GBBC
Global Blockchain
Business Council

STANDALONE REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 5.0

DECEMBER 2024

DIGITAL IDENTITY AND BLOCKCHAIN: USE CASES, DIGITAL PUBLIC INFRASTRUCTURE MODELS, AND KEY PRINCIPLES FOR GROWTH

GBBC GSMI 5.0

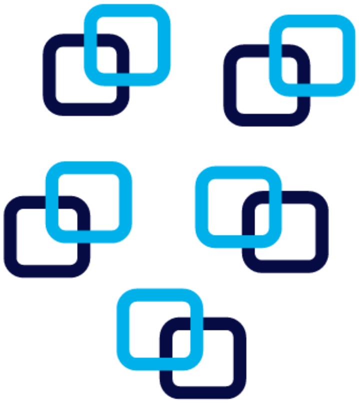
GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland

GSMI 5.0 IN-DEPTH REPORT

DIGITAL IDENTITY AND BLOCKCHAIN: USE CASES, DIGITAL PUBLIC INFRASTRUCTURE MODELS, AND KEY PRINCIPLES FOR GROWTH



EXECUTIVE SUMMARY

Digital Identity systems are essential for services that empower individuals to securely prove their identity and access a wide range of public and private services. Within a dynamic data economy built around data exchange, digital identities must work seamlessly across national boundaries and jurisdictions, be interoperable and resilient, and enable individuals to govern their digital identity.

A robust digital identity is a necessity and a catalyst for innovation. It paves the way for transformative use cases in decentralized finance, social services, healthcare, and other domains. The emergence of the need for a high-assurance digital identity in many countries is a testament to its potential. The current state of affairs in these use cases is plagued by data duplication, low data quality, loss and leakage during service delivery, loss of benefits, exclusion, and forgery of digital identity. A robust digital identity can address these issues and unlock possibilities.

INTRODUCTION

It is essential to highlight that digital identities are not limited to individuals. Businesses also use digital identities to establish bona fide relationships and exchange verifiable information. While the term "digital identity" implies a transformation from traditional forms of identification and authentication (such as printed ID cards, passports, etc.), there is much confusion around the definition of the term itself.

The Wikipedia entry[1] for the term describes it as

*"A **digital identity** is data stored on computer systems relating to an individual, organization, application, or device. For individuals, it involves the collection of personal data that is essential for facilitating automated access to digital services, confirming one's identity on the internet, and allowing digital systems to manage interactions between different parties. It is a component of a person's social identity in the digital realm, often referred to as their online identity.*

While this term is reasonably complete, it needs more insights into the capabilities of a digital identity. The UK government has published a UK Digital Identity Attributes and Trust Framework document where it defines a digital identity[2] as *"a digital representation of a person acting as an individual or as a representative of an organisation. It enables them to prove who they are during interactions and transactions. They can use it online or in person."*

For this document, we will consider a digital identity to be

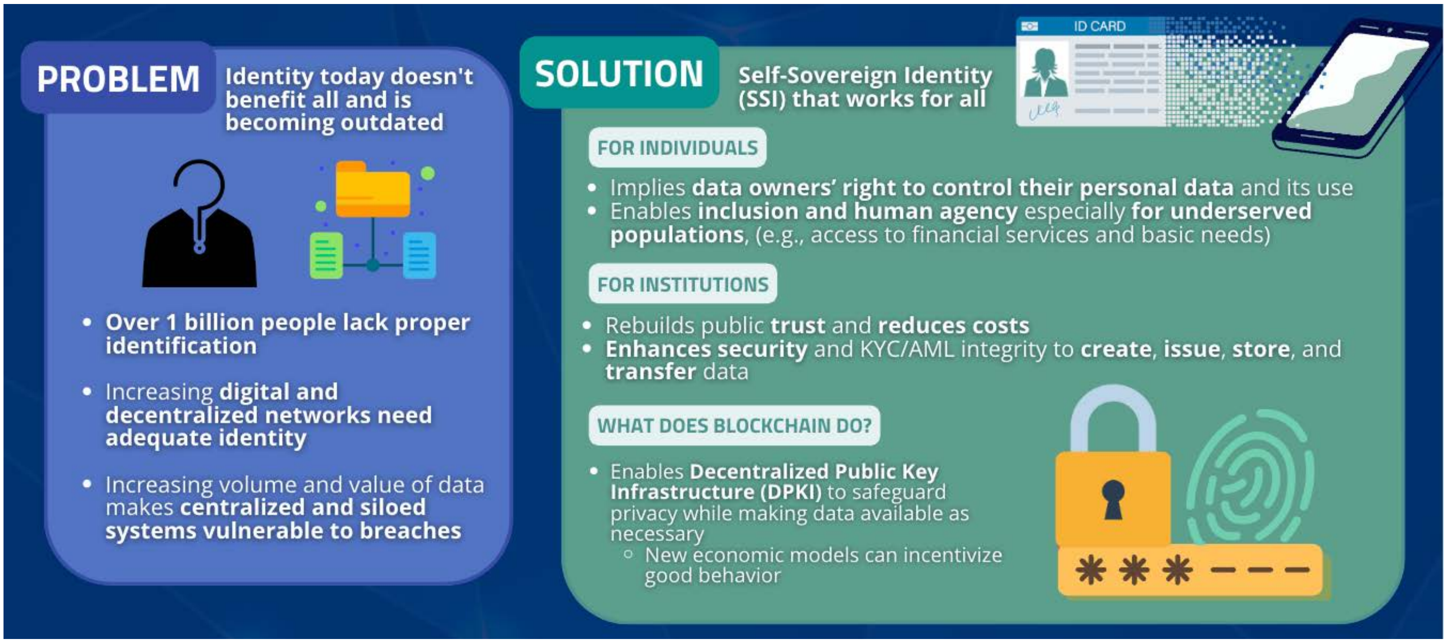
"A digital representation that enables people, organizations and things to present trustworthy data when interacting digitally."

Digital trust company Sezoo[3] published this definition in the paper "Trustworthy digital identities as a foundation for digital trust"[4]

(PART 1) DIGITAL IDENTITY & USE CASES: WHAT IS THE NEED FOR DIGITAL IDENTITY?

A fact often highlighted in any discussion around digital identities is that nearly a billion people do not have any verifiable identity or other legal documentation. The absence of such papers significantly encumbers, especially for underrepresented and marginalized communities, the ability to access services, seek employment, or discover ways to improve their way of life. In a digitally connected world that depends on digital transactions, the absence of trustworthy digital identities leads to exclusion and exploitation. It exacerbates the magnitude and consequences of a digital divide between those with access and those without access to networks of productivity. A foundational digital identity presents a form of "root of trust" that can be recognized by other entities and stakeholders in an ecosystem. Such recognition also establishes the acceptance of the assertions made by the individual through the digital identity they consent to share, which allows access to participate in the economic, legal and political aspects of the ecosystem or network.

Figure 1: The need for Digital Identity



PROBLEM **Identity today doesn't benefit all and is becoming outdated**

- **Over 1 billion people lack proper identification**
- Increasing **digital and decentralized networks need adequate identity**
- Increasing volume and value of data makes **centralized and siloed systems vulnerable to breaches**

SOLUTION **Self-Sovereign Identity (SSI) that works for all**

FOR INDIVIDUALS

- Implies **data owners' right to control their personal data** and its use
- Enables **inclusion and human agency** especially **for underserved populations**, (e.g., access to financial services and basic needs)

FOR INSTITUTIONS

- Rebuilds public **trust** and **reduces costs**
- **Enhances security** and KYC/AML integrity to **create**, **issue**, **store**, and **transfer** data

WHAT DOES BLOCKCHAIN DO?

- Enables **Decentralized Public Key Infrastructure (DPKI)** to safeguard privacy while making data available as necessary
  - New economic models can incentivize good behavior

The digital transformation of society has led to explosive growth in transactions that depend on reliable and trustworthy data exchange. Access to such high-trust data is now essential to the value-creation system. Therefore, data bound in some form to reliable digital identities is a critical component for governance, business and regulatory functions. The various use cases of digital identity demonstrate a fundamental need to create, issue and manage reliable digital identities, which offer the holders/principals/subjects the capability to mitigate the risks emanating from poorly designed data flow systems, and even data security breaches.

(1.1) FORMS OF DIGITAL IDENTITY

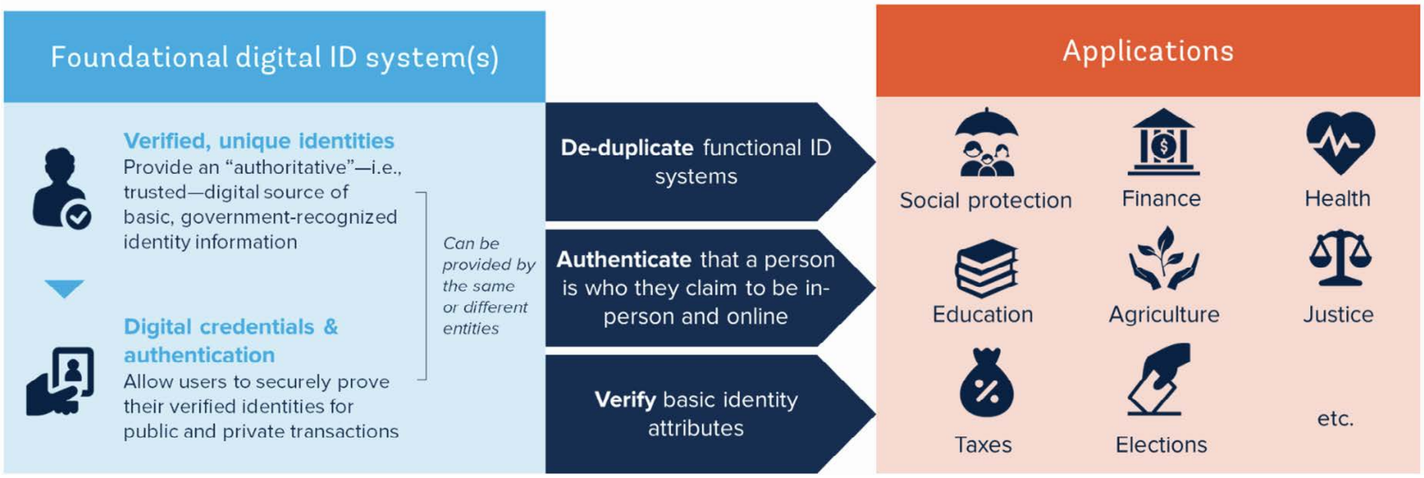
Digital identity refers to the use of data, represented and utilized as a digital identifier, identify an individual or entity. These identifiers can refer to the following broad categories:

1. Persons (Personal Identity)
   - **Definition:** This refers to an individual's unique identity used in the digital world for various personal activities.
   - **Usage:** For social media interactions, personal communications, and accessing non-work-related online services.
   - **Examples:** Social media profiles, email accounts, user IDs for personal apps. This also includes digital versions of government-issued IDs (e.g., e-passports, digital driver's licenses, national ID cards).
2. Employees of the Company / Organization
   - **Definition:** The digital identity assigned to an individual by their employer, representing them as part of an organization.
   - **Usage:** For accessing company systems, conducting business tasks, and collaborating on projects.
   - **Examples:** Work email addresses, employee ID numbers, login credentials for work platforms.
3. Legal Identities (Legal Entity Identifiers - LEI)
   - **Definition:** A unique, standardized code that identifies businesses and organizations in financial and legal transactions.
   - **Examples of LEI in Use:**
     i. **International Trade:** A shipping company uses its LEI to facilitate cross-border transactions, ensuring compliance with global trade regulations.
     ii. **Banking:** A financial institution verifies the LEI of a corporate client before opening a business account.
     iii. **Investments:** An asset management firm uses LEIs to identify counterparties in securities transactions.
     iv. **Tax Reporting:** A multinational corporation includes its LEI in regulatory tax filings to comply with international standards.
     v. **Regulatory Compliance:** A startup registers for an LEI to participate in financial markets and report transactions to regulators like the European Securities and Markets Authority (ESMA).
4. As Internet of Things (IoT)
   - **Definition:** Digital identities associated with connected devices and machines that communicate over the internet.
   - **Usage:** For device authentication, remote control, data sharing, and security management in smart environments.
   - **Examples:** Smart home devices, industrial IoT devices, wearable tech with unique device identifiers.

