum Virtual Machine. This makes it an attractive choice for developers who require cost-efficient on-chain operations, such as DID anchoring and credential verification [94].

Polygon has also been directly involved in decentralized identity through the development of Polygon ID, a privacy-preserving identity framework based on zero-knowledge proofs. Recently spun out as Privado ID, this initiative demonstrates Polygon's commitment to integrating verifiable credentials and Decentralized Identifiers into its broader Web3 ecosystem [32,95].

INDICIO NETWORK



The Indicio Network[96] is a public-permissioned ledger based on Hyperledger Indy and operated by Indicio. It has nodes distributed across five continents. As a permissioned system, only authorized participants have write access, while read remains open to the public.

The network supports decentralized identity infrastructure by enabling DID and VC exchange, following standards such as W3C DID, W3C VC, DIDComm, and AnonCreds. It is often used in conjunction with Hyperledger Aries and Ursa, and supports the deployment of identity stacks such as Indicio Proven, a project included in the map[97].

As of the current Web of Trust Map dataset, 14 projects are using Indicio as their underlying ledger, making it one of the most adopted Hyperledger Indy networks in the map.

DID METHODS AND ADOPTION

DID Methods are important because they specify how decentralized identifiers are created, managed, and resolved on different systems, making DIDs practical and usable in real-world applications. DIDs, published as a standard by the W3C, were introduced as a foundational component of SSI. They are meant to provide globally unique identifiers under the control of individuals or organizations without requiring centralized infrastructure or authorities. While DIDs are widely adopted in principle, the diversity of DID Methods [98]—which introduces challenges to interoperability and undermines uniform security guarantees—highlights the inherent limitations and contradictions of the decentralized identity ecosystem.

Among the DID Methods tracked in the Web of Trust Map[99], the five most commonly adopted are did:key, did:web, did:sov, did:indy, and did:peer:

1. **did:key:** A static, key-based DID method that derives the DID directly from a cryptographic public key, without relying on any external registry or infrastructure. Ideal for testing or device identities, though it does not support updates or deactivation[100].
2. **did:web:** A DID method that uses a domain name and HTTPS, with the DID Document hosted at a URL. It is adaptable and easy to implement with web infrastructure, but relies on DNS and domain ownership, making it more centralized[101].
3. **did:sov:** A DID method tied specifically to the Sovrin Network, designed for identity use cases on a public-permissioned ledger, and often used in controlled, high trust environments[102].
4. **did:indy:** A DID method built on Hyperledger Indy, allowing identifiers to be anchored on Indy-based ledgers like IDunion or Indicio. It supports schemas, credential definitions, and revocation registries, but adoption has declined as Indy network has shut down[103].
5. **did:peer:** A locally generated, peer-to-peer DID method intended for private, decentralized interactions without relying on public ledgers or resolvers. It is suited for secure, low-latency exchanges and avoids third party dependencies[104].

LEADING DID METHODS COMPARED

DID Method	Anchor / Infrastructure	Resolution	Use Case Highlights
DID:KEY	None (self-generated)	Local (no resolver)	Device identity; testing contexts
DID:WEB	HTTPS domain	HTTP fetches DID document	Simple org or personal identity; easy web integration
DID:SOV	Sovrin ledger	Ledger-based	Government-centric SSI deployments
DID:INDY	Indy-based distributed ledgers	Ledger-based	Complex SSI ecosystems, schema-aware credentialing
DID:PEER	No infrastructure (peer-to-peer)	Local exchange	Secure agent-to-agent or private multi-party setups

The current landscape of DID methods reflects both the diversity and fragmentation of the decentralized identity ecosystem. Each method offers different trade-offs in terms of infrastructure, governance, and usability. From simple options like did:key and did:peer, to centralized with bigger attack surface but practical approaches like did:web and did:webvh, to ledger-based methods like did:sov and did:indy. However, this diversity has not resulted in seamless adoption. There is no inherent interoperability between methods, and projects often face challenges aligning across different infrastructures.

Trends point toward centralization and pragmatism, with did:web gaining prominence due to its simplicity, even at the expense of decentralization and security. Meanwhile, ledger-based methods are in decline, with Sovrin shut down and Indy-based projects losing momentum.

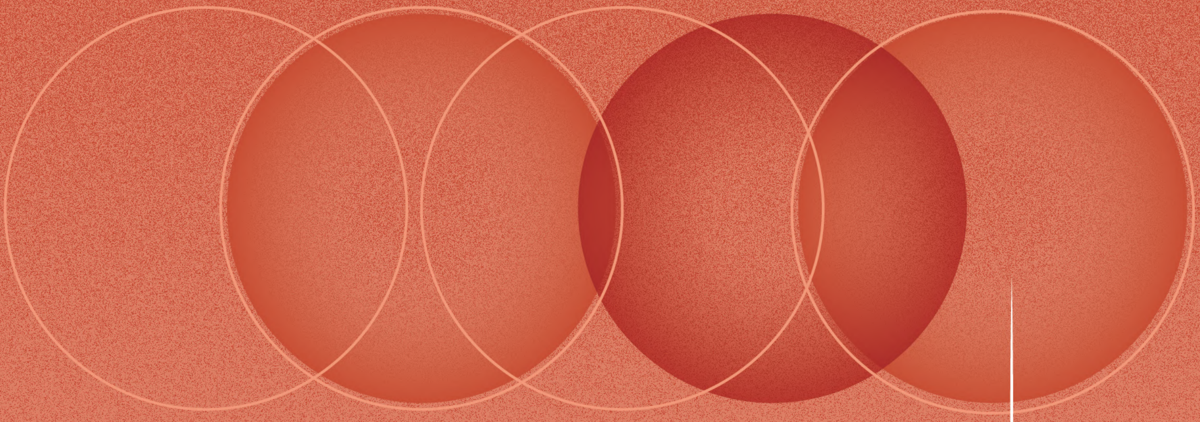
DID Methods remains a core building block for SSI, but the lack of interoperability, uneven infrastructure, and reliance on centralized systems continue to limit progress to the vision of a global, secure, and portable digital identity. This trend toward centralization is exemplified by Switzerland's plans to launch their digital ID solution on the did:webvh DID method [105], which shares did:web's centralization and resulting security concerns, which some experts have pointed out [106].

> *AS LONG AS WE ARE AWARE OF THE LIMITATIONS, AND NEVER USE IT FOR SYSTEMS THAT ARE SUPPOSED TO BE USED IN PRODUCTION BY END USERS OR SMES, THERE IS NOTHING WRONG WITH DID:WEB.*
>
> ***[...] IT'S REALLY USEFUL FOR RAPID PROTOTYPING, AND CAN BE USED AS A PLACEHOLDER DURING EXPERIMENTATION BEFORE SWITCHING TO A REAL DECENTRALIZED IDENTIFIER.*** *[...] THE PROBLEM STARTS WHEN PEOPLE PUT WEB-BASED IDENTIFIERS INTO PRODUCTION.* [106]

GEORG GREVE, CEO OF VEREIGN AND FOUNDER OF FREE SOFTWARE FOUNDATION EUROPE (FSFE)

5. STANDARDS, PROTOCOLS AND INTEROPERABILITY

Standards and protocols provide the foundational rules and formats that enable decentralized identity systems to interoperate securely and reliably across different services, geographies, and legal jurisdictions. Defined through collaborative working groups, such as W3C's Verifiable Credentials Working Group, DID Working Group, DIF's DIDComm, and OpenID Foundation's OID4VC bodies, these frameworks undergo rigorous drafting, public review, and testing before formal publication.



5. STANDARDS, PROTOCOLS AND INTEROPERABILITY

One of the most critical drivers of decentralized identity adoption is the use of open, interoperable standards. These standards aim to ensure that digital identity solutions can work across different systems, providers, and jurisdictions.

KTDI
iD
ADI
W3C Decentralized Identifiers (DIDs)
W3C Verifiable Credentials (VCs)
W3C
DC

The development of these standards is a collaborative, multi-phase process typically carried out within working groups of consortia (e.g. VC Working Group from W3C, DIDComm from DIF, OID4VC from OpenID Foundation). These working groups composed of technical experts and different stakeholders draft specifications, which then undergo multiple rounds of review, public consultation, and testing. Once a specification reaches consensus, it is formally published and promoted for adoption by developers, vendors, and service providers.

While most consortia share common elements in their standards development process, each defines its own specific procedures. As decentralized identity continues to evolve, standards are often revisited and updated regularly to incorporate new innovations and address emerging challenges.

Despite the diversity of technologies in the decentralized identity space, the Web of Trust Map reveals a clear convergence around a core set of technical standards. Projects across regions and sectors are aligning with these frameworks to ensure interoperability, security, and regulatory compatibility.