When it comes to individuals, digital identity can also take several forms and attributes, of which we highlight the most common below:

Foundational Identity: This refers to the general concept of a basic identifier, generally at a national level, that can be used to access a wide range of services offered by the public and private sector, and also engage in related transactions. A foundational identification system is to manage the identity data for the general population, providing credentials to serve as proof of identity to access such services and transactions. Increasingly, foundational identity systems are adopting digital formats.

Figure 5. Potential role of a foundational ID system


Foundational digital ID system(s)
Verified, unique identities
Provide an "authoritative"—i.e., trusted—digital source of basic, government-recognized identity information
Digital credentials & authentication
Allow users to securely prove their verified identities for public and private transactions
Can be provided by the same or different entities
De-duplicate functional ID systems
Authenticate that a person is who they claim to be in-person and online
Verify basic identity attributes
Applications
Social protection
Finance
Health
Education
Agriculture
Justice
Taxes
Elections
etc.

Source: https://id4d.worldbank.org/guide/types-id-systems

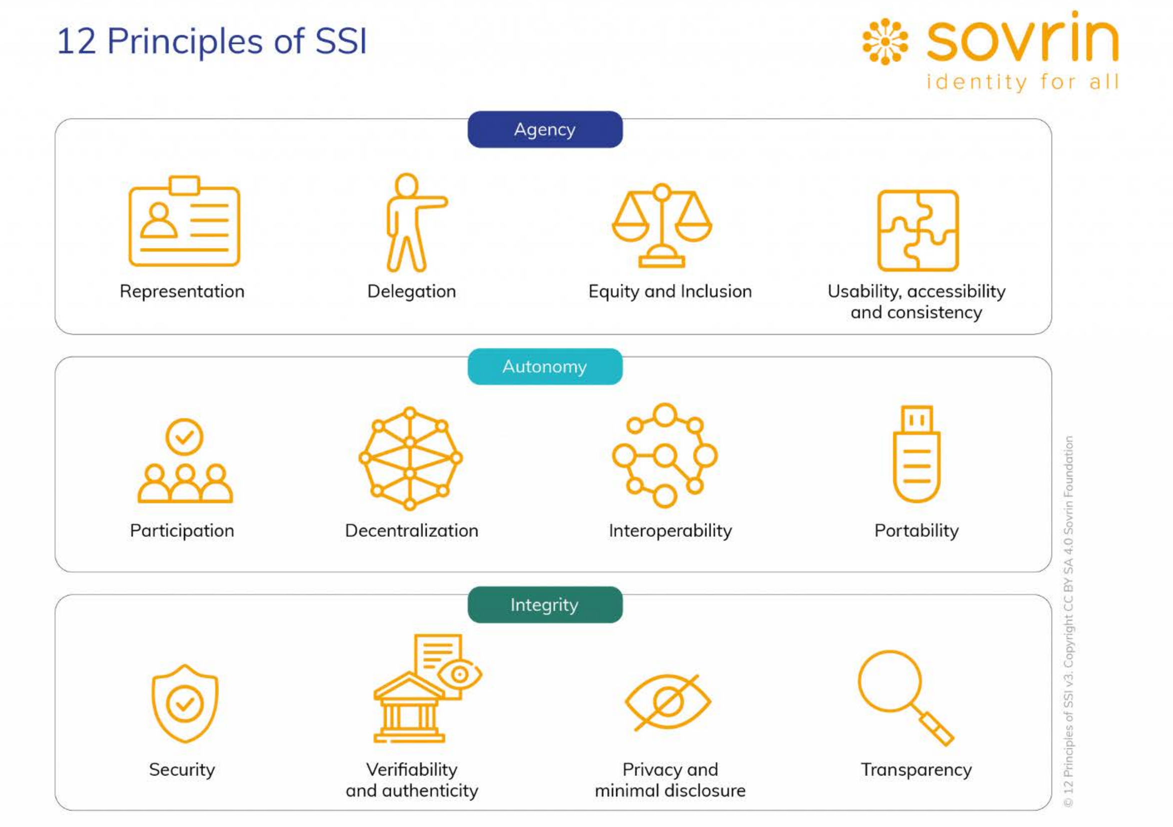
Derived Identity: In some cases, where a state-mandated national ID has yet to be slowly rolled out, bank IDs have become repurposed to provide a set of high-quality digital identifiers that can be linked to and integrated into many other services. These services do not have to be banking-related; many non-banking use cases have also emerged building on the basic digital identifiers provided by banks. In some cases, the interactions and transactions of the ID holder provide a good proxy for the notion that a derived ID can be attested and certified by external or third parties. Therefore, derived identity can serve as a proxy for a foundational identity that may not exist.

Biometric Identity: The unique biological characteristics of individuals can be used to verify their identity. These attributes can be biological characteristics (e.g., fingerprints, iris scans, facial recognition, veins, and shapes of body parts like ears, hand geometry, or even odor or DNA attributes) or behavioral attributes (e.g., voice, signature, keystroke patterns, or patterns in gestures, walking, or other movements). Biometric authentication is invoked when a select number of unique biological traits are used to verify a person's identity. In some digital identity systems, especially those related to high-trust and high-assurance data exchange use cases, the user enrollment workflow also includes registering biometric information. Many of the largest identity projects include a biometric component.

Biometrics may be considered more accurate than other forms of identity because they are inherently tied to the individual. Biometric characteristics, as opposed to passwords and other codes, are very difficult, or nearly impossible, to duplicate, lose, or share for use among multiple persons. Many national identity and immigration or border crossing records rely on biometrics. Security is of utmost importance for this form of identity because any personal data stolen through a breach would be nearly impossible to reverse. As opposed to changing a password, we cannot change the shape of our fingerprint. Therefore, the risks and overall downside of biometric identity (e.g., violation of privacy rights, high costs, invasive format) in many cases may not make this form of identity worthwhile because they may not be outweighed by the benefits.

Self-Sovereign Identity (SSI): The main challenge with a digital identity has always been to implement it safely and correctly. This usually means that the digital identity protects the holder's privacy, does not lead to exclusion, and functions in a way safe enough to prevent unwanted surveillance by correlating usage patterns of the digital identifier. Over time, self-sovereign identity (SSI) principles[6] have provided a working framework for designing, deploying, and managing a digital identity system where identity holders have the power and sovereignty over their own identities. These principles focus on the digital identity holder's agency, autonomy, and integrity.

Figure 2: 12 Principles of SSI from the Sovrin Foundation



CANADA'S DIGITAL SELF-SOVEREIGN IDENTITY FRAMEWORKS

In recent years Canada has led in the adoption of SSI based approach to digital identity and the creation of a regulatory framework which enables user-centric approach to the governance of such identifiers.

A digital identity would simply be the electronic equivalent of physical documents one already has. With the digital identity, the holder would be able to do things like:

- Claim social benefits
- File your taxes
- Access your health records
- Open a bank account
- Buy a home

Digital ID in Canada is protected by The Privacy Act, The Digital Charter and a Policy of Government Security Directive on Identity Management.

The Canadian government is in the planning stages of rolling out a country-wide digital identity program. https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world

Digital credentials allow people and businesses to access services online without having to go to a location in person, send sensitive information through mail, or remember another username and password. Enabling individuals and businesses to prove their identity and share verified information through digital means.

This approach is built around offering security, efficiency, convenience for the holder of the digital credentials. However, as this is an emerging technology landscape there are downsides to rapid adoption in the form of enabling robust cybersecurity, ensuring inclusiveness and equity through accessibility features, managing privacy and the overarching reliance on technology through the digital transformation process.

Digital ID generally offers greater protections from ID theft and leaks of sensitive info in boosting privacy. But concerns include data collection, who can access this data and how it's used, as well as location tracking, and questions around potential for government tracking.

The Privacy Act and the Digital Governance Council of Canada standardized framework (PCTF) define a duty of care that citizens, clients and customers should expect while using modernized digital services. This defined duty of care puts people's benefits at the center while enabling adopters to verify their practice, and trustmark to validate data integrity and security.

The Digital Identity and Authentication Coalition of Canada DIACC has produced a shared European and Canadian perspective on digital identity policy principles to maximize benefits for people. Comparing digital identity approaches to inform policy development and support interoperability efforts. More information is available about this approach https://diacc.ca/2022/11/02/policy-design-principles-to-maximize-people-centered-benefits-of-digital-identity/

Directive on Identity Management https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16577 is supported by two guidelines and one standard:

Guideline on Defining Authentication Requirements https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=26262;

Guideline on Identity Assurance https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30678;

Standard on Identity and Credential Assurance https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32612

The west coast Province of British Columbia now has a digital identity, the BC Services Card. The service provides cardholders the ability to prove their identity to access government services in-person and online using a physical or digital BC Driver's Licence and Services Card. DID will not be mandatory, other forms of physical ID may still be used.

The City of Vancouver is spearheading the use of digital credentials to reduce the need for manual verification steps in permitting and licensing services. Digital credentials are issued by recognized authorities to the BC Wallet mobile app where the information is encrypted and secure. Work is underway to further explore applications, including Digital Business Licences, Digital Certificate of Qualification, Digital Home-Owner Credential.

(1.2) DIGITAL ID AND BLOCKCHAIN

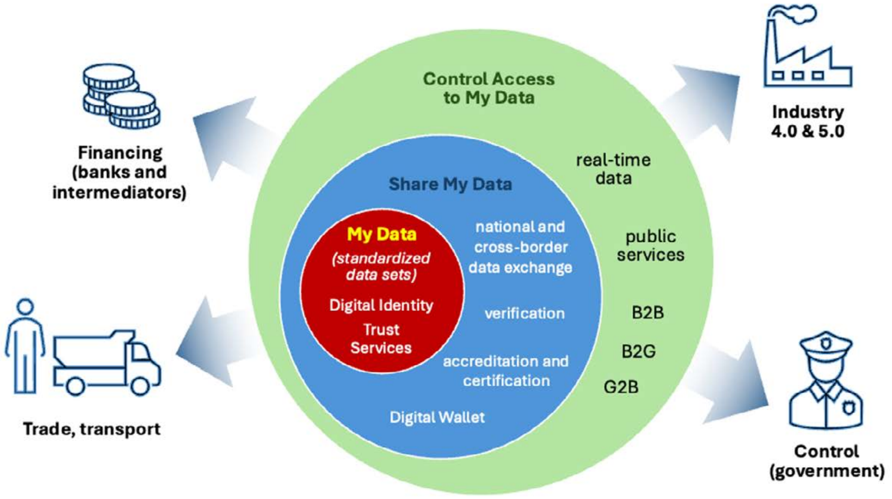
Blockchain, a technology usually more recognised for cryptocurrency moorings, has been pivotal for the adoption of SSI models. It has expanded access to underserved communities and enhanced the privacy and security of personal information. More importantly, it has empowered the holders to have more control over their data, enabling a significant shift in the digital landscape of activities.

Today, we see digital identities becoming the focal point of discussion when designing digital transformation policies globally, including those spearheaded by member states in the EU, and a wide range of programs currently developing and rolling out national ID projects in countries such as Bhutan[7]. The Modular Open Source Identity Platform (MOSIP)[8] project has enabled the implementation and adoption of digital identity as an open-source Digital Public Good (DPG)[9]. This approach has lowered the cost of digital identity deployment and encouraged many more countries to pivot toward creating the necessary business, legal and technical frameworks for successful digital identity rollouts.

In many cases, good biometric technology is a key binding element to digital identities, especially doing so in a manner that enables the person to have more agency, control, and autonomy.

DIGITAL ID CAN BE A CORNERSTONE OF A REAL-TIME ECONOMY

Digital Identity is fundamental to an ecosystem where economic transactions, processes, and activities occur in real-time or near real-time, as facilitated by blockchain technology. This is enabled by digital technologies and instantaneous data flows, allowing businesses, governments, and individuals to interact and make decisions with minimal latency. Key characteristics include automation, integration of systems, and immediate processing of payments, reporting, and other economic activities. Digital identity is a cornerstone of the Real-Time Economy, as it facilitates seamless, secure, and efficient transactions.



(1.3) FORMS OF DATA

Just as there are several forms of digital identity, there can also be several forms of data utilized to create digital identities. Each form of data can also facilitate certain kinds of identifiers. Therefore, digital identity use cases are often tied to a particular form of data.

Different forms of data can be used to achieve distinct use cases through a digital identity...

Extensive information

Less information

	1 Deterministic data	2 Probabilistic data	3 Self-managed data
Overview	• First party data that is trusted and true. • Deterministic data relies upon identity attributes that act as unique identifiers to create a match between one or several pieces of personally identifiable information.	• Predictive insights that are inferred from behavioral events across a wider range of data sets. • Statistical modeling is generally used to assess the probability that the data matches a specific person	• Individual (usually consumer) created data that provides the user with increased control and autonomy of verifiable credentials.
Scenario examples *Deep dive next page*	• Credit and financial identity • Data aggregators • Business and entity verification • Identity verification	• User-generated content management • Identity graphing and resolution • User and entity behaved analytics • Biometrics	• Identity wallets • Password managers • Master data management • Decentralized ID and verifiable credential management
Type of information requiered	• Legal name • Government issued ID number • Biometric data • Data verification data	• Usage patterns (i.e., statistical data) • Geolocation data • Social media activity and engagement	• Credentials and certifications • Nationality • User-generated profile information

... With each type of data category enabling a series of unique use cases

1 Deterministic data

- Credit and financial identity
- Data aggregators
- Business and entity verification (KYB)
- Identity verification (KYC)
- Identity proofing
- Regulatory compliance transaction monitoring
- Background screening
- Document verification
- Mobile identity and device intelligence
- eID and Civil IDs
- eSignature

2 Probablistic data

- Identity graphing and resolution
- Personal and signals based intelligence
- User and entity behaved analytics
- Fraud detection and prevention
- Biometrics

3 Self-maanged data

- Master data management
- Privacy, data protection, and consent
- Identity governance and administration
- Workforce IAM
- Customer IAM
- Privileged access management
- Authentication
- Machine identity
- Password managers
- Identity wallets
- Decentralized ID and verifiable credential management

FORMS OF DATA AFFECT ACCESS TO DIGITAL IDENTITY

The form of data that a given digital identifier comprises can have a fundamental impact on the use cases that it can facilitate, through which persons can be authenticated to the extent that they can be matched to records of digital identifiers. Self-managed data, for instance, can be flexible and take several forms. Deterministic data refers to an exact value (e.g., Identity card number) that leaves no margin of error in matching a person to an identifier. On the other hand, biometric data uses a probabilistic mechanism to match a person to an identifier (e.g., fingerprints). The patterns detected on a biometric record (e.g., past fingerprint image) may have a margin of error with respect to the biometric information provided by the person in real time (current fingerprint image capture). Therefore, there must be a tolerance value that must be considered.

ADDITIONAL CONSIDERATIONS FOR BIOMETRIC IDENTITY

Biometrics are being gradually introduced at scale, such as at border checkpoints, thus intersecting with traveler experience and a broad range of activities in which such identities are used. Many of these interactions primarily include Facial Recognition Technologies (FRTs). Implementations must keep current with the work underway at the National Institute of Standards and Technology (NIST), under the Face Recognition Technology Evaluation (FRTE), among many related initiatives and standards underway, which are meant to ensure the accurate and measurable quality of biometric data readings such as FRTs.

At the moment a person opens an online account, the identity verification process involves a form of device binding to the credentials utilized, ensuring the device acting on behalf of a person is actually owned by that real person and not someone else claiming to be that individual. An essential driver of binding biometric information during digital identity enrollment is the capability to use a mobile device-centric user experience during the data exchange stage. The Digital Identity Guidelines from NIST[10] (800-63-4, available for public comments until 7th October 2024) include a comprehensive set of aspects around the management of risks and determination of impact levels around the measures of risks for enrollment into a digital identity service.

ETHICAL CHALLENGES FOR BIOMETRIC IDENTITY: COMPLIANCE, SECURITY, AND TECHNICAL CONSIDERATIONS

A recent case highlighting the importance of ethical considerations has been the emergence of projects like WorldCoin, and subsequently the Orb project, which have become highly controversial in providing technology to capture biometrics to build reusable digital identities. After a high-profile rollout that was deemed to be non-compliant with local regulatory requirements, many countries have decided to revisit this approach and stopped further citizen enrollment using WorldCoin technology.

WorldCoin implementations didn't consider the legal requirements in the countries where they launched operations, leading to heavy regulatory scrutiny and investigations. There is sufficient research[11] [12] [13] that acquiring biometric data and enabling binding requires regulatory approvals and oversight. An important lesson learned from the response of various national governments to the approach adopted by WorldCoin is that a launch at a global scale must be compliant in all jurisdictions in which operations are to take place. This requires strategic considerations around security, both with respect to data and the applications themselves.

Another ongoing challenge with using biometric technology for identity binding during the enrolment process of creating a digital identifier is creating adequate guardrails against unintended consequences[14]. Since biometric technology- based authentication is often the first option for enabling access to the services, selecting good failsafes is crucial. Biometrics are a powerful tool, but they only work adequately if robust security measures can be ensured, given the magnitude of potential downsides (e.g., identity theft compromises uniquely personal information that cannot be replaced).

Moreover, biometric authentication which requires fingerprinting, for instance, can also become a barrier when there is a fingerprint mismatch or fingerprints can no longer be read with sufficient accuracy by the hardware used. Robust management of biometric data, preventing such data being accessed at rest or in transit, and ensuring secure encryption technology is essential for adopting biometric based digital identity workflows[15]. Given the level of digital literacy in a given population, it is essential that workflows which depend on biometric technology provide ways to record informed consent, protect the privacy of the holder and prevent data misuse.

EXAMPLES OF BIOMETRIC IDENTITY SOLUTIONS

Digital identity, with biometric components designed adequately, can lead to empowerment of underserved communities, while also allowing for cross jurisdiction exchange of data and services, spanning a wide range of activities and aspects of daily life.

- **Economic Community of West African States (ECOWAS) Biometric National Identity Card (ENBIC)** - The ENBIC[16] is expected to facilitate movement and business transactions among women and other vulnerable individuals in the border communities between Senegal and Guinea Bissau. The ECOWAS Commission intends to expand this offering to other member countries.
- **Electronic/Digital Civil Registration and Vital Statistics System (e-CRVS) Project** - The National Population Commission launched the e-CRVS[17] in partnership with the United Nations Children's Fund (UNICEF/WARCO) and the World Health Organization (WHO). The West and Central Africa region, and UNICEF Regional Office (WCARO) have also significantly advanced the digitalization of community health information systems across nine countries: Benin, Burkina Faso, Central African Republic (CAR), the Democratic Republic of the Congo (DRC), Liberia, Mali, Niger, Nigeria, and Sierra Leone.
- **The Ethipia Digital ID for Inclusion and Services Project (FAYDA)** - The World Bank financed the Ethiopia Digital ID for Inclusion and Services Project[18]. Fayda is built on the Digital Public Good platform MOSIP.
- **Digital Zambia Acceleration Project (DZAP)** - Funded by the World Bank this project also seeks to speed up Zambia's digital infrastructure development and improve Internet access and connectivity.[19] The goal is to promote inclusive access to the Internet and digital services.
- **Democratic Republic of Congo (DRC) Digital Transformation Project** - This project , also financed by the World Bank, aims to improve access to affordable and high-quality broadband connectivity, in addition to digital services, especially solutions with a high impact, and digital skills that are relevant to key industries.[20]

(1.4) NOTABLE USE CASES FOR DIGITAL ID

- **Humanitarian Assistance** - Digital identity of beneficiaries has increased access to aid funding for many and provision of funding in emergency situations, especially for unbanked populations. It also eliminated many bottlenecks that arise when attempting to make payments through different channels.
  – The United Nations High Commissioner for Refugees (UNHCR) has developed, in collaboration with the Stellar Organization "Stellar Aid Assist"[21], a blockchain-based application that enables the deposit of stablecoins[22] (USDC) into refugees' digital wallets. The application is equipped with biometric capabilities and mandates the provision of a government-issued ID or/ other forms of acceptable digital identification to ensure the authenticity of the beneficiary.
  – GBBC GIving, in partnership with the World Food Programme Innovation Accelerator, has developed the Food for Crisis joint initiative to track and trace donor funds, from donor to beneficiary, with blockchain technology and digital twins. Funds are traced using digital identifiers, and beneficiaries can also be validated with digital identifiers.
- **Environmental Impact** - Digital identifiers for workflows are also used to generate environmental impact. Digital identifiers of carbon credits enable a mechanism to create a marketplace for tokens enabling trade, exchange and burning. The use of blockchain technology can greatly improve trust and transparency in carbon markets.,

– The World Bank funds initiative[23] Carbon Assets Tracking System (CATS)[24] for low-carbon emission and emission tracking is an example. Of an emission reduction transaction registry.
– GBBC's InterWork Alliance has also developed an approach to a Carbon Emissions Token (CET) Protocol, using the Token Taxonomy Framework as a standard to define and guide the tokenization of emissions. The objective is to strengthen reporting of emissions with common guidance, specifications, and best practices of tokenizing carbon emissions.[25]

- **Farming and Agriculture** - Verified identities of farmers can greatly enhance their access to digital solutions.
  – With the support of a consortium of partners convened by USAID's Feed the Future Program, AgriFi provides rural farmers with digital extension and financial literacy workshops, increasing access to digital solutions. AgriFi is built on a unique blockchain infrastructure called ToroNet, specifically designed to solve real-world problems at scale. Toronet[26] aims to revolutionize farmers' market engagement and sovereignty by leveraging digitalization and smart contracts to create fairer, transparent, connected, and inclusive agricultural markets[27]. The project leverages the full power of tokenization, including zero-knowledge proof KYC technologies, to enable the creation of a digital yet verifiable business profile for farmers, solving the problem of access to capital, inputs, and offtake, all in one place. Aggregate lending pools powered by smart contracts enable farmers to get funded while providing industry-standard insurance and KYC solutions. The money from the lending pools can only be used by farmers to purchase the inputs needed for their crops. At the end of the harvest cycle, the off-takers sell the produce and credit the smart contracts that distribute the revenue to all parties involved.
- **Decentralized Finance (DeFi)** - The optimal function and scaling of DeFi will depend largely on a blockchain-based model of digital identity of participants that is decentralized and self-sovereign. This can provide the right balance between the need for anonymity and the right identifiers to ensure participants are legitimate actors. Individuals can have the burden of proof, providing their information voluntarily. In a self-managed approach, the type of data provided by individual participants can be the differentiating factor. An external party would have to certify the data provided by the individual. Regulatory developments and industry discussions are still underway regarding the role of central authorities and other key stakeholders in an ecosystem that seeks to preserve privacy and anonymity, while also defining adequate rules and requirements.
- **Global Identity Systems and Standards** - Data on individuals and entities can be utilized to carry out verifications, and then white list models to facilitate access to trust services. The importance of privacy preserving zero-trust architecture can be key in these scenarios. Common standards can also define best practices
  – The Legal Entity Identifier (LEI) is a 20-character, alpha-numeric code based on the ISO17442 standard developed by the International Organization for Standardization (ISO). The LEI uniquely identifies legal entities globally. It contains key reference information about the entity (e.g., its local registration number and registration authority, legal name, legal address, parent/child entity relationships, etc.), enabling clear and unique identification of legal entities globally. All users can access all the LEI reference data via the GLEIF website for free as an open database.

LEI COMMON DATA FILE FORMAT

- https://www.gleif.org/en/about-lei/common-data-file-format/current-versions/level-1-data-lei-cdf-3-1-format#
- https://www.gleif.org/en/about-lei/common-data-file-format/current-versions/level-2-data-relationship-record-rr-cdf-2-1-format#

- The Global LEI System is managed by the Global Legal Entity Identifier Foundation (GLEIF), established by the Financial Stability Board of G20 in 2014 as a Non-for-Profit Swiss Foundation. The Global LEI System is overseen by the Regulatory Oversight Committee of more than 65 regulators and 19 observers from 50 countries. Regulators mandate the LEI in global financial transactions. Currently, over 2.6 million entities in 200+ jurisdictions have LEIs.

(PART 2) DIGITAL PUBLIC INFRASTRUCTURE (DPI)

Large-scale deployments of digital identity projects mandate digital infrastructure development, maintenance, and operation. It is essential to consider this, as the state is often the primary sponsor and driver of digital identity initiatives. With technology advancements using public and private cloud infrastructure, it is now possible to design, build, and operate the necessary technology components that interplay to provide a robust consumer experience for digital identity and services associated with digital identity.

In recent years, the Digital Public Infrastructure (DPI) approach has found considerable success and adoption while designing the infrastructure for digital identity efforts. While there is no commonly accepted definition of "Digital Public Infrastructure", enough conceptual commonalities exist to help sponsors and stakeholders.

WHAT IS DPI?