This section highlights the three most adopted standards in the mapped ecosystem:

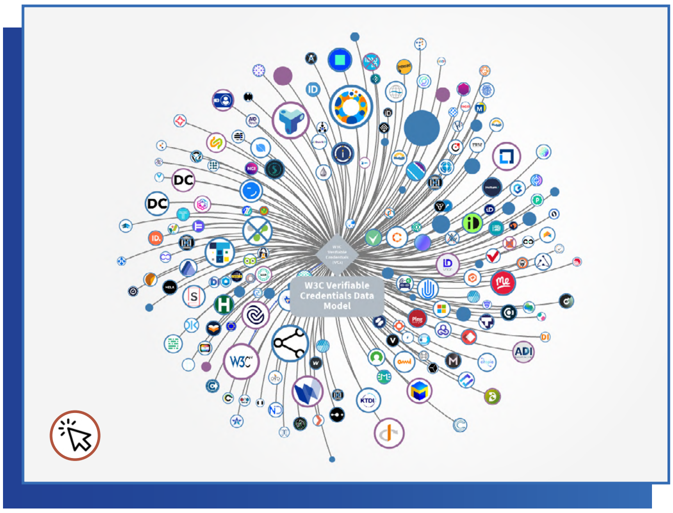
- Verifiable Credentials Data Model (W3C VC)
- Decentralized Identifiers (W3C DID)
- OpenID for Verifiable Credentials (OpenID4VC)

To see all the standards mapped, refer to the Standards page in the Web of Trust Map [107].

> *DECENTRALIZED IDENTITY IS AN EXCITING AND VERY DYNAMIC FIELD. IT IS ALSO COMPLEX AND CHANGING QUICKLY, AND **THEREFORE INTEROPERABILITY WILL BE ONE OF THE MAIN CHALLENGES GOING FORWARD.***
>
> *WE BELIEVE THAT THE WEB OF TRUST MAP IS A SUPER VALUABLE TOOL TO HELP UNDERSTAND THIS SPACE, AND WE ARE EXCITED THAT DANUBE TECH HAS BEEN ABLE TO CONTRIBUTE TO THIS TOOL BY PROVIDING INSIGHTS ON DID STANDARDS AND INITIATIVES.*

MARKUS SABADELLO, FOUNDER OF DANUBE TECH

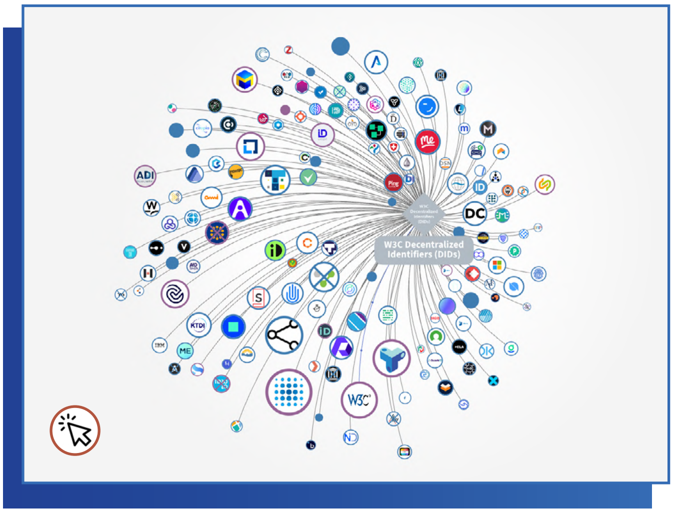
VERIFIABLE CREDENTIALS DATA MODEL (W3C VC)



The VC standard, developed by the W3C, is the most widely adopted in the dataset, used by nearly 80% of mapped projects[108, 109]. It defines the format for digitally signed, cryptographically secure credentials, such as digital diplomas, driver's licenses, or identity cards. These credentials are machine-verifiable, privacy-preserving, and can be presented without revealing more than necessary.

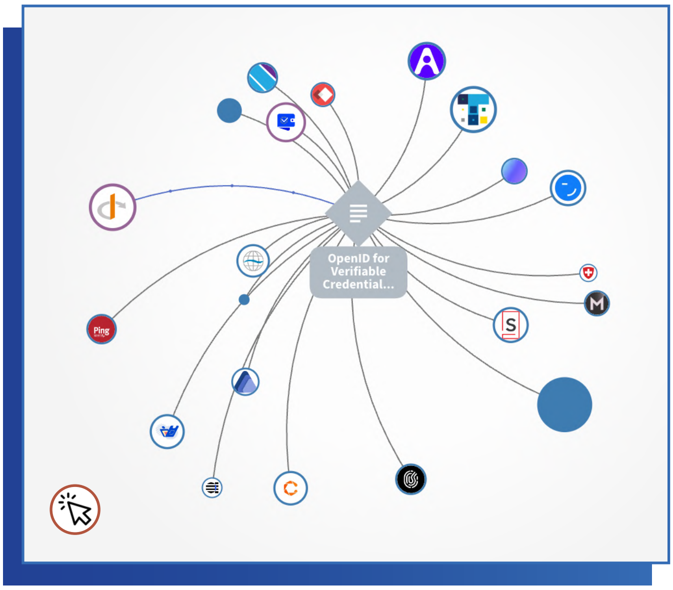
This strong adoption highlights a growing consensus on how digital credentials should be structured to ensure trust and portability across ecosystems.

DECENTRALIZED IDENTIFIERS (W3C DID)



Closely following VC is the DID standard, also published by W3C, and adopted by over two-thirds of projects[98, 110]. DIDs are globally unique identifiers that are not tied to centralized registries or authorities, enabling individuals and entities to control their identifiers and authenticate using cryptographic proofs. The DID standard supports cross-system interoperability and is fundamental to enabling SSI architectures. However, the use of DID alone does not automatically guarantee interoperability. Interoperability depends heavily on the DID method implemented for issuer key discovery, along with other design choices in DID-based systems.

OPENID FOR VERIFIABLE CREDENTIALS (OPENID4VC)



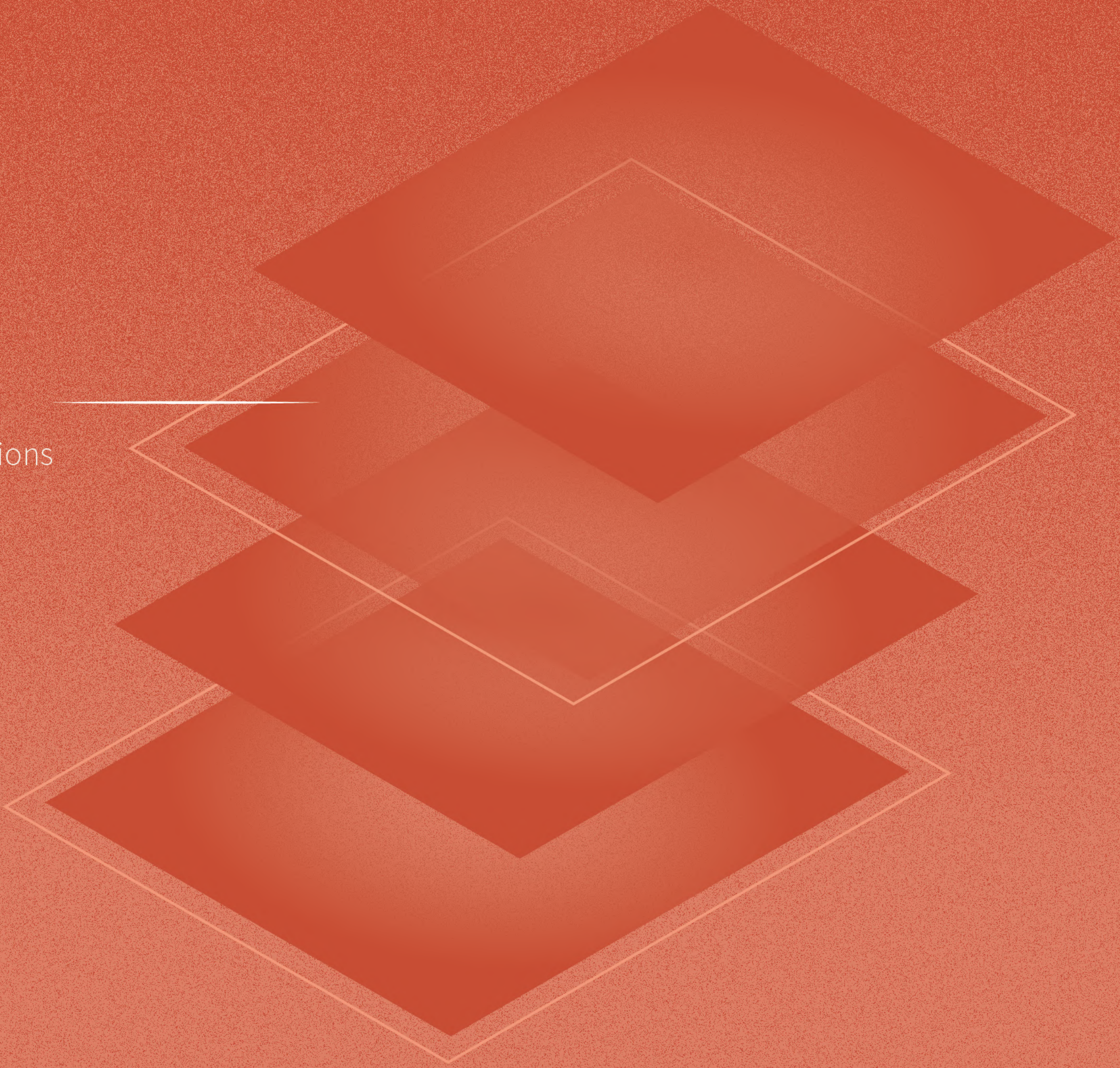
Though still evolving, the OID4VC[111] family of specifications is gaining momentum. Over 25 projects in the Web of Trust Map[112,113,114] are using at least one of the OID4VC protocols:

- OpenID for Verifiable Credential Issuance (OpenID4VCI) [115]
- OpenID for Verifiable Presentations (OpenID4VP) (the only one formally finalized) [116]
- Self-Issued OpenID Provider v2 (SIOPv2) [117]

These protocols extend the widely adopted OpenID Connect framework to support credential exchange in a user-friendly, OAuth2-compliant way. Their adoption signals growing interest in bridging decentralized identity with legacy digital identity infrastructures.

6. REGULATIONS

Regulations outline how decentralized identity should be used and set minimum requirements for trust, privacy, and accountability. While most projects in the Web of Trust Map follow national or regional data protection laws, few legal frameworks focus on digital identity, this chapter highlights three that do.



42
Regulations

6. REGULATIONS

The Web of Trust Map features regulations that govern digital identity as well as those that intersect with privacy and data protection, (e.g. EU's General Data Protection Regulation[118], California's California Consumer Privacy Act [119] South Korea's Personal Information Protection Act[120], Singapore's Personal Data Protection Act [121], given their interconnections.

Although regulations explicitly governing digital identity remain scarce, this section presents three frameworks worth highlighting.

EIDAS - ELECTRONIC IDENTIFICATION, AUTHENTICATION AND TRUST SERVICES REGULATION (REGULATION (EU) NO 910/2014) [122]

The eIDAS Regulation provides a legal framework for secure and interoperable electronic identification and trust services across EU member states, enabling mutual recognition of electronic IDs and qualified trust services, such as electronic signatures. This framework also serves as the foundation for eIDAS 2.0, which updates Regulation (EU) No 910/2014. Although technology-neutral and originally based on centralized trust models, eIDAS established a framework that many projects in the Web of Trust Map have aimed to align with, being the second most followed regulation on the map, with over 50 projects self-assessing as following or endorsing it.

EU DIGITAL IDENTITY REGULATION (EIDAS 2.0) [75]

The revised Regulation (EU) 2024/1183, commonly known as eIDAS 2.0, establishes a framework for a European Digital Identity, introducing the concept of the European Digital Identity Wallet. By 2026, all EU member states are mandated to provide their citizens and residents with a wallet to store and share VC[123]. This regulatory requirement has made wallet development a central focus across Europe. To support its implementation, the EU Digital Identity Toolbox was created[124], including the Architecture and Reference Framework, common standards, technical specifications and guidelines. Within the Web of Trust Map, eIDAS 2.0 emerges as one of the five most connected regulations, linking a broad range of European initiatives and wallet projects working towards compliance.

NATIONAL DIGITAL IDENTITY ACT OF BHUTAN (2023)[125]

On the Web of Trust Map, Bhutan appears as a unique case: the first country to legislate a national framework centered on decentralized identity. Bhutan's National Digital Identity Act establishes a legal foundation for a national digital identity infrastructure that explicitly promotes the use of decentralized public key infrastructure. The Act not only endorses decentralized identity principles but also directly incorporates key technical components such as DID and verifiable digital credentials.

To see all the regulations mapped, refer to the Regulations page in the Web of Trust Map [126].

7. REGIONAL HIGHLIGHTS

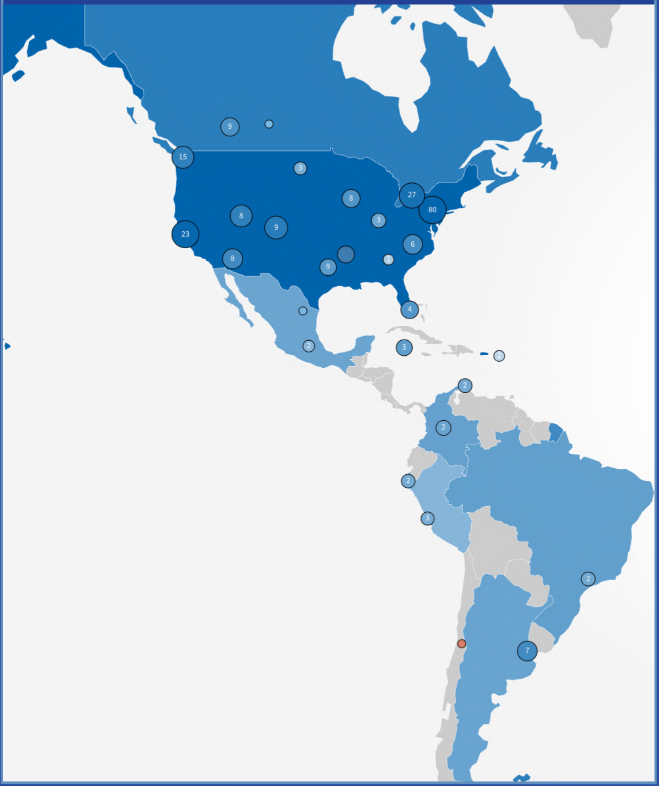
Decentralized identity is active in the entire world. Each region demonstrates efforts to adopt the technology, whether through government-backed initatives or private-sector innovation. The Web of Trust Map demonstrates the global trajectory of decentralzied identity and reveal both the opportunities for growth and the challenges that must be addressed per region.

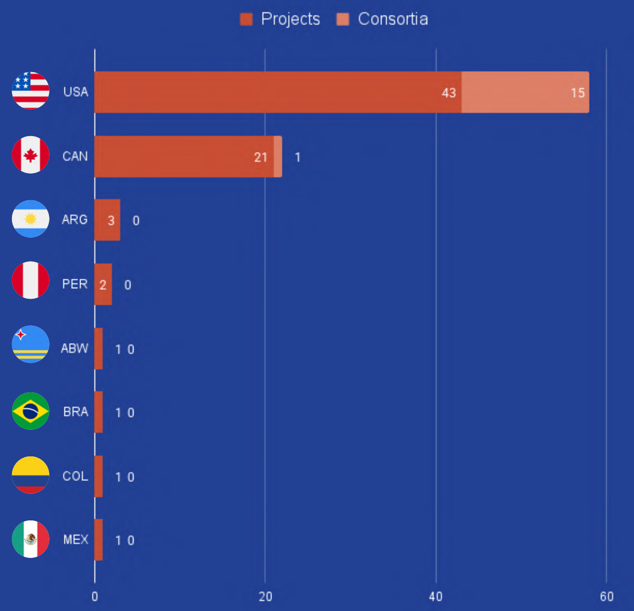
54
Countries
260+
Projects
Consortia - Regulations - Standards - Protocols - DLT Tech - DID Methods - Blockchains - Private Entities - Industries - Private Entities

REGION PROFILE

THE AMERICAS

PROJECTS PER COUNTRY





With over 40 projects, key players in the US are working across sectors like healthcare, government, finance, and education, offering verifiable credentials and self-sovereign identity (SSI) solutions using blockchain and other decentralized technologies.

OVERVIEW

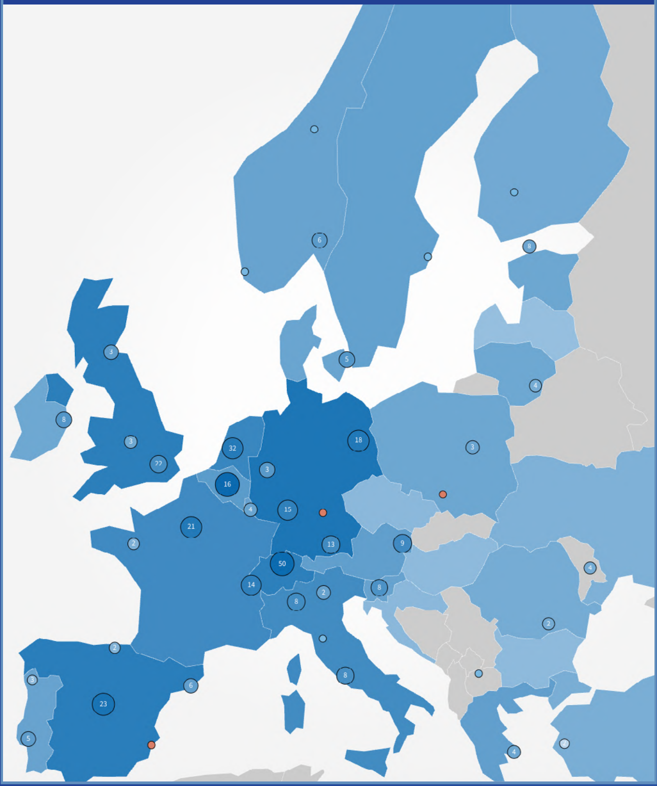
The development of decentralized identity in the Americas is largely concentrated in North America, where Canada and the United States have taken leading roles. Together, they host a significant share of the global decentralized identity ecosystem. Both countries have actively funded initiatives through public agencies and supported the creation of open-source, standards, and consortia, including contributions to W3C, DIF, and ToIP. This sustained investment has led to a growing number of pilot projects, public-private partnerships, and production-ready deployments.