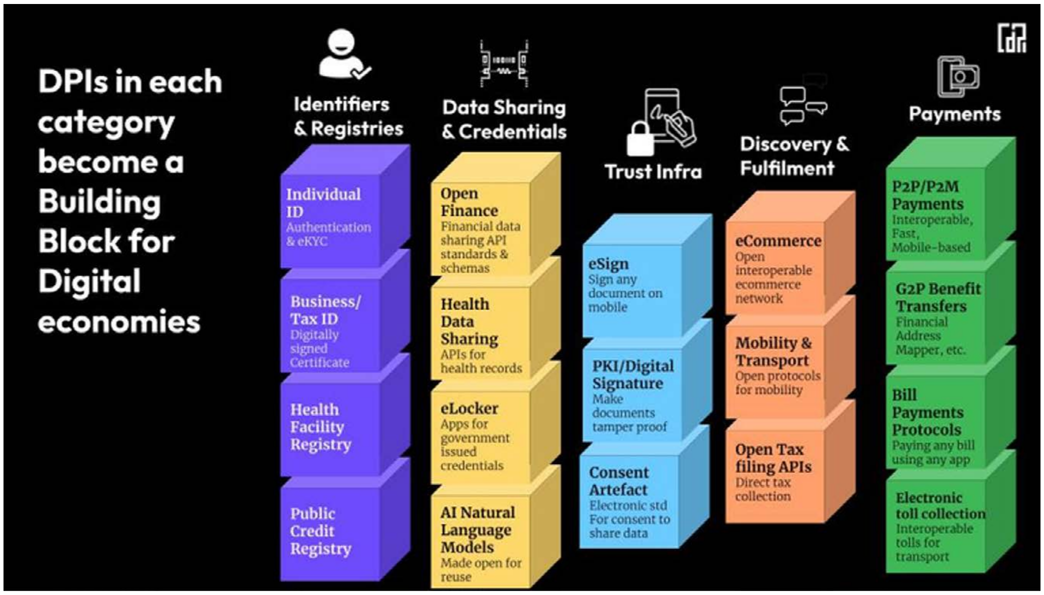
The Centre for Digital Public Infrastructure[28] mentions that **digital** does not require smartphones or connectivity to scale, **public**-minded yet still crafted to drive private innovation exponentially, and **infrastructure** is not just an app, a platform or a solution but a minimalist approach to build at a national scale.

According to the Centre for Digital Public Infrastructure:

Digital Public Infrastructure is an approach to solving socio-economic problems at scale, by combining minimalist technology interventions, public-private governance, and vibrant market innovation.

Common examples include the Internet, mobile networks, GPS, verifiable identity systems, interoperable payments networks, consented data sharing, open loop discovery and fulfillment networks, digital signatures, and beyond.

This perspective considers that digital public infrastructure (DPI) has core elements such as identifiers and registries, data sharing, credentials and data models, signatures and consent, discovery and fulfilment, and payments. These building blocks span all activities that emerge as possibilities for a robust and scalable digital identity deployment.


DPIs in each category become a Building Block for Digital economies
Identifiers & Registries
Individual ID Authentication & eKYC
Business/ Tax ID Digitally signed Certificate
Health Facility Registry
Public Credit Registry
Data Sharing & Credentials
Open Finance Financial data sharing API standards & schemas
Health Data Sharing APIs for health records
eLocker Apps for government issued credentials
AI Natural Language Models Made open for reuse
Trust Infra
eSign Sign any document on mobile
PKI/Digital Signature Make documents tamper proof
Consent Artefact Electronic std For consent to share data
Discovery & Fulfilment
eCommerce Open interoperable ecommerce network
Mobility & Transport Open protocols for mobility
Open Tax filing APIs Direct tax collection
Payments
P2P/P2M Payments Interoperable, Fast, Mobile-based
G2P Benefit Transfers Financial Address Mapper, etc.
Bill Payments Protocols Paying any bill using any app
Electronic toll collection Interoperable tolls for transport

While specific digital identity projects can be open-source and can be a digital public good (DPG - like the open-source MOSIP infrastructure introduced above), the overall technology design which makes a good digital identity worthwhile is Digital Public Infrastructure (DPI). In the design pattern of DPI, the more traditional approach of “platforms” is transformed into “networks”. This ensures that several interconnected and interoperable digital ecosystems can emerge using open standards, open-source software, open protocols and open networks.

The DPI approach fully uses digital identifiers and data registries, data exchange and processing (including AI/ML), trust infrastructure, digital payments and discovery and fulfilment. These are the building blocks, and blockchain and digital identity are the essential, foundational components of a DPI.

(2.1) DIGITAL IDENTITY AND REGISTRIES

Digital identities become meaningful and valuable when the holders can reuse, exchange, or share them to access various services. The data-centric dynamic economy is designed around the consent-based exchange of digital identities and metadata. The digital transformation from legacy systems to digital ones underscores the need to have “trust”. This implies that relying parties can easily verify the digital identity using some authentication.

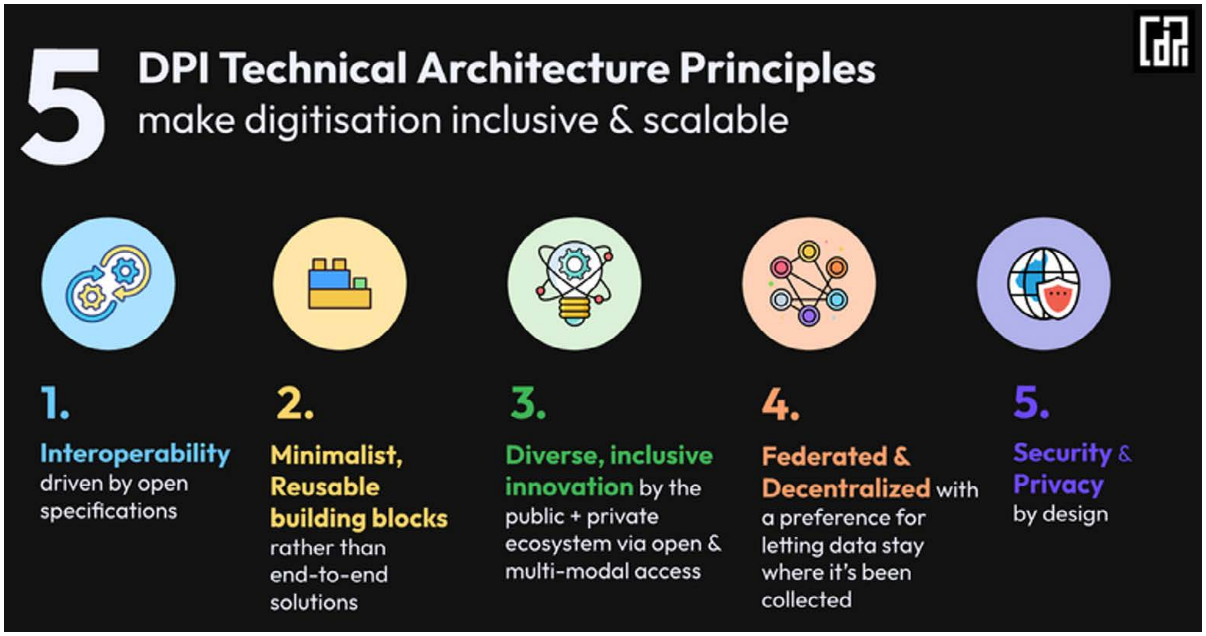
Additionally, as digital identities become more commonly used across sectors, it implies that issuers of digital identities maintain a registry of such digital identifiers. In some instances, such registries are publicly available, driven by the needs of the sectors and digital ecosystems. In other cases, these registries can be private or accessible only to authenticated and authorized entities. These decentralized digital registries, which contain digitally signed data, are a crucial driver to high-trust, low-cost consumption of digital identities for various purposes (such as authentication, KYC flows, civil registries, entity registries, etc.).

Many countries are adopting the DPI pattern when transforming services and building data registries, such as civil registries (of births and deaths), registries of attestors and notaries, and so forth. Some leading examples emerge from Brazil, Australia, Singapore, Switzerland, and others.

(2.2) PRINCIPLES OF DIGITAL PUBLIC INFRASTRUCTURE

Considering the emergence of Digital Public Infrastructure (DPI) as a preferred playbook or approach to deploying digital identity solutions, it is essential to examine some fundamental principles. Without a widely understood and commonly accepted definition of DPI, the principles provide a foundation for reviewing the merits of any digital identity infrastructure as a DPI.

The Centre for Digital Public Infrastructure has identified five principles that ensure digitization is inclusive, equitable, fair, and scalable. These principles are explained in the illustration below.



5 DPI Technical Architecture Principles make digitisation inclusive & scalable

1. **Interoperability** driven by open specifications

2. **Minimalist, Reusable building blocks** rather than end-to-end solutions

3. **Diverse, inclusive innovation** by the public + private ecosystem via open & multi-modal access

4. **Federated & Decentralized** with a preference for letting data stay where it's been collected

5. **Security** & **Privacy** by design

Digital identity systems should also demonstrate additional values that ensure they are designed to be user-centric and aligned with the requirements of the jurisdiction where the systems operate. Such values should include:

- Being human-centric to prevent unintended consequences or harm
- Focusing on informed consent to ensure that technology overreach is prevented
- Empowering innovation growth and fostering the UN Sustainable Development Goals

Digital Strategy of New South Wales (NSW)
For example, the government of New South Wales (NSW) announced a Digital Strategy[29], which focuses on delivering inclusive and secure digital services to improve residents' lives. The strategy is built around five missions:

- Accessibility - making digital services inclusive and accessible for all people in NSW
- Productivity - using digital transformation to advance service delivery
- Trust - sustainable digital infrastructure to build trust in government services
- Resilience - to deploy infrastructure that is resilient for emergencies
- Digital Skills - to uplift the digital capability in the public sector workforce

NSW has decided to create a NSW Digital ID and a NSW Digital Wallet to enable individuals to prove their identity while engaging in secure and safe digital data exchange. The enrolment workflow for the NSW Digital ID requires two or more ID documents, a mobile number and an email address. The image/photo verification flow uses a selfie to match against an existing photo.

(2.3) DPI AS A BLUEPRINT FOR DIGITAL IDENTITY

Digital Public Infrastructure using modular, reusable components enables a blueprint that can be easily adopted and adapted to the needs of any given use case, or even a nation seeking to implement a digital identity system. This flexibility has resulted in improved economics, as many open-source projects can easily fit into the technology requirements of a DPI focused on extensible digital identities.

DPIs that adopt open standards and protocols can incubate an ecosystem of digital services that includes private and public sector participants. Adopting open standards is essential to achieving the stated goal of interoperability, particularly data interoperability, as successful scaled DPI deployments of digital identity depend on extensive data exchange systems being established.

Digital Public Infrastructure Model in the United States
The U.S. Digital Public Infrastructure has evolved over the years, and with the support of advanced technologies, the US was able to successfully link individual IDs (for e.g. Social Security Numbers (SSNs) and International Tax Identification Numbers (ITINs) issued by Homeland Security Department, and Internal Revenue Service, respectively) with nationwide repositories and databases to allow individuals to be identified, authenticated, and authorized to access basic digital ID services such as Financial Institutions / Banking system, housing, taxation, education and healthcare.

Legal entities and corporations selling and trading activities are also governed by different government identification mechanisms, such as Tax IDs and Employer Identification Numbers (EINs) issued by Internal Revenue Service, with the former being used to oversee movement in employment activities, and the latter to monitor transactions and for tax reporting purposes.

U.S. Customs and Border Protection (CBP) is one of the key agencies that regulates movement of persons, goods and products. It applies diverse and sophisticated technologies in key airports and customs ports to scan persons, goods and products using their digital ID and permit details. Some of the advanced technologies that CBP adopts include Persistent Surveillance; Mobile Surveillance; Cargo Gamma Ray and X-ray Scanners, and Biometric ID technologies. The CBP initially started at exploring the wider capabilities of DLT, and then diverted its attention to working on resolving the global interoperability challenge between various systems. As a result, CBP had recommended to the World Wide Web Consortium (W3C) two standards on interoperability: Decentralized Identifiers and Verifiable Credentials that were accepted by W3C as official web standards.[30] [31]

Digital Public Infrastructure Model in Italy: A European Case.
The Digital Public Infrastructure model adopted in Italy is a good example of how digital transformation using strategic imperatives results in the availability of impactful nation-scale systems.