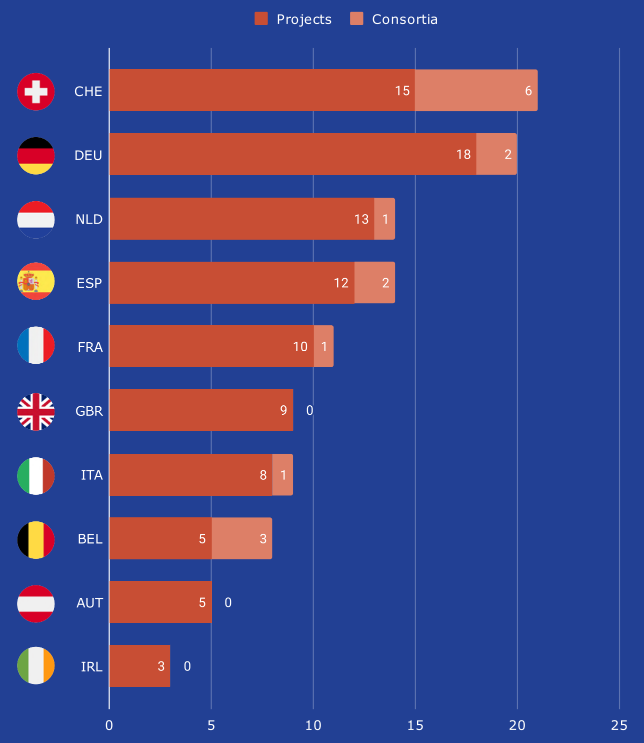
In contrast, Latin America has seen more limited adoption, with fewer than 10 mapped projects across the region. While initiatives in countries like Argentina, Mexico, Colombia, Peru, and Aruba are emerging, the overall development remains in early stages. This disparity may be attributed to a combination of factors, including lower access to digital infrastructure, reduced funding for emerging technologies, and less institutional focus on decentralized models. Nonetheless, the projects that do exist highlight the region's potential and reflect early interest in using decentralized identity to address local challenges around inclusion, trust, and data privacy.

REGION PROFILE

EUROPE

PROJECTS DISTRIBUTION





OVERVIEW

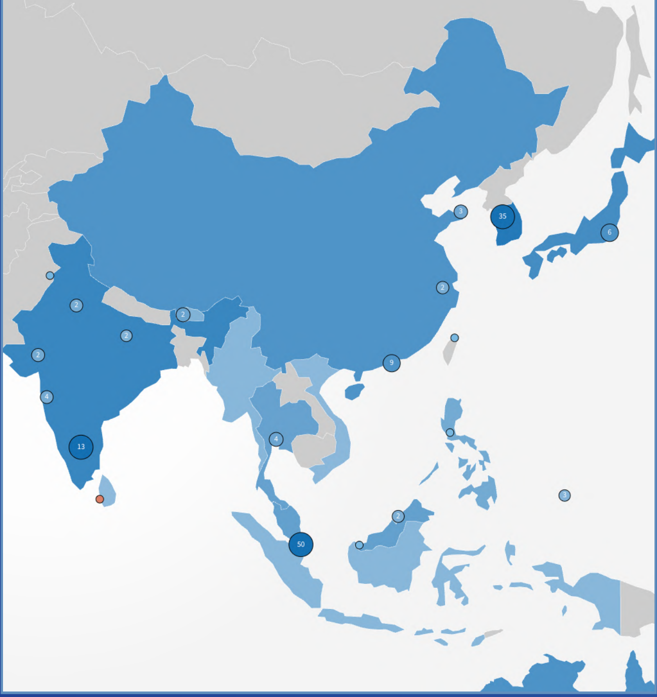
Europe is the most active region in the world when it comes to decentralized identity development, both in terms of the number of projects and the level of public sector involvement. The European Commission has played an essential role in advancing this space through a series of legislative and regulatory initiatives, including eIDAS 2.0, EBSI, and the EUDI Wallet Architecture and Reference Framework. These frameworks are not only creating a common legal basis for digital identity across EU member states but are also directly shaping the design and deployment of technical infrastructure. As a result, Europe is positioned as the leading region for large-scale, government-backed adoption of decentralized identity.

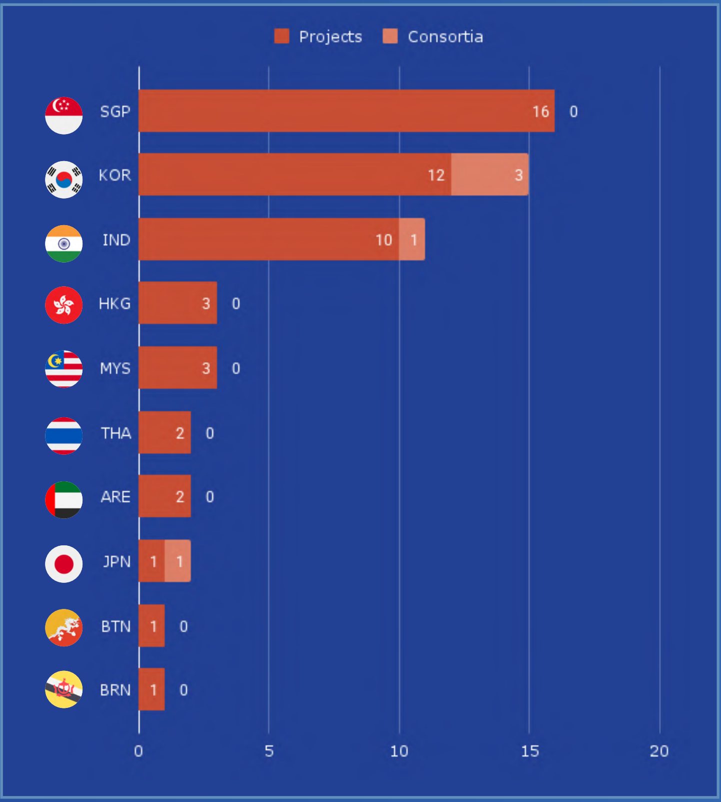
This progress is further reinforced by active public investment at the national level. Governments like Germany, Spain, and the United Kingdom have supported decentralized identity projects through their national innovation and digital transformation agencies, resulting in a high level of project activity and institutional engagement. These efforts have translated into significant ecosystem growth in their respective countries and demonstrate how targeted government funding and strategic alignment can accelerate adoption and innovation in decentralized identity.

REGION PROFILE

ASIA

PROJECTS PER COUNTRY





OVERVIEW

Asia presents a highly diverse landscape for decentralized identity, with distinct levels of development across its subregions: Southeast Asia, East Asia, South Asia, Central Asia, and the Middle East. Each region has taken different approaches to digital identity innovation, shaped by varying levels of digital infrastructure, policy direction, and institutional capacity.

The highest concentration of decentralized identity activity is found in Singapore and South Korea. South Korea has launched projects like Seoul Wallet [22] and B Pass[82], integrating decentralized identity into city services and public infrastructure. Singapore, through its national identity system Singpass, is introducing decentralized features such as sgID and SingVC to support privacy-preserving and interoperable identity use [127, 128, 129]. Both countries demonstrate strong institutional backing and a clear direction toward nationwide adoption.

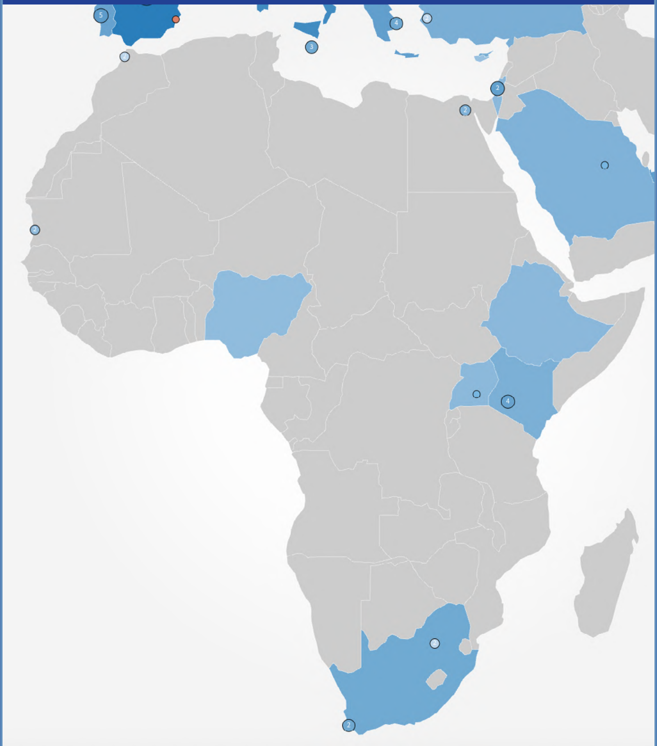
In South Asia, India and Bhutan stand out as regional leaders in technological adoption. India hosts a growing ecosystem of decentralized identity projects, including MOSIP[130], and private-sector developments like AyanWorks' Sovio Wallet (formerly Adeya Wallet)[131] and CREDEBL[128], now maintained by the LFDT's initiative. Meanwhile, Bhutan represents a major milestone in global adoption as the first country to implement a decentralized digital public infrastructure at the national level, backed by the National Digital Identity Act of 2023 [125].