Italy's digital transformation is driven by several strategic initiatives and infrastructure investments aimed at modernizing the country's economy and addressing its current digital gaps[32].

Italy's digital transformation push aligns with the European Union's broader objectives, including the Digital Agenda for Europe and the Recovery and Resilience Facility (RRF). Italy has earmarked significant funds from the EU recovery funds to close the digital divide, modernize public administration, and promote innovation across industries. The National Recovery and Resilience Plan (PNRR), a key policy initiative, allocates billions towards digital transformation, with a focus on:

1. Digital infrastructure development (e.g., fiber optics, 5G networks, cloud platforms).
2. Industry 5.0 technologies such as AI, IoT, and robotics to modernize manufacturing, logistics, and other sectors (sustainability, ESG)
3. Encouraging small and medium enterprises (SMEs) to adopt digital tools to improve their operations

The European Digital Identity (EUDI) Regulation will revolutionize digital identity in the EU by enabling the creation of a universal, trustworthy, and secure European digital identity wallet. A digital identity guarantees all citizens a single authentication method and access to all digital services provided by public administrations and accredited private entities in Italy and Europe. The identification tools used to access online services are the SPID (Public Digital Identity System), the Electronic Identity Card and the National Service Card.[33]

Italy's digital infrastructure expansion is essential to enabling new technologies:

1. Fiber optic networks: Italy has been lagging behind other European countries regarding broadband coverage, but it's now scaling up investments to expand fiber-to-the-home (FTTH) networks, aiming to cover underserved areas and rural communities. Companies like TIM (Telecom Italia) and Open Fiber are leading in this area.
2. 5G networks: Italy has been rolling out 5G infrastructure, which will unlock opportunities for new services, including smart cities, connected vehicles, and advanced IoT applications.
3. Data centers and cloud computing: The Italian government is also investing in national cloud computing infrastructure, including the development of public-sector cloud solutions to support the digitalization of public services. This infrastructure will help Italy manage the growing demand for data processing, storage, and security.
4. Cybersecurity: As digital adoption increases, cybersecurity is a critical area of focus. Investments in secure infrastructure and cybersecurity solutions are being prioritized by both public and private sectors.

Incorporating Digital Public Goods (DPGs) alongside Digital Public Infrastructure (DPI) is highly relevant to the evolving digital landscape in Italy. Like many countries, Italy is leveraging digital tools and open technologies to foster innovation, improve public services, and support the United Nations' Sustainable Development Goals (SDGs). DPGs, which include open-source software, open data, AI models, open standards, and content, are playing a growing role in Italy's digital transformation.

- Italy's IO app is a prime example of a digital public good. It is an open-source platform that provides citizens with a unified interface to interact with public administration services. It allows access to a variety of public services like digital identity (SPID), digital certificates, and payments (PagoPA), fostering transparency and improving the accessibility of public services.
- PagoPA is another key open-source platform that modernizes how citizens interact with public administration for payments. It supports financial inclusion and facilitates transparent, efficient digital payments, which helps in advancing SDG 16 (Peace, Justice, and Strong Institutions).
- SPID (Public Digital Identity System). This is Italy's national digital identity system, which is interoperable and designed to enable citizens to access public and private services securely. The

SPID system is based on open standards and helps promote digital inclusion and accessibility, aligning with SDG 9 (Industry, Innovation, and Infrastructure).

Italy's Industry 5.0 plan incentivizes businesses to adopt advanced digital technologies to increase automation, efficiency, and competitiveness. Key opportunities include:

1. Cloud computing: As companies shift to cloud-based solutions, the demand for platforms that offer scalability, flexibility, and security has surged. Italy's cloud market is growing rapidly, driven by both SMEs and larger enterprises adopting Software as a Service (SaaS) and Infrastructure as a Service (IaaS) solutions.
2. Artificial Intelligence (AI) and Big Data: Italian companies and public administrations are increasingly adopting AI for automating processes, enhancing customer service, and making data-driven decisions. AI applications in sectors like healthcare, finance, and manufacturing are also growing.
3. Internet of Things (IoT): Italy is becoming a leader in IoT technologies, especially in the manufacturing sector, where connected devices help optimize production processes, predictive maintenance, and supply chain management.
4. Cybersecurity: The rise in digitalization increases vulnerability to cyber threats. Italy is expanding its investment in cybersecurity frameworks to protect both private and public institutions.

Regulations: The initiative to enhance Italy's public administration systems through investments in a national hybrid cloud infrastructure, referred to as the "Polo Strategico Nazionale" (National Strategic Hub), is a significant step towards modernizing Italy's digital ecosystem[34].

The primary aim of the Polo Strategico Nazionale is to ensure that all public administration systems, datasets, and applications are hosted in highly reliable data centers. This includes a focus on:

1. Security: Protecting sensitive government data from cyber threats
2. Performance: Ensuring quick and reliable access to services for citizens and businesses
3. Scalability Allowing for future growth and increased demand for digital services
4. Interoperability: Ensuring that different systems and datasets can work together seamlessly within the European framework
5. Energy Efficiency: Promoting sustainability through efficient energy use in data center operations

The investment in the Polo Strategico Nazionale represents a transformative effort to modernize Italy's public administration through a robust, secure, and efficient cloud infrastructure. By focusing on high standards of quality, security, and interoperability, Italy aims to create a resilient digital framework that will enhance public services and meet the growing demands of its citizens. This initiative not only addresses immediate needs for modernization but also positions Italy to thrive in the increasingly digital future, leveraging data as a strategic asset.

The Italian government has taken significant steps to promote Open Data by making public administration data accessible, reusable, and transparent for its citizens. These initiatives align with global trends towards openness and transparency in governance and are aimed at fostering innovation, accountability, and civic participation.

- Dati.gov.it is the official national portal for open data in Italy. Launched by the Agency for Digital Italy (AgID), this platform provides centralized access to datasets from various public administrations. It encourages the reuse of public data by developers, researchers, businesses, and citizens to foster innovation and create services that benefit society.

- OpenCoesione is an open data initiative focused on the transparency of public spending in Italy, particularly in projects funded by EU cohesion policy funds. The platform offers detailed information on how these funds are allocated, which projects they support, and the progress and outcomes of these projects.
- Italy has adopted a National Strategy for Data and Artificial Intelligence (AI)[35], which underscores the importance of open data in driving AI development and fostering innovation. By making public sector data open and accessible, the government aims to enable the development of AI solutions that can support public administration, healthcare, transportation, and other sectors.

Italy is an active member of the Open Government Partnership (OGP), an international platform for domestic reformers committed to making their governments more open, accountable, and responsive to citizens. As part of its OGP commitments, Italy has launched several open data initiatives aimed at enhancing public sector transparency and fostering citizen participation. The OGP action plans regularly focus on open data efforts, encouraging collaboration between public authorities and civil society to maximize the impact of open data on governance and public service delivery.

(2.4) UNLOCKING THE POTENTIAL OF DIGITAL IDENTITY THROUGH DPI GLOBALLY

Digital Identity projects developed using the DPI pattern have recently unlocked tremendous potential and created socio-economic opportunities. The table below provides an at-a-glance view of the impact from a region-specific view. Many use cases below utilize open-source technologies, such as X-Road - an open access software that facilitates unified and secure exchange of data across organizations.

Table: DPI and Digital Identity in selected jurisdictions

Country	DPI	Regulation	Primary Use Cases	Digital Identity	Digital Identity Regulations	Digital Identity Use Cases
Argentina	Argentina has made progress toward online government services with a single citizen-focused portal that consolidates solutions that were previously dispersed across systems.	While several laws and presidential decrees have been issued to reinforce digital services, the major guiding policy is the country's Digital Agenda. It defines policy goals toward digital government	Government services are still undergoing digital transformation.	The government of Argentina and the city of Buenos Aires have announced[36] the adoption of a QuarkID-based digital identity protocol to issue, manage, and exchange verifiable records. This is the first government-backed deployment of a decentralized identity model. The city of Buenos Aires is also adopting a blockchain-based SSI protocol within its digital identity app.	Argentina's Digital Signature Law is meant to regulate the use and legal validity of digital and electronic signatures, clarifying the conditions in which they are acceptable, as well as use of authentication methods and identity data used.	Records include such as civil registry records, proof of income, and learning and education credentials.

Brazil	The PIX instant payment system is one of the main DPI platforms in the country, with more than 100 million users. At the regional level, X-Road DPI infrastructure has been implemented in states such as Mato Grosso and Amapá.	Brazil has a legal framework for digital payments and has developed a robust digital authentication and data protection framework using PKI.	PIX has facilitated financial inclusion through instant payments, supporting social programs such as Auxílio Emergencial, which allowed the rapid opening of digital bank accounts.	The Gov.BR system has registered more than 150 million digitally authenticated users, facilitating access to public services.	The country has implemented personal data protection laws and has a PKI infrastructure for electronic signatures.	Gov.BR allows citizens to access more than 4,500 digital services, including authentication for opening bank accounts during the pandemic.
Chile	Chile has implemented a single authentication system for public officials, allowing secure access to various databases, including health databases.	The country has implemented regulations on data interoperability and advanced electronic signatures to support data exchange between agencies.	The interoperability system facilitates the efficient delivery of social services and data management between different government areas.	Digital authentication at the government level facilitating secure access to public services.	Chile has legislated on advanced electronic signature and interoperability of services, allowing for greater integration between agencies.	Digital identity is used to access government platforms that provide health, social assistance, and other essential services.
Colombia	Colombia has implemented X-Road to improve secure data exchange between government agencies and has used this platform to verify the beneficiaries of assistance programs.	The country has developed interoperability and digital authentication regulations, focusing on personal data protection.	During the pandemic, Colombia used X-Road to verify the eligibility of beneficiaries of social programs such as “Ingreso Solidario”, improving targeting and reducing fraud.	Colombia has implemented digital authentication to verify the identity of beneficiaries of social programs, such as “Ingreso Solidario”.	Colombia is strengthening its regulatory framework around the protection of personal data and interoperability of services.	The digital identity system was crucial during the pandemic because it used multiple databases to verify the eligibility of social program beneficiaries.