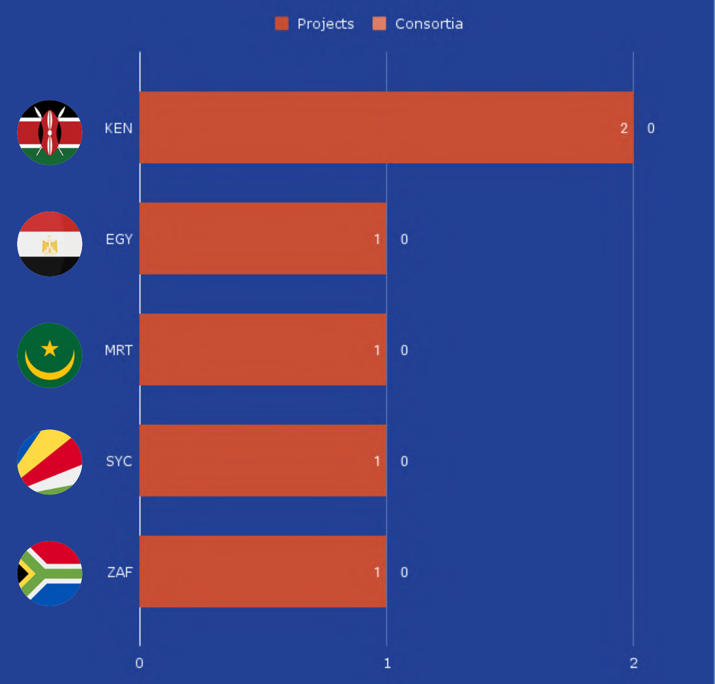
While the Middle East hosts at least four active decentralized identity initiatives, adoption in the region remains limited compared to other parts of Asia. Nonetheless, these early efforts signal a growing institutional interest in verifiable credentials and digital identity modernization. In contrast, Central Asia showed no mapped projects in the Web of Trust Map, suggesting that decentralized identity adoption in that subregion has yet to take off.

REGION PROFILE

AFRICA

PROJECTS PER COUNTRY





OVERVIEW

Decentralized identity adoption in Africa is still emerging, with fewer than 10 active projects across countries like Kenya, Mauritania, Egypt, Seychelles, and South Africa. Much of the region's activity is supported by foreign-led initiatives and humanitarian pilots, rather than domestic public-sector programs or private initiatives.

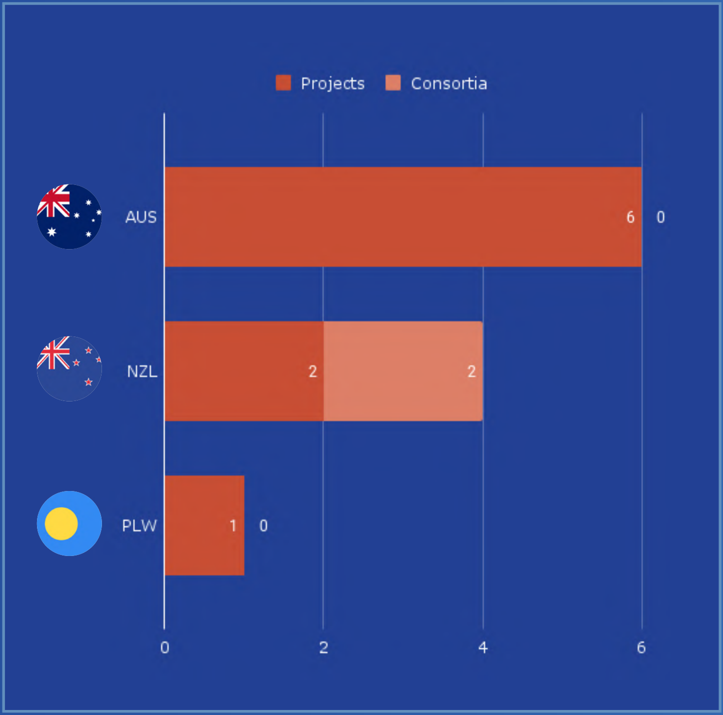
DIF has launched an Africa Special Interest Group to accelerate the adoption of decentralized identity technologies across the continent by opening space for collaboration, knowledge sharing, and regional alignment[133]. Humanitarian organizations like the International Federation of Red Cross and Red Crescent Societies are also exploring decentralized identity for aid distribution and crisis response[134]. Pilots such as NeoLink[135], focused on healthcare identity, and the Kiva Protocol in Sierra Leone, which aimed to build a blockchain-based credit bureau, have tested the feasibility of the technology in real-world contexts. However, the Kiva Protocol was eventually discontinued, highlighting the challenges of scaling such solutions without sustained government support and infrastructure readiness[136].

Similar to Latin America, the region faces challenges such as limited digital infrastructure, funding constraints, and institutional readiness, which have slowed large-scale development. The long-term success of decentralized identity in Africa will depend on overcoming these barriers and transitioning from pilot to sustainable deployment.

REGION PROFILE

OCEANIA

PROJECTS PER COUNTRY



OVERVIEW

Adoption in Oceania is growing steadily, supported by active government involvement. While the number of initiatives is modest compared to other regions, the level of innovation and institutional engagement, particularly in Australia and New Zealand, positions the region as an emerging player in the space.

In Australia, the federal government and other government agencies support private sector initiatives such as Connect ID, Meeco, and ShareRing [137, 138, 139]. The New South Wales Government has also rolled out a Digital ID and Wallet through the Service NSW platform, providing citizens with a secure way to store and use VC for public services [140]. In New Zealand, the project Āhau [141] offers a culturally focused platform to help the Māori and tribal communities preserve and manage their histories using decentralized identity tools. Meanwhile, the Republic of Palau has launched PalauID [21], a national resident ID built on verifiable credentials.

In early 2024, a Cross-Border Working Group [142] was established by representatives from Japan and Australia to explore the technical, legal, and commercial requirements for seamless digital identity and data sharing across borders. The initiative, involving organizations like Meeco, ConnectID, Mitsubishi UFJ Financial Group, DNP Group, National Australia Bank, and Commonwealth Bank of Australia, reflects growing efforts to build interoperable identity infrastructure beyond national boundaries, recognizing the need for shared standards in an increasingly connected digital ecosystem.

While still developing, the region shows consistent progress driven by public-private partnerships, cultural relevance, and government involvement, indicating a strong foundation for further decentralized identity adoption.

8. CONCLUSION

CONCLUSION

The decentralized identity ecosystem has grown substantially in experimentation since 2020, with projects piloted across health, education, finance, government, and even creative industries. Regardless, the ecosystem today is heavily shaped by government funding and mandates, rather than market-driven demand or organic adoption. While governments, particularly in Europe and parts of Asia, continue to invest in pilots and regulatory frameworks, the private sector has shown little evidence of sustainable business models (e.g., Sovrin, Kiva Protocol, Evernym, Trinsic). Of the promising examples, most of the actual applications in the field tend to use whatever is simple (did:key), which avoids solving many of the central problems decentralized identity set out for.

Early decentralized visions that relied on blockchains and other decentralized public key infrastructures as verifiable data registries are fading. DID methods illustrate this shift clearly: ledger-based approaches such as did:sov and did:indy are in decline, while web-based identifiers like did:web and did:webvh are gaining prominence because of their simplicity and compatibility to existing infrastructure. However, this convenience comes at the cost of greater centralization, reduced security, and a higher risk of surveillance [106]. Government frameworks are reinforcing this trajectory, eIDAS 2.0's evolution and Switzerland's adoption of did:webvh for its eID [105] both exemplify how regulatory choices are accelerating the move toward centralized, less secure implementations [106] in practice.

> *IN REALITY, WEB BASED DID METHODS **GIVE UP ON DECENTRALIZATION, CONTROL, PRIVACY AND SECURITY** TO THE SAME LEVEL THAT TODAY'S FEDERATED IDENTITY SOLUTIONS HAVE GIVEN UP ON THEM.* [106]

GEORG GREVE, CEO OF VEREIGN AND FOUNDER OF FREE SOFTWARE FOUNDATION EUROPE (FSFE)

The vLEI[37] remains a notable exception to the rule, in their adoption of KERI, which is an emerging decentralized identity stack. KERI introduces an alternative approach which enables self determination of both individuals and institutions while also allowing for interoperability, without using blockchain or centralized points of failure. The capabilities of KERI are also being felt in places like Utah, where their introduction of SEDI (state endorsement digital identity) via SB 260 necessitates the technical capabilities that currently only KERI can provide.