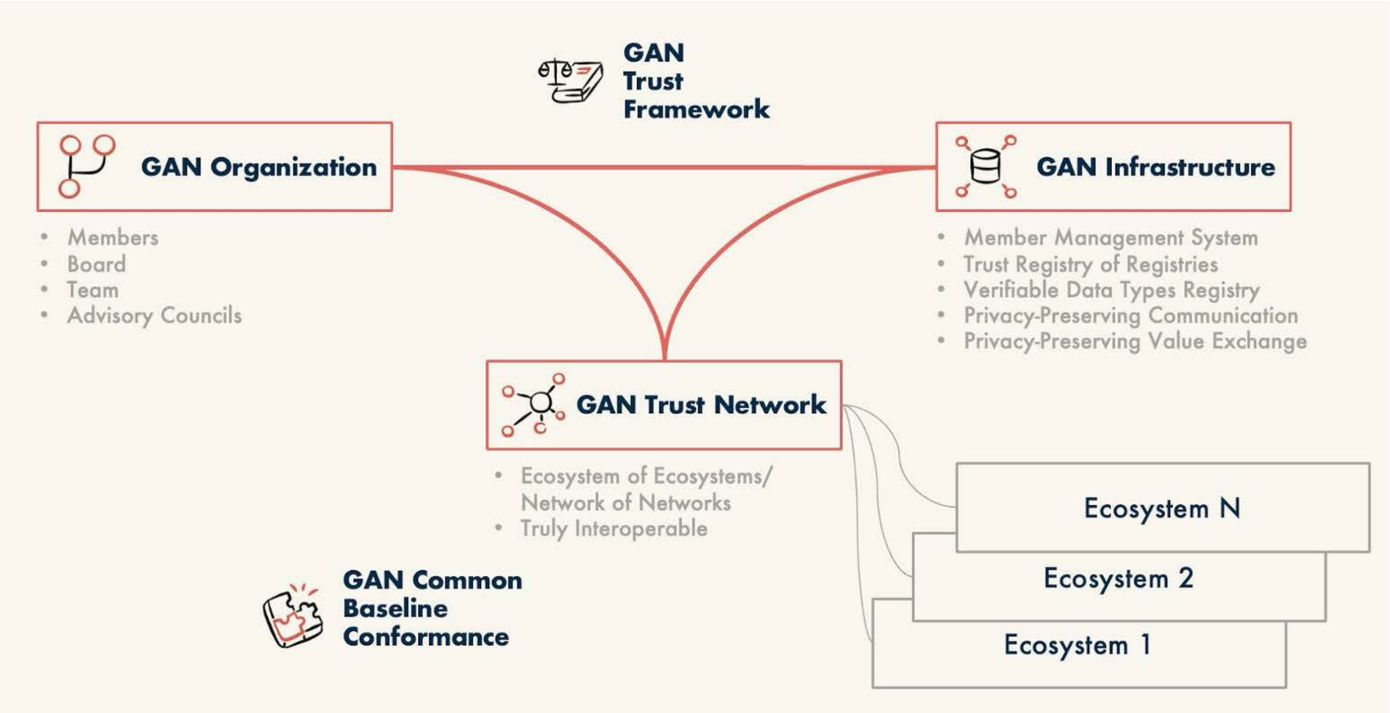
El Salvador	El Salvador has adopted X-Road through the Tenoli platform, allowing data exchange between government agencies. Moreover, as Bitcoin was made legal tender, a new class of DPI was announced to grant citizens access to USD and BTC, enabling holdings, sending, and receiving funds while prioritizing financial inclusion, interoperability and international trade.	El Salvador is working on regulations to strengthen interoperability and digital authentication within the public sector.	The Tenoli platform facilitates data interoperability between government agencies, improving efficiency in service delivery.	El Salvador is developing its digital identity system, which will allow authentication in public services, together with the Tenoli platform.	In the process of creating a regulatory framework that supports digital authentication and advanced electronic signatures.	Tenoli allows user authentication across multiple government agencies, facilitating the provision of services to citizens.
Estonia	Using the open-source data-sharing protocol X-Road, Estonian service providers can share user data in a secure way while still allowing changes to be recorded on the blockchain. This form of digital public infrastructure allows the government to provide its services more efficiently, securely and conveniently to citizens, forming the concept of a digital society e-Estonia. The unified platform allows citizens to see everything from their tax dues to their drivers license renewal date in one place. While the data is owned by each individual party, it is shown and made available to the user in a unified interface. When someone pays their taxes, renews their license, or buys a new house, that change is recorded by the tax authority, DMV, or Property registry, and that update is recorded on the blockchain. Because the update was recorded on blockchain, if there is ever a corruption or dispute about the data the DMV has, for example, the blockchain reference can be used to validate or invalidate truth from the timestamped event record.	Estonia became the first country to implement blockchain technology in its digital government services in 2012, and has leveraged it as a backbone of digital public infrastructure since. One of the key enabling factors of innovation in Estonia was their early adoption of bold regulation around digital services, such as the Principles of Estonian Information Policy. Establishing cornerstone legislation like the Digital Signature Act in 2000, which was updated in 2016, the requirements and protocols required for a Digital Signature to be legally binding were clear before any scaled infrastructure was established. This clarified technological requirements or uncertainty for new software providers or legacy businesses looking to provide legally binding services online. Similar such legislation in the EU such as Open Banking law and GDPR have consequently become pillars of directional clarity for the evolution of digital infrastructure.	As a layer of immutable data record, citizen activities interacting with public services including healthcare, land titling, taxes, and more, are all time stamped and recorded on a blockchain. The integration of x-roads and blockchain enable user-friendly and cohesive interaction points for citizens to access government services digitally.	All Estonians have access to a state-issued digital identity, the e-ID card. Alongside, the country has also offered a digital wallet to enable secure identification, digital signatures, and document storage on mobile devices.	The Identity Documents Act requires all residents, citizens or non-citizens, living permanently in Estonia to possess an identity document which includes a digital identity	The e-ID card is the cornerstone of Estonia’s model of an e-state, embracing digital governance at its core, and all the services it provides digitally.

Guatemala	The Guatemalan government has committed to implementing a complete DPI system within the next five years as part of the "50 in 5" initiative[37].	Guatemala is developing legal frameworks for interoperability and digital authentication, including using advanced electronic signatures.	The system under development seeks to enable interoperability between agencies, facilitating the secure exchange of information.	The country is working on implementing an interoperable digital identity system to improve access to public services.	Guatemala is developing legal frameworks for digital authentication and interoperability of services.	Digital authentication will facilitate citizen access to multiple government platforms, allowing identity verification across various services.
Mexico	Mexico has implemented the instant interbank payment system (SPEI), which has been expanded with the CoDI platform for mobile payments.	The country has regulations on personal data protection and a framework for interoperability through PKI, applicable to both the public and private sectors.	SPEI and CoDI have transformed digital payments in Mexico, facilitating financial inclusion through interoperable platforms.	They are used for authentication in payment services and access to government platforms.	Personal data protection laws and a PKI infrastructure support the use of digital identity in Mexico.	Digital identity is essential for using CoDI, enabling instant payments and facilitating the integration of financial services.
Uruguay	Uruguay uses a centralized platform, managed by AGESIC, that facilitates data interoperability between government agencies.	Uruguay has an advanced regulatory framework for data interoperability and digital authentication, supported by its PKI infrastructure.	The "ID Uruguay" system allows citizens to access public services through a unique digital identity, improving service delivery digital identity.	The "ID Uruguay" system allows citizens to authenticate themselves to access public services digitally.	Uruguay has an advanced regulatory framework around digital identity, supported by its PKI infrastructure.	Digital authentication facilitates citizens' access to a wide range of public services, simplifying government procedures.

(PART 3) REGULATORY CONSIDERATIONS

Regulatory interventions are an essential driver for the wider adoption of digital identity. Robust frameworks for data governance, privacy, and citizen services provide the impetus for innovative approaches to reusing digital identity data.

In the last two years, many countries have introduced regulations along these lines, with the intent of enabling the efficient delivery of citizen services through digital public infrastructure. Organizations such as the Global Acceptance Network (GAN)[38], which focuses on enabling a sustainable layer of decentralised digital trust infrastructure, have also given this issue attention[39].



GAN Trust Framework
GAN Organization
Members
Board
Team
Advisory Councils
GAN Infrastructure
Member Management System
Trust Registry of Registries
Verifiable Data Types Registry
Privacy-Preserving Communication
Privacy-Preserving Value Exchange
GAN Trust Network
Ecosystem of Ecosystems/ Network of Networks
Truly Interoperable
GAN Common Baseline Conformance
Ecosystem N
Ecosystem 2
Ecosystem 1

Approaches such as the one illustrated above envision the presence of public directories. This, in turn, implies the need for a decentralized directory protocol[40] - developed as part of the Finternet. The DeDi Protocol offers a standardized, open-source specification that can be integrated into existing or new systems. It aims to unify diverse implementations, ensuring interoperability and trust across the ecosystem.

In this section, we will introduce three examples of regulatory frameworks of digital identity and digital wallet systems, the Bhutan NDI, UAE framework, and EU eIDAS initiative. These are meant to present examples of how focused improvements in the regulatory environment have resulted in better infrastructure, standards, and deployments being made available to citizens.

UNITED ARAB EMIRATES

The Federal Authority for Identity, Citizenship, Customs & Port Security (ICP) is the main administrator of ID, customs authorities and border security services across the UAE. The Authority was established in September 2004 as “"Emirates Identity Authority"” under Federal Law No. (2) for the year 2004 to establish the “Population Register and Emirates Identity Card Program”, which included recording personal and vital data for all population in the state and keeping them in electronic databases in coordination with the competent authorities, and issuing the Emirates ID Card for each individual to be registered and to contain the Emirates ID number, readable data and data stored on an electronic chip, which can be used in all entities."

On the other hand, the main regulation governing Know Your Customer (KYC), Customer Due Diligence (CDD), Enhance Due Diligence (EDD), and Simplified Due Diligence (SDD) activities is Federal Decree Law No. 20 of 2018 on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT). To enable better execution of the law, the UAE Government has issued Cabinet Decision No. 10 of 2019, which provides further guidance on compliance expectations for KYC AML and CFT requirements. The Central Bank of UAE (CBUAE) has also issued "Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations" detailed guidelines for financial institutions for better understanding and clarity on the application of KYC, CDD, EDD, and SDD requirements.

It is also important to note that there are other KYC regulations that may be established by regulators located across the UAE (e.g., Abu Dhabi Global Markets, Virtual Assets Regulatory Authority, and a large number of other authorities); however, all these regulations are separate and do not contradict the spirit and approved direction of the aforementioned Federal laws.

Drivers for Digital Identity:

1. 1. ICP is the main custodian/driver for adopting Digital ID services specific to affirming persons and organizations legal status in the UAE, and customs and borders protection and security, and has established proper governance, controls and systems for these purposes and is constantly improving those to enable the transition to a highly efficient and effective ecosystem that caters to the needs of the millions living and organizations transacting in the UAE.

   Moreover, it gauged the interest of many semi-government and private sector entities in adopting Digital ID services to identify and verify persons and organizations. ICP also works with local agencies and departments that are focused on achieving digital enablement, and integration happens between its systems (e.g., UAE Pass) and local government agencies and departments' web applications.

2. CBUAE is the main custodian/driver for adopting Digital ID services specific to identifying, verifying and affirming persons and organizations financial diligence status (KYC, CDD, EDD, and SDD). It does so by ensuring all banking and financial sector actors comply with federal laws, decisions and regulations. Local regulatory authorities provide their Digital ID services while aligning with the expectations and requirements set forth by federal laws and overseen by the CBUAE.

BHUTAN NDI INITIATIVE[41]

The Kingdom of Bhutan launched a national digital identity[42] system in 2023 adopting SSI as a design pattern with which to develop a nation-scale digital trust ecosystem. Adopting the "Digital Trust Ecosystem Building Blocks" model proposed by the Trust Over IP Foundation (ToIP), the Bhutan NDI[43] includes trust registries, trust enabling systems, governance and ecosystem parties who participate in the system. The NDI Act of Bhutan[44], 2023 provides the overarching governance for the digital trust ecosystem.

It is important to understand that given the wide ranging impact of the NDI project, the stakeholders included the Department of Civil Registration and Census, the Department of Immigration and other agencies. The VCs issued as part of the project cover foundational digital identities and permanent address credentials as well as permits issued for tourism, residency and other purposes. The "trust registries" (NDI Trust Registry and Verifiable Data Registry) are enabled through the inclusion of a vLEI (Verifiable Legal Entity Identifier) issued to trusted parties. With organizations from a cross-section of institutions being involved in the NDI effort, the value is unlocked through the wider acceptance network achieved by including academic institutions, BFSI sector, Telcos and others.

At present the set of verifiable data which can be presently issued, exchanged and verified include foundational ID, permanent address credential, academic credential, employment related information, mobile number, driver's license, vehicle ownership etc. The NDI initiative also enables the creation of self-attested credentials which can be presented during eKYC workflows.

REGULATORY APPROACHES IN THE EU

EU eIDAS 2.0 Regulation

eIDAS 2.0 represents a significant upgrade to the European Union's electronic Identification, Authentication, and Trust Services (eIDAS) regulation. This enhancement aims to refine and expand cross-border digital identity solutions and trust services, allowing citizens and businesses to securely access a wide range of public and private services across the EU.

By enhancing trust services and website authentication, eIDAS 2.0 ensures that transactions across European Union Member States are secure and legally recognized, promoting greater trust, interoperability and reliability in digital interactions.

The three pillars of the regulation are the following:

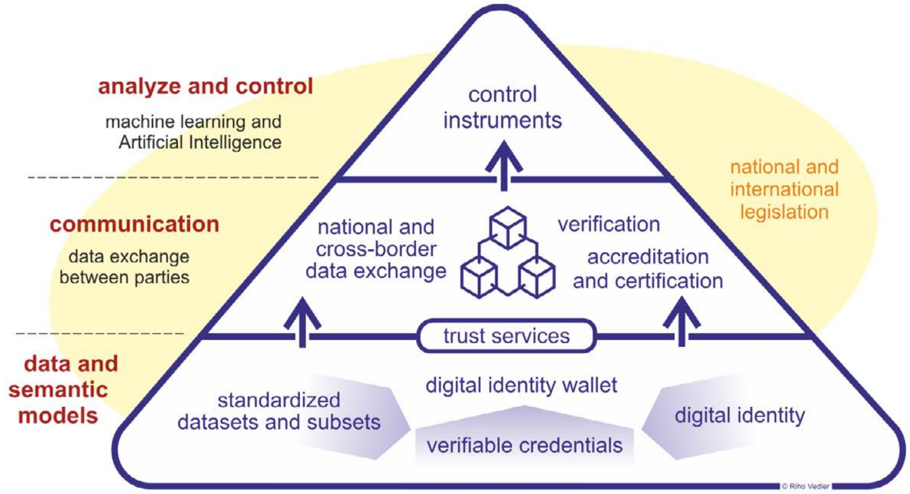
1. eID Schemas. Allows individuals to prove their identity digitally when accessing services. Each EU member state establishes these schemes and can vary in implementation but must comply with eIDAS standards for cross-border recognition. The eIDAS framework defines three levels of assurance for eID schemes:
   a. Low: Suitable for low-risk transactions, offering basic security.
   b. Substantial: Provides a higher level of security and is suitable for moderately sensitive transactions.
   c. High: Offers the highest level of assurance for high-risk or sensitive transactions, such as financial services.
2. EUDI Wallet. A secure, digital identity wallet solution enables citizens and businesses to store and manage their personal information, credentials1, and documents (e.g., ID, driver's license, banking details) in one place. It allows users to authenticate themselves and access online (trust) services across the EU, including cross-border services, without needing multiple logins or paper documents.
3. Trust Services. The legal framework is built upon acceptance, mutual recognition and equal conditions. Digital services that ensure the security, authenticity, and legal validity of electronic transactions.