Globally, the landscape remains highly uneven. Europe, North America, and parts of East and Southeast Asia are driving adoption, supported by strong institutions, regulatory frameworks, and significant financial backing. Yet, in Latin America, Africa, Central Asia, and much of the Middle East, adoption remains limited to isolated pilots or foreign-led experiments, constrained by weaker infrastructure, limited institutional support, and fewer funds. This disparity demonstrates how much decentralized identity remains a story of institutional capacity and resource concentration rather than organic innovation.

The Web of Trust Map reveals an ecosystem at a crossroads. The founding ideals of decentralization, privacy-preserving, user-controlled, and censorship-resistant identity systems, remain largely unfulfilled. In practice, the field is moving toward government-backed, regulator-shaped systems that integrate some elements of decentralized identity but function in centralized ways.

This regulator-driven shift is reinforced by the absence of viable business models beyond government adoption. Most private-sector players now depend on public contracts or raise capital on the narrative of future regulatory mandates driving use of their products, leaving little room for true decentralized innovation. **Without sustainable models, genuine interoperability, or renewed commitment to its original principles, decentralized identity risks consolidating into yet another layer of state-managed digital infrastructure, centralized and dependent on single points of failure.**

GET INVOLVED

The Web of Trust Map is an evolving resource that benefits from contributions across the decentralized identity community. There are several ways individuals and organizations can help improve and expand the dataset:

SUBMIT NEW PROJECTS

If you are aware of a decentralized identity initiative that fits the scope of the Web of Trust Map but is not yet included, we welcome suggestions. All project submissions are reviewed to ensure they meet the map's inclusion criteria.

SUBMIT NEW PROJECTS HERE

Contribute or Correct Information

If you notice missing, outdated, or inaccurate information about a project, consortium, or connection, your contributions are valuable. On each profile page, you'll find a "Suggest Changes" button that allows you to submit additions, edits, or removal requests. All submissions are reviewed and verified before any updates are made to the dataset.

Share General Feedback

General feedback is encouraged, whether related to the structure of the map, areas for improvement, data quality, or potential new features. Input from users helps shape future iterations of the project.

SUBMIT FEEDBACK HERE

CITE THE WEB OF TRUST

All data on the Web of Trust is open data and available at no cost to the general public.

You are free to:

- Share — copy and redistribute the material in any medium or format for any purpose, including commercial.
- Adapt — remix, transform, and build upon the material for any purpose, including commercial.

Under the following terms:

- Attribution — You must give appropriate credit, provide a link to the Web of Trust Map, and indicate whether changes were made.
- No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything that the license permits.

SOURCES

1. Beduschi A. Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. Data & Policy. 2021;3:e15. Available from: https://doi.org/10.1017/dap.2021.15

2. O'Halloran D, George M, Duda C, Leong C, Johnson J, Keeling J. Digital Identity Ecosystems: Unlocking New Value [Internet]. Switzerland: World Economic Forum; 2021 Sep [cited 2025 July]. Available from: https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf

3. Air France tests the ICC AOK Pass solution for digitizing COVID-19 test results. Air France; 2021 Feb 17 [cited 2025 Aug]. Available from: https://corporate.airfrance.com/en/press-releases/air-france-tests-icc-aok-pass-solution-digitizing-covid-19-test-results

4. de Juniac A, Careen N. IATA Media Update on COVID-19. International Air Transport Association; 2020 Dec 16 [cited 2025 July]. Available from: www.iata.org/contentassets/43b7bfbb70ad4db18d47c41f34c9a38e/iata-travel-pass-media-briefing.pdf

5. Korea Disease Control and Prevention Agency. First In Korea Digital Vaccination Certificate (COOV) [Internet]. Innovation 24; 2023 Dec 29 [cited 2025 July]. Available from: https://www.innovation.go.kr/en/bbs/govFirstBest/govFirstBestDetail.do?bbsId=B0000079&nttId=15790

6. Key State Capital. Sovrin Foundation [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/sovrin_foundation-417

7. Key State Capital. Evernym [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/evernym-266

8. Key State Capital. Lissi ID-Wallet [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/lissi_id-wallet-8

9. Key State Capital. DIDI [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/didi-166

10. Key State Capital. Mobile ID [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/mobile_id-145

11. Key State Capital. HPEC [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/hpec-201

12. Home [Internet]. Bio Passport. BIONES PTE. LTD.; [cited 2025 Aug]. Available from: https://biopassport.io/

13. Key State Capital. IBM Digital Credentials [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/ibm_digital_credentials-210

14. Key State Capital. Hyland Experience Credentials [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/hyland_experience_credentials-237

15. Key State Capital. DCC - Digital Credentials Consortium [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/dcc_-_digital_credentials_consortium-435

16. Key State Capital. MyID by Parameta [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/myid_by_parameta-134

17. Key State Capital. ConnectID [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/connectid-190

18. THEPOL Intro [Internet]. THEPOL. CPLABS, Inc.; 2023 [cited 2025 Aug]. Available from: https://thepol.com/en/

19. Key State Capital. Bhutan National Digital Identity [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/bhutan_national_digital_identity-182

20. Key State Capital. sgID [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/sgid-123

21. Key State Capital. Palau ID [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/palau_id-185

22. Key State Capital. Seoul Wallet [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/seoul_wallet-138

23. Key State Capital. Quark ID [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/quark_id_wallet-15

24. Key State Capital. Service NSW [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/service_nsw-183

25. Key State Capital. MOBI - Mobility Open Blockchain Initiative [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/mobi_-_mobility_open_blockchain_initiative-414

26. Key State Capital. MOBIX [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/mobix-338

27. Key State Capital. Cardossier [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/cardossier-358

28. Key State Capital. Domi [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/domi-335

29. Key State Capital. The Creative Passport [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/the_creative_passport-308

30. Key State Capital. Cheqd [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/cheqd-403

31. Key State Capital. Indicio Proven [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/indicio_proven-202

32. Key State Capital. Privado ID (formerly Polygon ID) [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/privado_id_(formerly_polygon_id)-198

33. Global Legal Entity Identifier Foundation. Introducing the vLEI Ecosystem Governance Framework [Internet]. Organizational Identity. [cited 2025 Sep]. Available from: https://www.gleif.org/en/organizational-identity/introducing-the-verifiable-lei-vlei/

introducing-the-vlei-ecosystem-governance-framework

34. Key State Capital. Global Legal Entity Identifier Foundation [Internet]. Web of Trust; 2025 [cited 2025 Sep]. Available from: https://www.weboftrust.org/project/gleif_-_global_legal_entity_identifier_foundation-313

35. Key State Capital. vLEI - verifiable LEI [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/standard/vlei_-_verifiable_lei-104

36. Key State Capital. KERI - Key Event Receipt Infrastructure [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/standard/keri_-_key_event_receipt_infrastructure-2

37. Key State Capital. vLEI - The Rise of Organizational Digital Identity [Internet]. 2025 [cited 2025 Sep]. Available from: https://www.keystate.capital/post/report-vlei-the-dawn-of-organizational-digital-identity

38. Sporny M. Verifiable Claims Working Group Proposal [Internet]. World Wide Web Consortium: Verifiable Claims Task Force; 2016 Jul [cited 2025 Aug]. Available from: https://lists.w3.org/Archives/Public/public-credentials/2016Jun/att-0235/VerifiableClaimsWGProposal.pdf

39. Key State Capital. W3C - World Wide Web Consortium [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/w3c_-_world_wide_web_consortium-177

40. Key State Capital. DIF - Decentralized Identity Foundation [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/dif_-_decentralized_identity_foundation_(consortia)-175

41. Key State Capital. LFDT - LF Decentralized Trust [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/lfdt_-_lf_decentralized_trust-440

42. Key State Capital. OWF - Open Wallet Foundation [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/owf_-_open_wallet_foundation-415

43. Key State Capital. Trust Over IP Foundation [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/trust_over_ip_foundation-167

44. Key State Capital. ACDC - Authentic Chained Data Containers [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/standard/acdc_-_authentic_chained_data_containers-1

45. Key State Capital. INATBA - International Association for Trusted Blockchain Applications [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/inatba_-_international_association_for_trusted_blockchain_applications-408

46. Key State Capital. Ayra Association [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/ayra_association-459

47. Key State Capital. OpenID for Verifiable Credentials [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/openid_for_verifiable_credentials_-_oid4vc-406

48. Key State Capital. DIDAS - Digital Identity and Data Sovereignty Association [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/didas_-_digital_identity_and_data_sovereignty_association-432

49. Key State Capital. DIACC - Digital ID and Authentication Council of Canada [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/diacc_-_digital_id_and_authentication_council_of_canada-409

50. Digital ID & Authentication Council of Canada. Overview [Internet]. Diacc.ca; 2021 [cited 2025 Aug]. Available from: https://diacc.ca/overview/

51. EU Digital Identity Wallet Pilot implementation [Internet]. European Commission; 2023 [cited 2025 Aug]. Available from: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

52. Key State Capital. Potential [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/potential-425

53. 19 European Member States and Ukraine [Internet]. Potential - For European Digital Identity [cited 2025 Aug]. Available from: https://www.digital-identity-wallet.eu/about-us/19-european-member-states-and-ukraine/

54. Key State Capital. EWC - EU Digital Identity Wallet Consortia [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/ewc_-_eu_digital_identity_wallet_consortia-420

55. The EU Digital Identity Wallet Consortium [Internet]. EU Digital Identity Wallet Consortium [cited 2025 Aug]. Available from: https://eudiwalletconsortium.org/#:~:text=all%2027%20EU%2DMember%20States%20and%20partners%20from%20other%20countries

56. Key State Capital. NOBID Consortium [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/nobid_consortium-438

57. Welcome to the NOBID Consortium [Internet]. NOBID Consortium; [cited 2025 Aug]. Available from: https://www.nobidconsortium.com/#:~:text=We%20are%20a%20set%20of%20Nordic%20and%20Baltic%20countries%20who%2C%20together%20with%20Italy%20and%20Germany%2C%20are%20developing%20a%20large%2Dscale%20pilot%20for%20the%20payment%20use%20case%20in%20the%20EU%20Digital%20Wallet.

58. Key State Capital. DC4EU Consortium [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/dc4eu_consortium-418

59. Consortium - DC4EU [Internet]. DC4EU; 2024 [cited 2025 Aug]. Available from: https://www.dc4eu.eu/consortium/#:~:text=DC4EU%20involves%2022%20EU%20Member%20States%20plus%20Norway%2C%20Ukraine%20and%20Switzerland.

60. esatus AG. "SSI for Germany" Consortium starts decentralized identity network [Internet]. Pressebox; 2020 Aug 31 [cited 2025 Aug]. Available from: https://www.pressebox.com/pressrelease/esatus-ag/SSI-for-Germany-Consortium-starts-decentralized-identity-network/boxid/1020932

61. Key State Capital. Bundesagentur für Sprunginnovationen GmbH [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/entity/bundesagentur_f%C3%BCr_sprunginnovationen_gmbh-5652

62. Key State Capital. Bundesdruckerei Gruppe GmbH [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/entity/bundesdruckerei_gruppe_gmbh-2697

63. Key State Capital. Federal Ministry of Education and Research [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from:

https://www.weboftrust.org/entity/federal_ministry_of_education_and_research-3098

64. Key State Capital. European Commission [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/entity/european_commission-649

65. Key State Capital. European Blockchain Service Infrastructure [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/entity/european_blockchain_service_infrastructure-1658

66. Key State Capital. eIDAS 2.0 - European Digital Identity (EUDI) Regulation [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/reg/eidas_2.0_-_electronic_identification,_authentication_and_trust_services_regulation_2.0-39

67. Transport Canada. The Government of Canada to test cutting-edge technologies to support secure and seamless global travel for air passengers [Internet]. Switzerland: Government of Canada; 2018 Jan 25 [cited 2025 Aug]. Available from: https://www.canada.ca/en/transport-canada/news/2018/01/the_government_ofcanadatotestcutting-edgetechnologiestosupportse.html

68. Lemoie K, Soares L. Connected Impact: Unlocking Education and Workforce Opportunity Through Blockchain [Internet]. Washington, DC: American Council on Education; 2020 [cited 2025 Aug]. Available from: https://www.acenet.edu/Documents/ACE-Education-Blockchain-Initiative-Connected-Impact-June2020.pdf

69. ATB Ventures. ATB Ventures is Working with the Government of Canada to Power its National Digital Trust Proof of Concept [Internet]. PR Newswire; 2022 Feb 15 [cited 2025 Aug]. Available from: https://www.prnewswire.com/news-releases/atb-ventures-is-working-with-the-government-of-canada-to-power-its-national-digital-trust-proof-of-concept-301482547.html

70. Alusa S. INATBA Launches Task Force to Drive the Future of Digital Credentials! [Internet]. INATBA; 2023 [cited 2025 Aug]. Available from: https://inatba.org/news/digital-credentials-task-force-of-inatba/

71. Key State Capital. Government of British Columbia [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/entity/government_of_british_columbia-413

72. Key State Capital. BC Wallet [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/bc_wallet-59

73. Key State Capital. OrgBook BC [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/orgbook_bc-79

74. Key State Capital. Ontario's Digital ID [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/ontario's_digital_id-71

75. Key State Capital. Government of Ontario [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/entity/government_of_ontario-403

76. Key State Capital. Korea Internet & Security Agency [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/entity/korea_internet_&_security_agency-68

77. Key State Capital. Ministry of Science and ICT [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/entity/ministry_of_science_and_ict-67

78. Key State Capital. Initial DID Association [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/initial_did_association-421

79. Key State Capital. B Pass [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/b_pass-24

80. Key State Capital. Initial [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/initial-143

81. Key State Capital. Wepublic Wallet [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/wepublic_wallet-140

82. News Release: DHS S&T Awards $1.3 Million to Small Businesses for Cyber Security Research and Development [Internet]. U.S. Department of Homeland Security. DHS Science & Technology Press Office; 2016 Aug 12 [cited 2025 Aug]. Available from: https://www.dhs.gov/archive/science-and-technology/news/2016/08/12/news-release-dhs-st-awards-13-million-small-businesses-cyber-security-research-and

83. Key State Capital. United States Department of Homeland Security [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/entity/united_states_department_of_homeland_security-434

84. Verifiable Credentials Working Group - Participants [Internet]. World Wide Web Consortium (W3C); 2021 [cited 2025 Aug]. Available from: https://www.w3.org/groups/wg/vc/participants/?sortaff=1

85. Hendrickson L. The Importance of Interoperability in Digital Identity [Internet]. Identity; 2024 Oct 30 [cited 2025 Aug]. Available from: https://www.identity.com/the-importance-of-interoperability-in-digital-identity/

86. Key State Capital. Ethereum [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/dltinstance/ethereum-2

87. Codezeros. Securing Identities Through Ethereum's Role in the Future of Digital Identity Management [Internet]. Medium; 2024 Oct 3 [cited 2025 Aug]. Available from: https://codezeros.medium.com/securing-identities-through-ethereums-role-in-the-future-of-digital-identity-management-c7bc03200e77

88. Key State Capital. Sovrin [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/dltinstance/sovrin-32

89. Sovrin Governance Framework [Internet]. Sovrin [cited 2025 Aug]. Available from: https://sovrin.org/library/sovrin-governance-framework/

90. Fulling S, Windley P, Law J, George N. Indy Project Proposal [Internet]. 2017 Mar 17 [cited 2025 Aug]. Available from: https://docs.google.com/document/d/1YzXz0aM8w7kSp3_ao3ue9tOFwK9paofXbtBptR1Jucg/edit?tab=t.0

91. Curran S. Sovrin Foundation MainNet Ledger Shutdown Likely on or before March 31, 2025 [Internet]. Sovrin; 2025 Feb 8 [cited 2025 Aug]. Available from: https://sovrin.org/sovrin-foundation-mainnet-ledger-shutdown-likely-on-or-before-march-31-2025/

92. Key State Capital. EBSI Network [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/dltinstance/ebsi_network-13

93. Key State Capital. Polygon [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/dltinstance/polygon-3

94. Ethereum vs Polygon: Scaling, Collaboration, and the Future of Blockchain [Internet]. Crypto.com; 2025 Feb 26 [cited 2025 Aug]. Available from: https://crypto.com/en/university/ethereum-vs-polygon-scaling-collaboration-and-the-future-of-blockchain

95. Introducing Privado ID: Moving Beyond Polygon to Deliver Independent, Privacy-Preserving Identity Solutions [Internet]. Privado.id; 2024 Jun 13 [cited 2025 Aug]. Available from: https://www.privado.id/blog/introducing-privado-id-moving-beyond-polygon-to-deliver-independent-privacy-preserving-identity-solutions

96. Key State Capital. Indicio Network [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/dltinstance/indicio_network-14

97. #HyperledgerIdentity round-up: A cross section of production digital identity solutions built using Hyperledger technologies [Internet]. LF Decentralized Trust; 2022 Sep 28 [cited 2025 Aug]. Available from: https://www.lfdecentralizedtrust.org/blog/2022/09/28/hyperledgeridentity-round-up-a-cross-section-of-production-digital-identity-solutions-built-using-hyperledger-technologies

98. Sporny M, Longley D, Sabadello M, Reed D, Steele O, Allen C. Decentralized Identifiers (DIDs) v1.0 [Internet]. World Wide Web Consortium (W3C); 2022 Jul 19 [cited 2025 Aug]. Available from: https://www.w3.org/TR/did-1.0/#methods

99. Key State Capital. DID Methods [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/topo/didmethod

100. Longley D, Zagidulin D, Sporny M. The did:key Method v0.7 [Internet]. W3C Credentials Community Group; 2025 Mar 26 [cited 2025 Aug]. Available from: https://w3c-ccg.github.io/did-key-spec/

101. Gribneau C, Prorock M, Steele O, Terbu O, Xu M, Zagidulin D. did:web Method Specification Unofficial Draft [Internet]. W3C Credentials Community Group; 2024 Jul 31 [cited 2025 Aug]. Available from: https://w3c-ccg.github.io/did-method-web/

102. Sovrin DID Method Specification. W3C Editor's Draft [Internet]. World Wide Web Consortium (W3C); 2025 Apr 03 [cited 2025 Aug]. Available from: https://sovrin-foundation.github.io/sovrin/spec/did-method-spec-template.html

103. Indy DID Method Specification [Internet]. Hyperledger [cited 2025 Aug]. Available from: https://hyperledger.github.io/indy-did-method/

104. Deventer O, Lundkvist C, Csernai M, Den Hartog K, Sabadello M, Gisolfi D, et al. Peer DID Method Specification [Internet]. Decentralized Identity Foundation; [cited 2025 Aug]. Available from: https://identity.foundation/peer-did-method-spec/

105. Federal Office of Justice. Swiss e-ID and trust infrastructure: Roadmap (initial version - deprecated) [Internet]. GitHub. Swiss E-ID Ecosystem; 2024 [cited 2025 Aug]. Available from: https://github.com/e-id-admin/open-source-community/blob/main/tech-roadmap/tech-roadmap.md

106. Georg GCF. Self Sovereign Identity: Over before it started? [Internet]. Medium; 2024 Dec 22 [cited 2025 Aug]. Available from: https://ggreve.medium.com/self-sovereign-identity-over-before-it-started-661b4b0dbdc6

107. Key State Capital. Standards/Protocols [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/topo/Standard

108. Sporny M, Longley D, Chadwick D, Herman I. Verifiable Credentials Data Model v2.0 [Internet]. World Wide Web Consortium (W3C); 2025 May 15 [cited 2025 Aug]. Available from: https://www.w3.org/TR/vc-data-model-2.0/

109. Key State Capital. W3C Verifiable Credentials Data Model [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/standard/w3c_verifiable_credentials_data_model-12

110. Key State Capital. W3C Decentralized Identifiers (DIDs) [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/standard/w3c_decentralized_identifiers_(dids)-3

111. OpenID for Verifiable Credentials - Overview [Internet]. OpenID Foundation; [cited 2025 Aug]. Available from: https://openid.net/sg/openid4vc/

112. Key State Capital. OpenID for Verifiable Credential Issuance - OID4VCI [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/standard/openid_for_verifiable_credential_issuance_-_oid4vci-98

113. Key State Capital. OpenID for Verifiable Presentations - OID4VP [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/standard/openid_for_verifiable_presentations_-_oid4vp-99

114. Key State Capital. Self-Issued OpenID Provider v2 - SIOP v2 [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/standard/self-issued_openid_provider_v2_-_siop_v2-100

115. Lodderstedt T, Yasuda K, Looker T. OpenID for Verifiable Credential Issuance - Editor's draft [Internet]. OpenID Foundation; 2025 [cited 2025 Aug]. Available from: https://openid.github.io/OpenID4VCI/openid-4-verifiable-credential-issuance-wg-draft.html

116. Terbu O, Lodderstedt T, Yasuda K, Fett D, Heenan J. OpenID for Verifiable Presentations 1.0 [Internet]. OpenID Foundation; 2025 Jul 9 [cited 2025 Aug]. Available from: https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html

117. Yasuda K, Jones M, Lodderstedt T. Self-Issued OpenID Provider v2 - draft 13 [Internet]. OpenID Foundation; 2024 Feb 17 [cited 2025 Aug]. Available from: https://openid.github.io/SIOPv2/openid-connect-self-issued-v2-wg-draft.html

118. Key State Capital. EU GDPR - EU General Data Protection Regulation [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/reg/eu_gdpr_-_eu_general_data_protection_regulation-50

119. Key State Capital. CCPA - California Consumer Privacy Act [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/reg/ccpa_-_california_consumer_privacy_act-6

120. Key State Capital. PIPA - Personal Information Protection Act [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/reg/pipa_-_personal_information_protection_act-2

121. Key State Capital. PDPA - Personal Data Protection Act [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/reg/pdpa_-_personal_data_protection_act-17

122. Key State Capital. eIDAS - electronic IDentification, Authentication and trust Services Regulation [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/reg/eidas_-_electronic_identification,_authentication_and_trust_services_regulation-1

123. EU Digital Identity Wallet. The Digital Identity Regulation Enters into Force [Internet]. European Commission;

2024 May 21 [cited 2025 Aug]. Available from: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/736100362/The+Digital+Identity+Regulation+Enters+into+Force

124. EU Digital Identity Wallet Toolbox [Internet]. European Commission [cited 2025 Aug]. Available from: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox

125. Key State Capital. NDI Act 2023 - National Digital Identity Act 2023 [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/reg/ndi_act_2023_-_national_digital_identity_act_2023-65

126. Key State Capital. Regulations [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/topo/Regulation

127. Tay S. Exclusive: How Singapore is building a privacy-based digital ID [Internet]. GovInsider; 2020 Sep 27 [cited 2025 Aug]. Available from: https://govinsider.asia/intl-en/article/exclusive-how-singapore-is-building-a-privacy-based-digital-id

128. IMDA. The SingVC Sandbox is officially live, marking a major milestone for digital identity and verifiable credentials [Internet]. Linkedin; 2025 [cited 2025 Aug]. Available from: https://www.linkedin.com/posts/imdasg_singvc-sandbox-activity-7342853957150511104-A1xm/

129. Digital Utilities [Internet]. Infocomm Media Development Authority; [cited 2025 Aug]. Available from: https://www.imda.gov.sg/how-we-can-help/digital-utilities

130. Key State Capital. MOSIP - Modular Open Source Identity Platform [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/mosip_-_modular_open_source_identity_platform-32

131. AYANWORKS Technology Solutions Private Limited. Sovio Wallet [Internet]. [cited 2025 Aug]. Available from: https://www.ayanworks.com/products/adeya

132. Home [Internet]. CREDEBL. CREDEBL a Series of LF Projects, LLC; [cited 2025 Aug]. Available from: https://credebl.id/

133. DIF Africa Special Interest Group [Internet]. Decentralized Identity Foundation [cited 2025 Sep 15]. Available from: https://identity.foundation/special-interest-groups/africa

134. International Federation of Red Cross and Red Crescent Societies, Kenya Red Cross Society. Set-Up Guide: DIGID Platform [Internet]. DIGID Consortium; 2021 Jun [cited 2025 Aug]. Available from: https://interoperability.ifrc.org/wp-content/uploads/2023/11/DIGIDSetUpGuide31052021.pdf

135. Key State Capital. NeoLinkID [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/neolinkid-83

136. Heiring B. Kiva announces the sunset of Kiva Protocol [Internet]. Kiva; 2022 May 13 [cited 2025 Aug]. Available from: https://www.kiva.org/blog/sunset-kiva-protocol

137. Macdonald A. Australia accredits eftpos for digital identity exchange [Internet]. Biometric Update; 2021 Sep 28 [cited 2025 Aug]. Available from: https://www.biometricupdate.com/202109/australia-accredits-eftpos-for-digital-identity-exchange

138. Dai Nippon Printing Co., Ltd., MUFG Bank, Ltd. DNP and MUFG Aiming to Commercialize Digital IDs: Successfully conducted connection tests with Australian firms [Internet]. Meeco; 2024 Jun 3 [cited 2025 Aug]; Available from: https://www.meeco.me/news/dnp-and-mufg-aiming-to-commercialize-digital-ids-successfully-conducted-connection-tests-with-australian-firm

139. Mayhew S. ShareRing joins Australia's age assurance technology trial [Internet]. Biometric Update; 2025 Apr 9 [cited 2025 Sep 15]. Available from: https://www.biometricupdate.com/202504/sharering-joins-australias-age-assurance-technology-trial

140. NSW Digital ID. NSW Digital ID will make government more accessible. NSW Government [Internet]. NSW Government; 2023 Jun 6 [cited 2025 Aug]. Available from: https://www.nsw.gov.au/nsw-government/digital-identity-and-cybersecurity/nsw-digital-id/nsw-digital-id-journey/nsw-digital-id-will-make-government-more-accessible

141. Key State Capital. Āhau [Internet]. Web of Trust; 2025 [cited 2025 Aug]. Available from: https://www.weboftrust.org/project/%C4%81hau-189

142. Cross-Border Working Group. Enabling Interoperable and Scalable Cross-Border Digital Identity [Internet]. Meeco; 2024 [cited 2025 Aug]. Available from: https://www.meeco.me/cross-border