In summary, key components include trust frameworks, legal recognition, a common set of rules and eIDAS cross-border standards, and legal recognition across Member States.

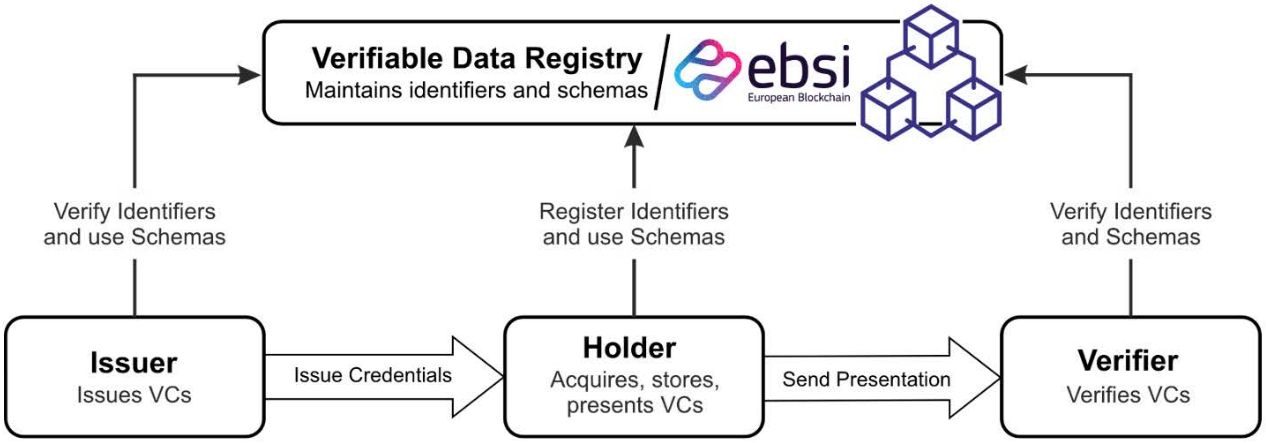
Categories of qualified trust services

- Electronic (digital) Signatures. An electronic way for a person to agree to a document or data. Qualified Electronic Signatures hold the same legal weight as handwritten ones.
- Electronic Seals. Like a traditional business stamp, it can be used on electronic documents to ensure their origin and integrity.
- Timestamps. Connects an electronic document, like a purchase order, to a specific time, proving the document existed then.
- Electronic Certificates. Electronic certificates that show your customers that your website is safe and reliable. They confirm the website is connected to the certificate holder and help prevent data phishing.
- Electronic Registered Delivery Services enable users to send data electronically. They offer proof of sending and delivery, safeguarding companies from loss, theft, damage, or unauthorized changes.

Technical infrastructure


analyze and control
machine learning and Artificial Intelligence
control instruments
national and international legislation
communication
data exchange between parties
national and cross-border data exchange
verification
accreditation and certification
trust services
data and semantic models
standardized datasets and subsets
digital identity wallet
verifiable credentials
digital identity
© Riho Vedler

Verifiable Credentials Data Exchange Model 2.0 and EBSI


Verifiable Data Registry
Maintains identifiers and schemas
ebsi
European Blockchain
Verify Identifiers and use Schemas
Register Identifiers and use Schemas
Verify Identifiers and Schemas
Issuer
Issues VCs
Issue Credentials
Holder
Acquires, stores, presents VCs
Send Presentation
Verifier
Verifies VCs

This model developed by the W3C promotes trust data exchange (for B2C, B2B, B2G, and C2G), privacy, and data sovereignty, ensuring compliance with GDPR, Interoperable Europe Act and other regulatory frameworks. By EBSI supported verification service based on ‘Zero Trust Architecture.

EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE AND BLOCKCHAIN NOTES

European Blockchain Services Infrastructure (EBSI) complements eIDAS 2.0 by enabling trusted, blockchain-based digital transactions, while EUDI ensures seamless identity verification. Together, they enhance secure cross-border digital interactions.

The EBSI comprises a peer-to-peer network of interconnected nodes running a blockchain-based services infrastructure. Each European Blockchain Partnership (EBP) member – the 27 EU countries, Norway, Liechtenstein and the European Commission – will run at least one node.

The infrastructure is made up of different layers, including:

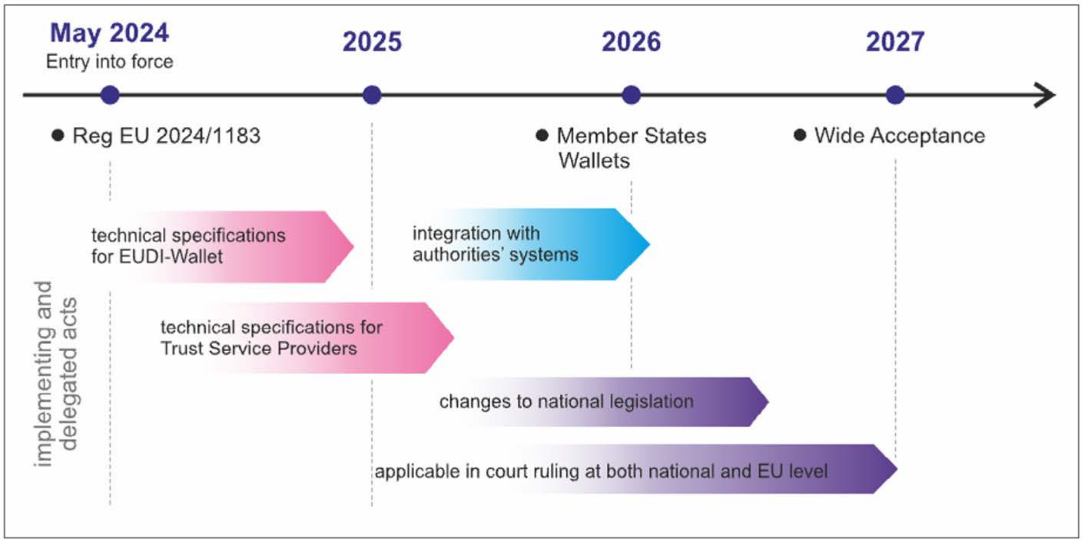
- a base layer containing the basic infrastructure, connectivity, the blockchain and necessary storage;
- a core services layer that will enable all EBSI-based use cases and applications;
- additional layers dedicated to use cases and specific applications.

POSSIBLE SERVICES TO BE DEVELOPED[45]

Generic relevant regulatory areas: AI, Environmental, Social & Governance (ESG), commercial registers, cybersecurity, consumer protection, competition law, customs, data protection & data regulation, Digital identity, Batteries/Digital product passports, Trade finance
Sector specific relevant regulatory areas: Automotive, cryptoassets, energy & utilities, education, financial markets, government, healthcare, media, retail, trade & logistics

- **Logistics, trade and trade finance.** eIDAS 2.0 with trust services (electronic signature, eSeal, etc.) enables seamless cross-border transactions by verifying identities, signing documents electronically, and securing data exchanges. This fosters smoother supply chain operations, efficient customs processing, and more secure trade finance, driving increased trust and transparency across these sectors.
- **Financial Services.** Speed up account opening by reusing existing verified identities. Improve KYC and fraud protection through richer identities.
- **Licenses.** Digital documents, such as identity and health documents, driving licenses, vehicle registration and voter cards, are always kept and carried in the safest and most convenient place possible.
- **eGovernment.** Increases efficiency and reduces manual processes by reducing in-person appointments. Automate data exchange between government agencies.
- **Travel & Hospitality.** Digitalize customer check-in and registration. Speed up processes and reduce manual labor through increased automation.
- **Mobility.** Automate customer onboarding and speed up driver license verification. Benefit of a European standard that works for various markets.
- **Telecommunications.** Speed up registration for prepaid cards by using existing verified identities. Improve fraud detection through richer identities.
- **eHealth.** Store health information and access other relevant information. Increase efficiency and effectiveness through reduced data handling and GDPR compliance.

Implementation indicative timeline


May 2024
Entry into force
2025
2026
2027
Reg EU 2024/1183
Member States Wallets
Wide Acceptance
implementing and delegated acts
technical specifications for EUDI-Wallet
integration with authorities' systems
technical specifications for Trust Service Providers
changes to national legislation
applicable in court ruling at both national and EU level

Source: DigitalTrade4.EU

eIDAS 2.0 was adopted by the European Parliament in February 2024 and is already published in the Official Journal of the EU. It entered into force on 20 May 2024.

- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework https://eur-lex.europa.eu/eli/reg/2024/1183/oj

EU Member States must implement trust services within 24 months after the implementing legislation is adopted.

RELATED ACTS (EUDI WALLET)

Status: The public feedback period has ended (09 September 2024). After approval by the European Parliament, they will be published in the Official Journal of the European Union.

1. **Trust framework** [link]
   It aims to ensure that the electronic notification system established by the European Commission acts as a secure and transparent communication channel for exchanging information between the Commission and the Member States.
2. **Protocols and interfaces to be supported** [link]
   It aims to ensure the proper implementation of protocols and interfaces crucial for the effective operation of the wallets.
   By supporting common protocols and interfaces, the wallets can guarantee:
   - successful issuance and presentation of identification data and electronic attestations;
   - successful data sharing between wallet units; and
   - efficient communication with relevant parties.
3. **Integrity and core functionalities** [link]
   It aims to lay down rules to ensure that Member States provide wallets that are interoperable and can be used for all their intended purposes. For example, the wallets should enable:

- ○ secure online cross-border identification for a wide range of public and private services;
- ○ sharing of electronic attestations; and
- ○ issuance of electronic signatures.

4. **Person identification data and electronic attestations of attributes** [link]
   It aims to ensure the smooth lifecycle management of both personal identification data and electronic attestations, covering issuance, verification, revocation and suspension. This guarantees that users' personal identification data and electronic attestations are issued to the wallet and can be disclosed to relevant parties.
5. **Certification** [link]
   This initiative aims to lay down the requirements for certification of the conformity of European Digital Identity Wallets. Where Member States cannot use European cybersecurity certification schemes based on Regulation (EU) 2019/881 or if such schemes are not sufficient, they must establish national certification schemes to supplement them. These schemes must, for instance, specify the competence requirements and an evaluation process.

RELATED ACTS (TRUST SERVICES)

Status: To be published 1 quarter 2025 to public feedback.

1. **Cross-border identity matching [link]**
2. **Security breaches [link]**
3. **Registration of relying parties [link]**
4. **Verification of electronic attestation of attributes [link]**
5. **List of certified wallets [link]**

(PART 4) RECOMMENDATIONS

Digital ID systems are making the leap from merely a digital identifier to a multi-purpose reusable set of identifiers that have significant impact on the lives of individuals and the workflows of organizations. To ensure that new technologies and capabilities are introduced while continuing to offer the benefits of a fair, equitable, secure and inclusive digital identity, it is important to examine the recommendations below.

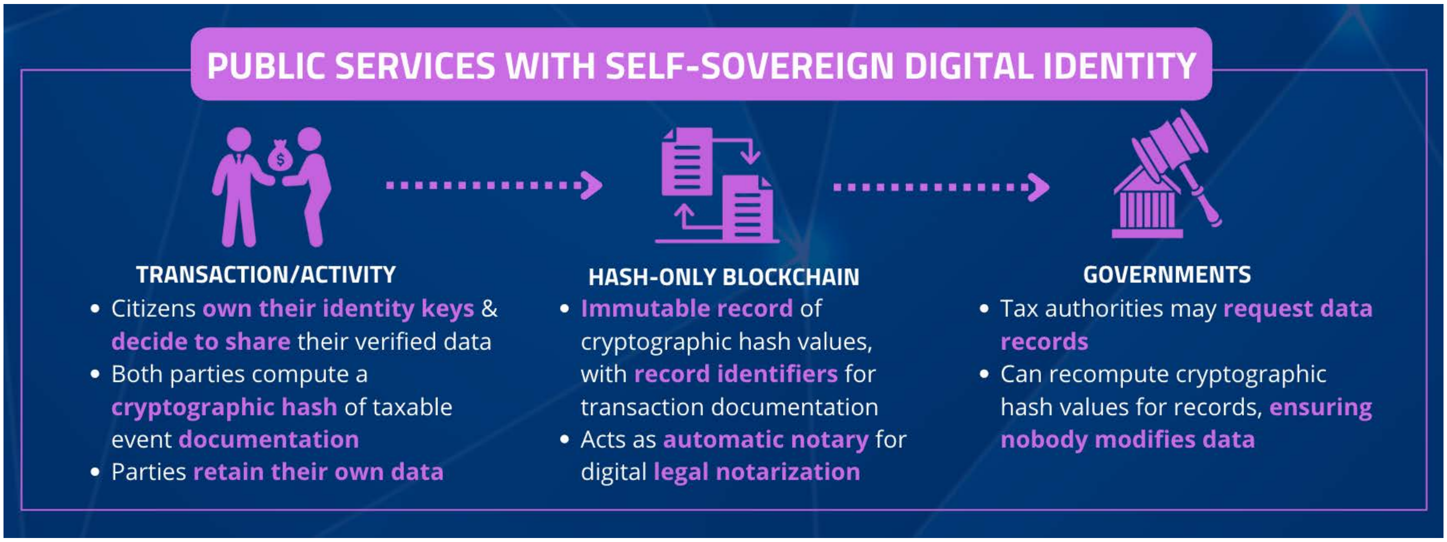
Recommendations for impact-driven Digital ID systems

- Adopt a Privacy-by-Design Approach
  ○ Incorporate privacy protections into the digital identity system from the outset, ensuring minimal data collection and anonymization where possible.
  ○ Allow users to control their data, with options to consent to sharing and revoke access at any time.
  ○ Encrypt sensitive information both at rest and in transit to prevent unauthorized access.
- Ensure Universal Accessibility and Inclusivity
  ○ Design the system to accommodate people of all abilities, including those with disabilities, low literacy levels, or limited technical skills.
  ○ Provide multilingual support and alternative offline registration options for individuals in remote or underserved areas.
  ○ Make participation voluntary and offer alternative forms of identification for those who opt out.

- Develop Robust Legal and Regulatory Frameworks
  - Establish clear laws that govern data protection, user rights, and the accountability of system operators.
  - Create mechanisms for independent oversight and redress in cases of misuse or grievances.
  - Define clear penalties for data breaches and misuse by government or private entities.
- Promote Interoperability and Open Standards
  - Use open standards to ensure the system can integrate with existing public and private services.
  - Enable cross-border recognition of digital identities for international travel and trade while maintaining national sovereignty over data.
  - Allow flexibility for future upgrades to keep pace with technological advancements.
- Implement Advanced Security Measures
  - Use multi-factor authentication to verify identity securely.
  - Employ biometric data cautiously, ensuring it is stored securely and used only for authentication purposes.
  - Conduct regular security audits and simulate potential attack scenarios to strengthen the system against threats.
- Address Digital Divide Challenges
  - Provide affordable and widespread access to necessary technology, such as smartphones or biometric devices.
  - Partner with local organizations to educate communities about the benefits and use of the digital identity system.
  - Invest in infrastructure improvements to support reliable internet connectivity in rural and remote areas.
- Foster Public Trust and Awareness
  - Engage communities through public consultations to ensure their needs and concerns are addressed in the system’s design.
  - Be transparent about how the system works, what data is collected, and how it is used.
  - Run public awareness campaigns to inform citizens about the system’s benefits and security measures.
- Guarantee Non-Discrimination and Equity
  - Conduct impact assessments to identify and mitigate risks of exclusion or bias in the system.
  - Avoid embedding discriminatory algorithms or practices that could marginalize vulnerable populations.
  - Ensure equitable treatment regardless of socioeconomic status, gender, ethnicity, or geographic location.
- Enable Decentralized and Federated Models
  - Explore decentralized digital identity architectures to reduce reliance on a single central authority and enhance resilience.
  - Use federated systems to allow individuals to use a single ID across multiple domains without risking privacy or security.
- Monitor, Evaluate, and Evolve the System
  - Set up mechanisms for continuous monitoring and evaluation to identify issues and areas for improvement.
  - Incorporate feedback loops to adapt the system based on user experience and technological developments.

Regularly update the system to incorporate advances in security, privacy, and inclusivity.

By adhering to these recommendations, policy makers, bureaucrats, technologists and other stakeholders can collaboratively develop a digital identity system that is fair, equitable, secure, and inclusive, fostering trust among users and contributing to societal advancement.



PUBLIC SERVICES WITH SELF-SOVEREIGN DIGITAL IDENTITY

TRANSACTION/ACTIVITY

- Citizens **own their identity keys** & **decide to share** their verified data
- Both parties compute a **cryptographic hash** of taxable event **documentation**
- Parties **retain their own data**

HASH-ONLY BLOCKCHAIN

- **Immutable record** of cryptographic hash values, with **record identifiers** for transaction documentation
- Acts as **automatic notary** for digital **legal notarization**

GOVERNMENTS

- Tax authorities may **request data records**
- Can recompute cryptographic hash values for records, **ensuring nobody modifies data**

(PART 5) CONCLUSION

As societies globally continue to embrace digital transformation, digital identity systems are poised to play a central role in enabling secure access to services, fostering economic growth, and promoting social inclusion. These systems are evolving beyond mere identity verification to becoming dynamic platforms that integrate with a wide range of public and private services, from financial inclusion and healthcare to cross-border mobility and e-commerce. The trajectory of digital identity systems points toward greater interoperability, decentralization, and personalization, making them a cornerstone of modern digital economies.

Emerging trends indicate a growing emphasis on privacy-enhancing technologies (PETs) such as zero-knowledge proofs and decentralized identifiers (DIDs). These innovations aim to balance the dual imperatives of data security and user convenience, empowering individuals to control their digital identities while minimizing exposure to privacy risks. Additionally, artificial intelligence and machine learning are expected to refine the efficiency of identity verification processes, ensuring faster and more accurate authentication.

The integration of digital identity systems with blockchain technology is a promising development, offering immutable record-keeping and enhanced transparency. Furthermore, the rise of global standardization efforts suggests a future where digital identities can facilitate seamless cross-border interactions, unlocking new possibilities for international trade, migration, and cooperation.

However, this bright future comes with significant challenges and risks. One major concern is the potential for digital identity systems to exacerbate existing inequalities. Without equitable access, marginalized populations could face further exclusion from essential services. Similarly, the misuse of personal data, whether through data breaches or unwarranted surveillance, threatens individual privacy and public trust. Biometric data, while secure, raises ethical questions and must be handled with utmost care to avoid misuse.

Cybersecurity remains a persistent risk as attackers target digital identity infrastructures. Sophisticated cyberattacks could undermine the reliability of these systems and erode user confidence. Additionally, poorly designed or biased algorithms in identity verification could perpetuate discrimination, undermining efforts to create fair and inclusive systems.

The success of digital identity systems will depend on collaboration between governments, private entities, civil society, and international organizations. By working together, stakeholders can create systems that are not only secure and efficient but also inclusive and empowering. The opportunity to transform lives is immense—providing people with a digital identity can unlock access to opportunities, reduce barriers to participation, and drive innovation across sectors.

While challenges and risks are inevitable, the future of digital identity systems holds immense promise. By embracing a people-centric, privacy-preserving approach, these systems can serve as powerful tools for progress, bridging gaps and enabling a world where everyone has the opportunity to thrive in the digital era.

ENDNOTES:

1. https://en.wikipedia.org/wiki/Digital_identity (accessed on 14th October, 2024)
2. https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2#what-are-digital-identities (accessed on 14th October, 2024)
3. https://www.sezoo.digital/
4. https://www.linkedin.com/posts/sezoo_trustworthy-digital-ids-as-a-foundation-for-activity-7240235397006442497-hCrj/ (accessed on 20th October, 2024)
5. Umar Bashir Mir, Arpan K. Kar, Yogesh K. Dwivedi, M.P. Gupta, R.S. Sharma, Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India, Government Information Quarterly, Volume 37, Issue 2, 2020, 101442, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2019.101442
6. https://sovrin.org/principles-of-ssi/ : Principles of Self-Sovereign Identity published by The Sovrin Foundation (accessed on 14th October, 2024)
7. https://www.bhutanndi.com/ : Bhutan NDI (accessed on 14th October, 2024)
8. https://mosip.io/ : MOSIP (accessed on 14th October, 2024)
9. https://www.digitalpublicgoods.net/ : Digital Public Good Project (accessed on 14th October, 2024)
10. https://pages.nist.gov/800-63-4/ (accessed on 7th October, 2024)
11. https://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf
12. https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf
13. https://www.ibia.org/download/datasets/5741/IBIA%20Ethical%20Use%20of%20Biometric%20Technology%20FINAL.pdf
14. https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf
15. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/
16. https://www.iom.int/news/west-africa-moves-towards-biometric-identity-cards (accessed on 2nd November, 2024)
17. https://nationalpopulation.gov.ng/press-release/launching-of-the-national-geospatial-data-repository-the-digital-civil-registration-and-vital (accessed on 2nd November, 2024)
18. https://projects.worldbank.org/en/projects-operations/project-detail/P179040 (accessed on 2nd November, 2024)
19. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099090424093523075/p505094127c43207b1a297190f5dac37edb (accessed on 2nd November, 2024)
20. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099061523065541763/p18049509fb3f3000b48602cc780351af2 (accessed on 2nd November, 2024)
21. https://stellar.org/case-studies/unhcr
22. https://stellar.org/blog/thought-leadership/one-year-of-stellar-aid-assist
23. https://www.worldbank.org/en/news/press-release/2024/05/21/global-carbon-pricing-revenues-top-a-record-100-billion
24. https://www.worldbank.org/en/news/factsheet/2024/11/12/carbon-markets
25. https://gbbcouncil.org/wp-content/uploads/2023/11/CET-Protocol-IWA-November-2023.pdf
26. https://toronet.org/agrifi-2/
27. https://toronet.org/wp-content/uploads/2024/06/Toronet-Whitepaper.pdf

28. https://cdpi.dev/ (accessed 10th November, 2024)
29. https://www.nsw.gov.au/media-releases/digital-roadmap-drives-innovation-and-delivers-for-communities (accessed 10th November, 2024)
30. https://publicsafety.ieee.org/topics/high-tech-border-security-current-and-emerging-trends
31. https://www.cbp.gov/border-security/along-us-borders/us-border-patrol-technology
32. https://www.trade.gov/country-commercial-guides/italy-digital-economy
33. https://www.agid.gov.it/en/intervention-areas/digital-identity
34. https://www.italiadomani.gov.it/en/Interventi/investimenti/infrastrutture-digitali.html
35. https://www.agid.gov.it/en/news/the-italian-strategy-for-artificial-intelligence
36. https://blockworks.co/news/buenos-aires-id-ethereum-zksync (accessed 14th November, 2024)
37. https://50in5.net/
38. https://gan.foundation/ (accessed on 12th November, 2024)
39. https://identifinity.net/what-is-the-global-acceptance-network-gan-and-do-we-need-it-e4fc2147ee0b (accessed on 12th November, 2024)
40. https://github.com/finternet-io/dedi (accessed on 12th November, 2024)
41. https://www.bhutanndi.com/article/bhutan-s-national-digital-identity-embodies-the-king-s-vision-of-a-digitally-connected-prosperous-society_3a777c24-8891-480b-9b02-e583ba1565da
42. https://parliament.bt/uploads/topics/16920885498838.pdf
43. https://www.bhutanndi.com/company/vision-mission
44. https://parliament.bt/national-digital-identity-act-of-bhutan-2023
45. https://digital-strategy.ec.europa.eu/en/library/european-blockchain-sandbox-best-practices-report

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland