SELF-SOVEREIGN IDENTITY

The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain

IDB IDB | LAB LACCHAIN

SELF-SOVEREIGN IDENTITY

The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain

Author: Marcos Allende López (@marcosallendeL)
Supervisors: Marcelo Da Silva and Alejandro Pardo Vegezzi

Design: .Puntoaparte Editors

This document was produced in collaboration by the LACChain Global Alliance digital identity working group. Without the direct and indirect contributions of each and every member of this group, this publication would not exist. Special appreciation to Kenneth Foley, Ignacio Alamillo, Suzana Maranhão, Paula Ventoso, Melissa Julian, Melissa Penteado, Mariano Sturla, María Weisson, Andrea Ortega, Itzel Nava, Daniel Zarate, and the .Puntoaparte team for their essential contributions. Particularly grateful also to Nuria Simo and Irene Arias for their fundamental support. Last but not least, the document is dedicated to Marcelo Da Silva and Alejandro Pardo, with love and gratitude, for making it possible.

Author: Marcos Allende López.

Collaborators: Moisés Menéndez Andrés, Oscar Bazoberry, Ismael Arribas, Albi Rodríguez Jaramillo, David Ammouial, Juan José Miranda, Pelle Braendgaard, Andrew Hughes, Zaira Pérez, Antonio Leal, Adrián Pareja, Sergio Cerón, Diego Lopez, David Peces, Guillermo Villanueva, Pedro Perrotta, Jaime Centellas, Sergio Bazoberry, and Jesus Ruiz.

Reviewers: Ignacio Alamillo, Pelle Braendgaard, Kenneth Foley, Suzana Maranhão, Moises Menendez, and Ismael Arribas.

Supervisors: Marcelo Da Silva and Alejandro Pardo Vegezzi.

Table of Contents

Chapter I
The Future of Identity

Self-Sovereign Identity

IDB IDB | LAB LACCHAIN

Much of the world's population has access to advanced technology, and progress in implementing these technologies in some fields has been more successful than many had predicted. At present, people can fly to almost any place on the planet within a day and see a loved one's face across the globe in real-time with a videocall on a wireless device. However, there are fields where there is still much progress to be made in order to properly leverage existing digital technologies, such as the systems that create, store, protect, and track our identities, both physical and digital.

Today, the most reliable mechanism for physical identification and authentication consists of requesting a photo-ID document and establishing a match with attributes of our physical appearance. The ID verifier rarely has the appropriate technology to verify that the physical-ID is legitimate and, only in very specific places, a biometric check can be successfully utilized.

Regarding digital identification and authentication, a few countries are currently issuing ID cards for their citizens that allow access to electronic services in an authenticated manner. However, even in the most advanced countries, these services are generally limited to those offered by public administrations, rendering it impossible to use the ID cards to access services provided by private sector companies.

The inability to fully leverage available technologies in the field of personal identity has considerable consequences. Lack of proofs of identity, falsification of identity documents, identity theft, and loss of identity documents, among many other identity-related problems, are common. In vulnerable populations exposed to natural disasters or forced to migrate, the situation is even more critical. Each year, millions of people not only lose their homes, but also lose the identity documents that serve to prove who they are, where they are from, or what professional or educational experiences they may have.

Additionally, non-existent individual electronic identification and authentication mechanisms limits the digitalization of services, generates monopolies of intermediaries that only provide trust between parties, makes it almost impossible to verify sources of information, and is a restraint for data privacy and protection.

In recent years, we have seen the development of a set of standards, protocols, and technologies that seek to offer a new concept of identity with the potential to make it universal, cheap, safe, and scalable. It has the potential to solve the problems of current systems of identification and authentication and give individuals full control of their digital persona. This new identity model is known as self-sovereign identity and combines two innovative technological elements: digital wallets and decentralized registries of information.

As the name, self-sovereign identity, can be a bit misleading, it is important to clarify that self-sovereign identity does not entail individuals certifying their own identity. As long as societies are structured in non-anarchical political systems with well-defined government structures that guarantee and enforce laws while allowing for the establishment of public and private trust frameworks, the public administrations will still have the final sovereignty of the identification of citizens.

Therefore self-sovereign identity proposes sovereignty for the individual not in the issuance but in the management of their identity. Firstly, this model enables sovereignty for individuals over their digital assets and credentials -such as digital passports, digital diplomas, digital property titles, and tokenized currencies such as dollar, euro, pound, or pesos- using digital wallets that can take the form of a mobile app. Secondly, when the subject of these digital assets and credentials presents them to a third party to prove ownership, the third party does not need to reach out to the issuer to verify them, as they can go against a public, decentralized, and immutable registry, such as a blockchain network, where the cryptographic proofs of the asset or credential were registered and are maintained by the issuer in an standardized and trustable way.

SELF-SOVEREIGN IDENTITY

Block 1
Identity

1.1. Definition

The *identity* of a person, an organization, a thing, or a process refers to everything that characterizes them. For individuals, identity encompasses physical features, biometric information, experiences, belongings, titles, properties, relationships, and gender, among many others. Therefore, there are infinitely many attributes that make up our identities as human beings and most of them are in constant change and evolution.

The quantity of factors that contribute to identity makes having all these factors listed or collected at one time or stored in one place impossible. However, we can put together finite subsets of a person's attributes that are exclusive enough to be different from anyone else's, making them unique. Being able to define, collect, present, and verify these subsets in a standardized way allows human beings to prove who they are to others. This is known as authentication.

The authentication of an individual consists of convincing someone else that he or she can be reliably captured by a collection of identifiers and/or sets of attributes. This is typically based on attestations collected in one or several certificates (e.g. a passport) issued or certified by a third-party entity that is trusted by the entity the individual is aiming to prove their identity to. The third-party entity typically holds public "authority" or at least is recognized by the verifying entity as having the ability to recognize and remember individuals (e.g. a public administration).

Identity is defined in a similar way by different international agencies of standards:

"Identity is the representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context" – ITU (ITU, 2018)

"Identity is a set of attributes related to an entity" – ISO/IEC 24760-1 (ISO, 2019)

1.2. Identification as a Human Right

According to ISO/IEC 24760-1, "identification is the process of recognizing an entity in a particular domain as distinct from other entities" (ISO, 2019). Identification is essential to request and grant access to services of all kinds. Paradoxically, the Universal Declaration of Human Rights does not mention the word identity even once, nor does it explicitly recognize the right to be identified. However, it does recognize "the right to recognition everywhere as a person before the law" in Article 6, the "right to a nationality" in Article 15, and the "right to own property" in Article 17. In order to guarantee these human rights, people need to be identifiable. (UN, 1948) Thus, the right to have an identity and be identifiable is indirectly recognized.

In 2016, the Inter-Agency and Expert Group on Sustainable Development Goals indicators (AEG-SDGs) published a final list of Sustainable Development Goal indicators as a practical starting point for the United Nations. The Target 16.9 reads "by 2030, provide legal identity for all, including legal identity for all, including birth registration". (SDG, 2016)

At present, in most countries and regions of the world, governments are responsible for providing the first identity credential: the birth registry and associated certificate. The essential action behind this process is recording the person's information in a civil registry, which is maintained by the administration over time. The information stored as part of the birth registry process typically includes names, date and place of birth, nationality, parent(s), and physical characteristics among others. The person legally responsible for the newborn may receive a credential or certificate that represents the information present in the registry.

After birth, throughout the lifespan, humans generate several pieces of identifiable information and

we are issued credentials that, similar to our birth certificate, allow us to prove who we are to others. Some examples are government issued identification cards, diplomas, titles of registry, and digital footprints, including social network identities.

According to estimates by the World Bank ID4D Dataset in February 2016, some 1 billion individuals around the world lack proof of identity (WB-ID4D, 2018). Given this is 14% of the global population, it is clear that there is a major problem with the way identification works today. Not only does this problem bar 3 of every 20 people in the world from the human right of personal identity, but it also contributes to huge setbacks for global development, and social and financial inclusion, which will be explored in Block 4.

Since the beginning of the 20th century, the advent of the modern internet, smart phones, and the internet of things (IoT) have changed the type of services we consume and the way we socialize as human beings. The digitalization of our lives has introduced new challenges and opportunities for the identification of individuals, which is essential to a safe and organized society.

SELF-SOVEREIGN IDENTITY

Block 2
Digital Identity

2.1. Definition

As a natural extension of the definition of identity, a *digital identity* is a finite set of attributes that allows a person, an animal, a thing, or a process to be uniquely identifiable and to authenticate to others electronically. Our Digital Persona is a collection of digital identities. Each digital identity is represented by one or several identifiers and a set of attributes that are unique within a context.

Proving one's digital identity presents several challenges. For example, visual verification of identity is no longer valid in the way that it is with physical forms of identity. However, it also presents numerous advantages, as it allows us to have access to global digital services without the need for physical presence or a physical form of identity. This opens a wide variety of possibilities, many of which are related to inclusion: it allows for otherwise inaccessible services to be provided remotely in real time to communities and populations with limited in-person access.

As stated by the World Bank, digital identities are created and used as part of a lifecycle that includes four fundamental stages: (a) registration, including enrollment and validation, (b) issuance of documents or credentials, (c) identity authentication, and (d) authentication for service delivery or transactions. (WB-TS, 2018).

Digital identity is defined in a similar way by different international agencies of standards:

"For these guidelines, digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known."
– NIST (NIST-IDG, 2017)

"Digital identity is the sum of all digitally available data regarding an individual, regardless of its degree of validity, its form, or its accessibility, comprised of direct and inferred (or indirect) data." – OIX (OIX-TOOLS, 2019)

"Digital identity is the digital representation of an entity detailed enough to make the individual distinguishable within a digital context."
– ITU (EU-BDID, 2019)

Image 1. Examples of identity information in three different digital contexts.

2.2. Benefits of Digital Identity

As we claimed in the previous section, digital identity allows individuals to avoid the limitations of the physical world, and enables worldwide real-time trustable connections, transactions, and the provision and reception of digital services. In a world that is becoming more digital every-day, robust, useful, and scalable digital identity management systems are essential to be able to identify and authenticate ourselves electronically and to know who we are interacting with. This gives us control over our data by allowing us to decide who we would like to share it with and for what purposes.

According to McKinsey[1], "good Digital ID is identification that is verified and authenticated to a high degree of assurance over digital channels, unique, established with individual consent, and protects user privacy and ensures control over personal data". To them, this can "unlock value by promoting inclusion, formalization and digitalization. For example:

- 45% of women aged 15+ in low-income countries lack ID while only 30% of men do
- 1.7 billon people could gain access to financial services
- 90% of customer onboarding costs could potentially be reduced
- Digital ID could unlock economic value between 3-13% of GDP in 2030"

In Block 4 we will be analyzing in detail the potential of digital identity. In particular, we will be exploring the use of self-sovereign identity for financial and social inclusion. In this introductory section, we would like to present some of the benefits of digital identity for individuals and both the public and private sectors, depicted in Table 1.

Table 1. Benefits of digital identity.

Benefits for individuals	Benefits for public sector	Benefits for private sector
Convenience	Better service delivery	Commercial opportunities in cybersecurity
Usability	Reduction of costs for staffing	Commercial opportunities as identity providers
Reduction of costs	Reduction of costs for paper-based processes and storage	Reachability of customers
Inclusion	Reduction of costs for service delivery	Easier user verification
User experience	Data prepared for data analysis	Reduction on costs for service delivery
	More security	

1 https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/infographic-what-is-good-digital-id#

2.3. Issues with Current Digital Identity Management Systems

Digital identity management systems are evolving from completely centralized to more decentralized approaches in the pursuit of guaranteeing data protection, portability, and interoperability. As new technologies emerge, regulators gain a greater understanding of the digital world, governments and private entities find better ways to interact electronically, and users become more confident with all the previous, better digital identity management systems continue to be proposed and adopted.

As pointed out by the European Union (EU), "without a way to identify each other and our possessions we would hardly be able to build large nations or create global markets. Unfortunately, there are persistent –and increasingly serious– problems with the way digital identity works. Due to historical and other reasons, the digital identity experience today is fragmented, with few standards or interoperability, and it is insecure, as the almost daily reports of hacks and data breaches reminds us." (EU-BDID, 2019) We can classify the main issues of today's digital identity management systems into three categories: regulation, technology, and security.

2.3.1. Regulation and Standards

As societies become more digital, new ways of connecting and interacting between individuals and organizations require a constant evolution of the requirements for digital identification. First, it is essential to identify the different contexts in which electronic interactions exist so that standards and regulations can be adapted to support them if necessary.

One of the issues that electronic identification, authentication, and authorization face today is that the existing regulations on electronic transactions are mainly focused on a limited number of digital identities used for interactions between individuals and services provided by governments. There is a lack of frameworks that allow private entities to become qualified to provide trusted and qualified electronic services for identification, authentication, and authorization that cannot be repudiated by law. Further, it is also necessary to develop standards that allow cross border interoperability and recognition.

For example, in Europe, where we can find the most advanced frameworks and regulations for electronic identification (eIDAS) and data protection (GDPR), the definition in the eIDAS regulation of the role of Trust Service Provider (TSP) enables for private entities to be certified to provide services such as the creation, verification, and validation of electronic signatures, seals, or timestamps, among other services for the country members of the European Union. Certified entities can be found in the official trusted list of service providers[2] and are recognized internationally. Without these kinds of regulations and trust frameworks, non-discrimination of electronic signatures, seals, or timestamps cannot be guaranteed.

2.3.2. Technology

The current technology used for electronic identification of individuals is far from ideal. The most secure mechanisms used to access sensitive electronic services for government platforms are either X.509 certificates or chip cards. In both cases, costs for generation are high and key recovery is difficult.

X.509 certificates are generally stored in specific servers or computers, which makes portability hard to achieve. Additionally, they do not allow pseudonymity, as the subject's personal information is reflected in the certificate. In the case of chip cards and passwords, individuals are generally required to have a combination of these two elements for each service they want to access, and chip cards can also be easily lost or theft. This makes their use highly unpractical.

2 https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

Suitable technological tools used for electronic identity proofing, authentication, and authorization should at least have the following seven essential requirements:

Interoperability: accessible to all kinds of public and private services
Portability: ability to take one's digital identifier credentials anywhere
Pseudonymity: ability to interact without disclosing one's real identity
Recovery: able to retrieve keys and credentials easily and safely
Scalability: feasible for adoption and replication
Security: protects data and information, including keys and credentials
Usability: human-meaningful and good user experience

Complying with these seven requirements would require a total technological paradigm change, such as an evolution from the use of X.509 and chip cards to something more robust. First, in terms of credentials, a new solution that allows pseudonymous interaction with the same level of assurance of the unpractical X.509 and chip cards is required. Second, in terms of storage and management, the ability to manage credentials in a user-friendly, portable, safe, and usable way, guarantying security and recovery is necessary. Last but not least, the combination of the new digital credentials and the management devices must allow us to access all kind of digital services, both public and private.

2.3.3. Security

Currently, individuals are not in control of their digital identities because they are not in control of their digital authenticators, data, and credentials. We do not own the information about ourselves stored on the internet. Even information accessed via username and password (e.g. banking information or social network profiles) is stored in third-party databases that provide us with access to it.

Additionally, we are required to memorize several usernames and passwords to access these various digital services and platforms; often, we must have a different set of credentials for each site that requires authentication, unless we trust a third-party platform such as Facebook or Google to manage them when the option is available. With this approach, rights on data protection, such as consent, right to be forgotten, portability, and pseudonymization, that have already been recognized by different government regulations, as we will cover in Section 6.2, can hardly be guaranteed.

Overall, the large majority of our current electronic interactions either involve service providers giving us access to our own data and information that they ultimately control or involve third-party identity providers to manage our authenticators, with the ability to use them on our behalf. This leads to expensive costs for identity providers to build and maintain infrastructure and for service providers to store and protect that information. Additionally, these infrastructures are often vulnerable to data leakages. According to the US 2019 Consumer Data Breach Report (ForgeRock, 2019):

- In 2018, more than 2.8 billion consumer data records were exposed in 342 breaches at an estimated total cost of more than $654 billion.
- Unauthorized access was the primary type of attack in 2018, totaling 34% of all attacks.
- In Q1 2019, financial services breaches cost the industry $6.2 billion, a strong jump from only $8 million in Q1 2018.
- Healthcare was the most affected industry, with the sector falling victim to 48% of all breaches.
- Personal identifiable information (PII) was by far the most common type of breach in 2018, representing 97% of all breaches.
- Date of birth and/or Social Security Numbers were the most frequently compromised type of PII in 2018, with 54% of breaches exposing this data.

According to Gartner, although current identity management systems have offered usability improvements, they still have many weaknesses: (Gartner, 2020)

- Expensive to build and maintain

- Inefficient to establish and sustain real trust via identity proofing
- Prone to data proliferation and privacy abuse by way of data aggregation
- Exposed to privacy regulations due to the collection, storage, and analysis of the sensitive data
- The cause of myriad data quality issues due to many silos of information
- Vulnerable to security attacks with major data loss exposure (due to centralized repositories)
- Susceptible to identify theft due to a lack of control by the identity owner
- Are not censorship-resistant since identity providers can suspend accounts at their discretion

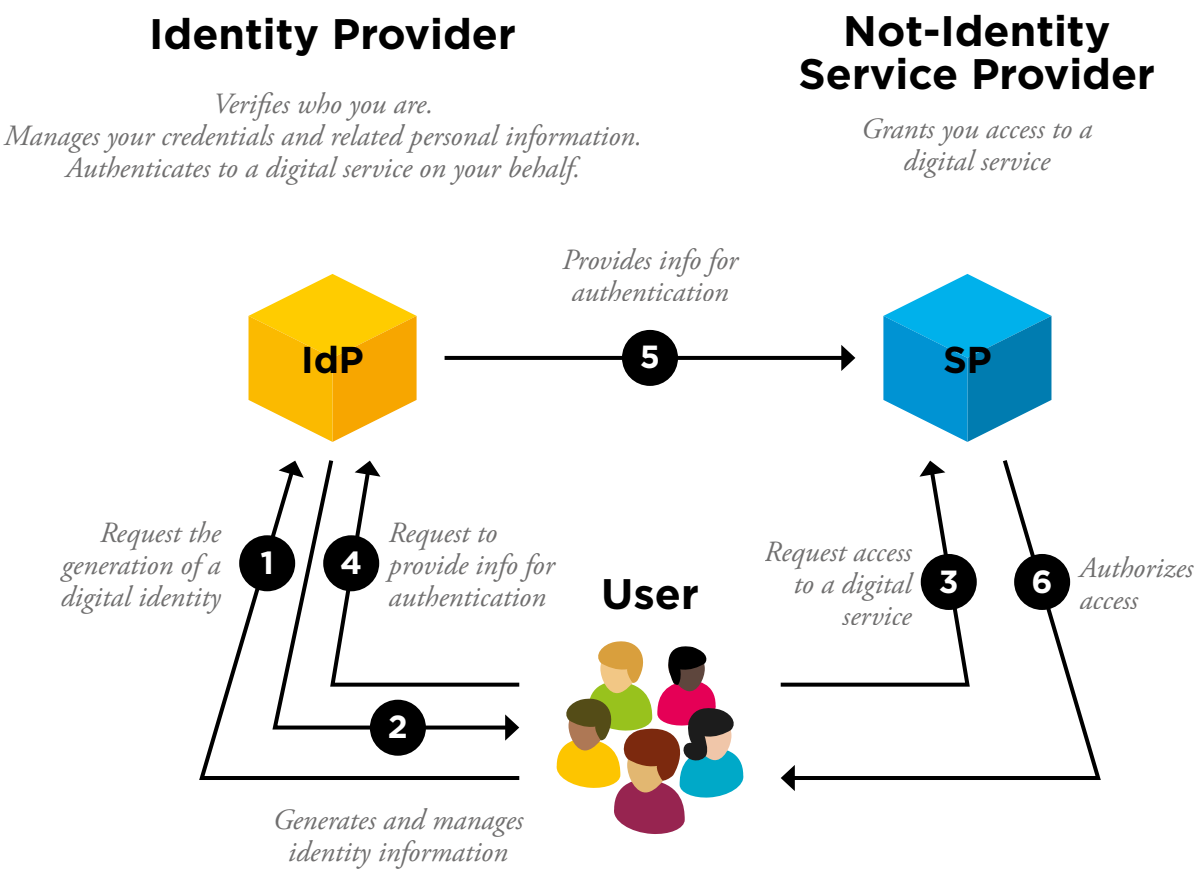
We believe that self-sovereign identity solutions can help mitigate all these issues, as we will argue in Sections 2.5, 3.1, and 4. In order to provide more context, let's take a look at the different digital identity management systems available today.

2.4. Overview of Digital Identity Management Systems

There are five different models or schemes of digital identity management systems: centralized, third-party provider, federated, user-centric, and self-sovereign identity. Before covering them, it is useful to introduce two important concepts: identity provider (IIP or IdP) and non-identity service provider (SP),

Identity provider (IIP or IdP): According to ISO/IEC 24760-1, an identity provider is "an entity that makes available identity information" (ISO, 2019). This includes identity information creation as well as maintenance and management of credentials on behalf of natural or legal persons, while providing authentication services to service providers or relying party applications.

Image 2. Relationship between Identity Provider, Non-Identity Service Provider, and User.

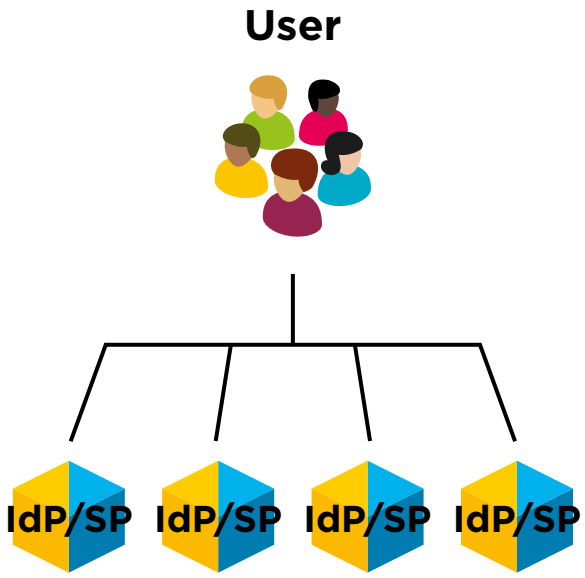


Non-identity service provider (SP): A service provider is any entity that provides a service for natural or legal persons. Some service providers also act as identity providers. In order to distinguish between entities acting as identity providers and entities providing any other kind of digital service, we introduce the concept of the non-identity digital service provider (SP), which are those entities who offer services other than identity services. For simplicity purposes we will refer to them as *service providers*, with the assumption that if the service provider is also an identity provider, we would call them an *identity provider* instead.

2.4.1. Centralized

The centralized identity model is the most basic and traditional digital identity management system. Here, every digital service one consumes is acting both as an identity and service provider. All websites we log in to with a username and password that is created when we signed up, such as social networks, e-mail platforms, and countless others, are within this centralized identity model.

Image 3. Simplified schema of the centralized identity model.



This model presents several disadvantages:

- Hacks are frequent as data is kept in centralized databases, which are not always well protected
- Users must memorize or store several authenticators because they must authenticate independently to each organization
- Organizations must take on high costs and large hardware infrastructure (either on-premise or cloud) to ensure user authenticators, credentials, and data are safe.
- Centralized databases are considerable liabilities for organizations and firms

2.4.2. Third-Party Identity Provider

In the third-party model, the identity provider and the service provider are different entities that communicate with each other. Every time a natural or legal person wants to access the digital service offered by the service provider, the person draws on their identity provider to authenticate on their behalf instead of authenticating directly to it. The communication between the identity provider and the service or resource is made through common protocols, standards, and frameworks, such as SAML (OASIS, 2008), OAuth (IETF, 2012), and OpenID.[3]

This practice has become popular with the advent of social networks such as Facebook and the domination of Google. For example, often instead of logging into a website with a username and password created for that website, we have the option to authenticate with a Facebook or Google account. It is also worth mentioning third-party identity providers Okta and Azure AD which are increasingly adopted by corporations to manage employees' identification, authentication, and authorization.

For clarification purposes, when Facebook or Google is accessed through their respective credentials, this represents a centralized model. When other services are accessed with Facebook or Google credentials, this represents a third-party identity provider model. In

3 https://openid.net/connect/

Table 2. Examples of the three different identity schemes with multiple identity providers, according to ITU. (ITU, 2018)

One unique identity provider	Multiple identity providers	Identity broker/s with multiple identity providers
The Aadhaar program in India (the largest in the world) The Estonian ID-card and Mobile-ID for a wide amount of private and public services The digital authentication system for Dutch government services DigID The Digital Identity issued by RENIEC in Peru The Finnish Population Registry in Finland, used for elections, tax filing, judicial administration, …	Italian SPID, for public administrative services, managed by the Agency for Digital Identity (AgID)	GOV.UK Verify program, an external authentication system that allows UK citizens to access different government services online using up to ten different identity providers

both cases, Facebook and Google are the identity providers, but in the second case, they are not the service providers -according to the terminology introduced in Section 2.4-. In both cases, the information and data is centralized within the identity provider.

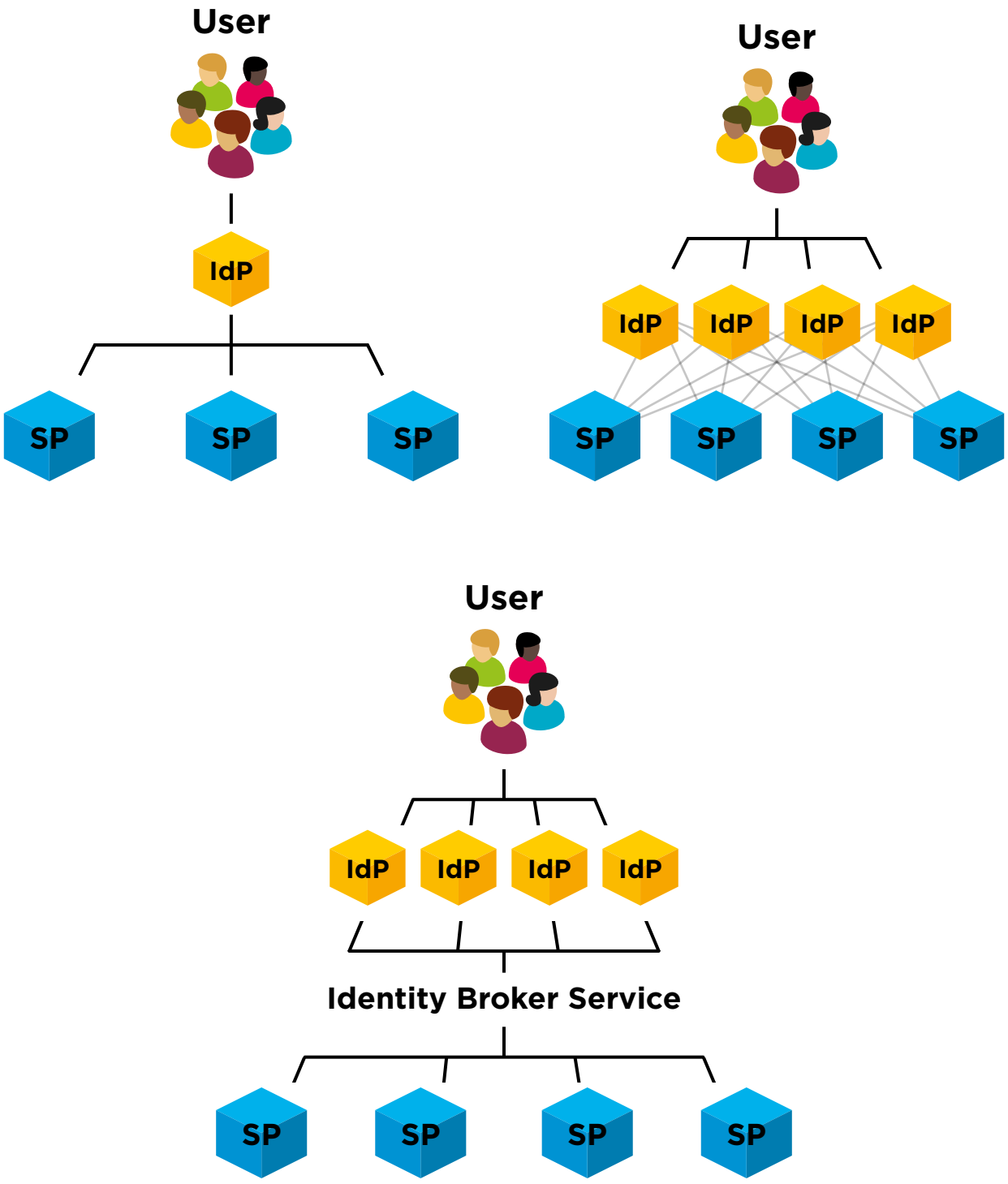
There are three sub-models of third-party identity providers: a single identity provider, multiple identity providers, and identity broker/s with multiple identity providers. When considering the third-party identity model for social services that require the highest level of assurance in identity proofing, authentication, and authorization, the government is always involved, which is exemplified in Table 2.

When there is only one identity provider, the government itself typically acts as that sole identity provider. When there are multiple identity providers, the government is responsible for defining criteria and accrediting the identity providers. In the broker's model, the government is typically responsible for defining requirements and providing accreditation, as well as acting as a broker or designating an entity to act as a broker.

The third-party provider model presents several disadvantages:

- Identity providers are required to maintain large infrastructures and assume high costs to provide secure storage, similar to the centralized model.
- Because the number of identity providers is low compared to the centralized model, there is a concerning monopolization. This impacts both security and reliability.
- Because platforms such as Google and Facebook already serve as identity providers for many digital services (logging into most websites, which do not require high levels of assurance), the revenue model for other identity providers is reduced to only a few social, government, and financial services.
- As there are more organizations involved in the management of our identity, information, and data, individuals have less control of their identity, making it very difficult to guarantee data protection rights such as consent, right to be forgotten, portability, and pseudonymization.

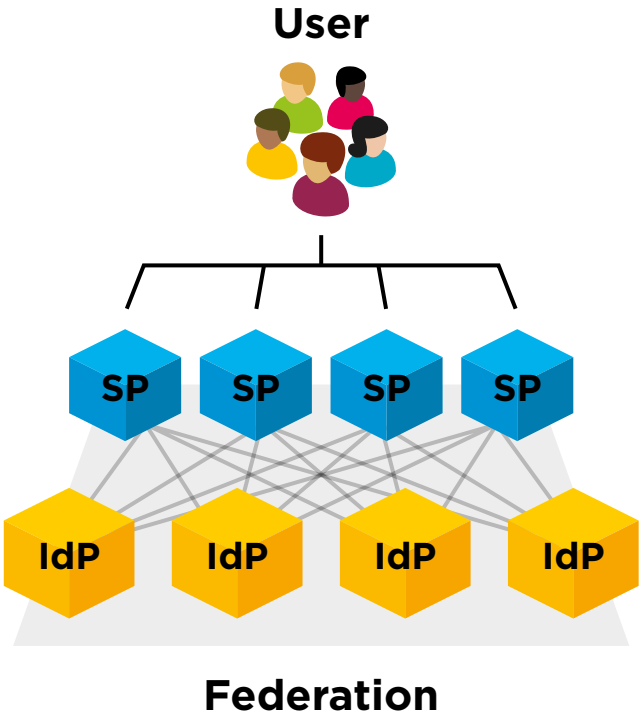
Image 4. Simplified shemas of the three models of third-party identity provider.



2.4.3. Federated

In the federated identity model, several identity providers establish agreements between each other and operate under a common trust-framework. This trust-framework can be public and endorsed by regulation, as is the case with eIDAS in the European Union. Alternatively, the trust-framework can be private, enabled by private agreements between the parties.

Image 5. Simplified schema of the federated model.



In this model, the digital information of the users is distributed across multiple identity providers instead of being centralized within one. This organization of identity providers is generally called a federation, and they typically share a unique identifier for each user. The main difference between the federated approach and the centralized and third-party approaches is that the federated approach is a many-to-many identity management scheme, while the centralized and third-party approaches can be seen as one-to-one and one-to-many, respectively.

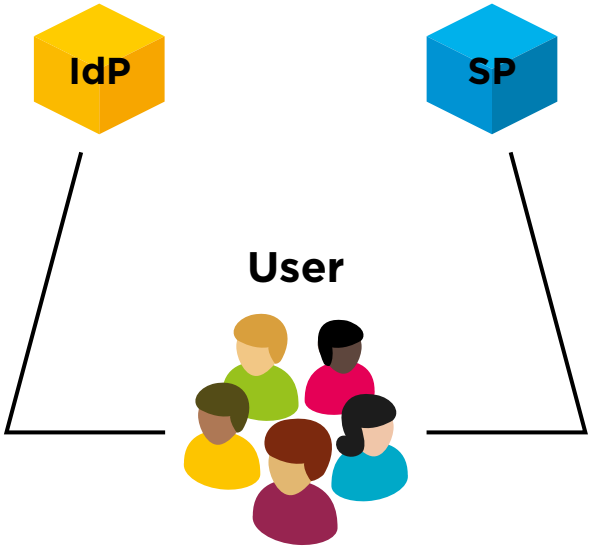
The federated approach has the same benefits and disadvantages as the third-party provider model with multiple identity providers, with or without a broker.

2.4.4. User Centric

In the user centric model, the user stores authenticators and credentials issued by different service providers within a personal device. Thus, the user is in control of their data. A. Josang and S. Pope presented this model in 2005, naming the hardware used to store the data a personal authentication device (PAD) (Josan & Pope, 2005). According to them, the PAD could be any hardware, with or without a keyboard and a screen, that requires authentication, such as a PIN.

As proposed, it is not clear when this model is different from the traditional centralized model and from the self-sovereign model. If the user only stores keys and authenticators or tokens to access a digital service, then this user centric model could be considered a centralized model where the service provider allows one to authenticate with a key stored in their hardware instead of with a username and password. However, if the user truly manages all data in their device and can select which data to be disclosed to which service provider, with the ability to use different digital identities and identifiers to

Image 6. Simplified schema of the user centric model.



authenticate to different service providers, then this is closer to the self-sovereign identity model.

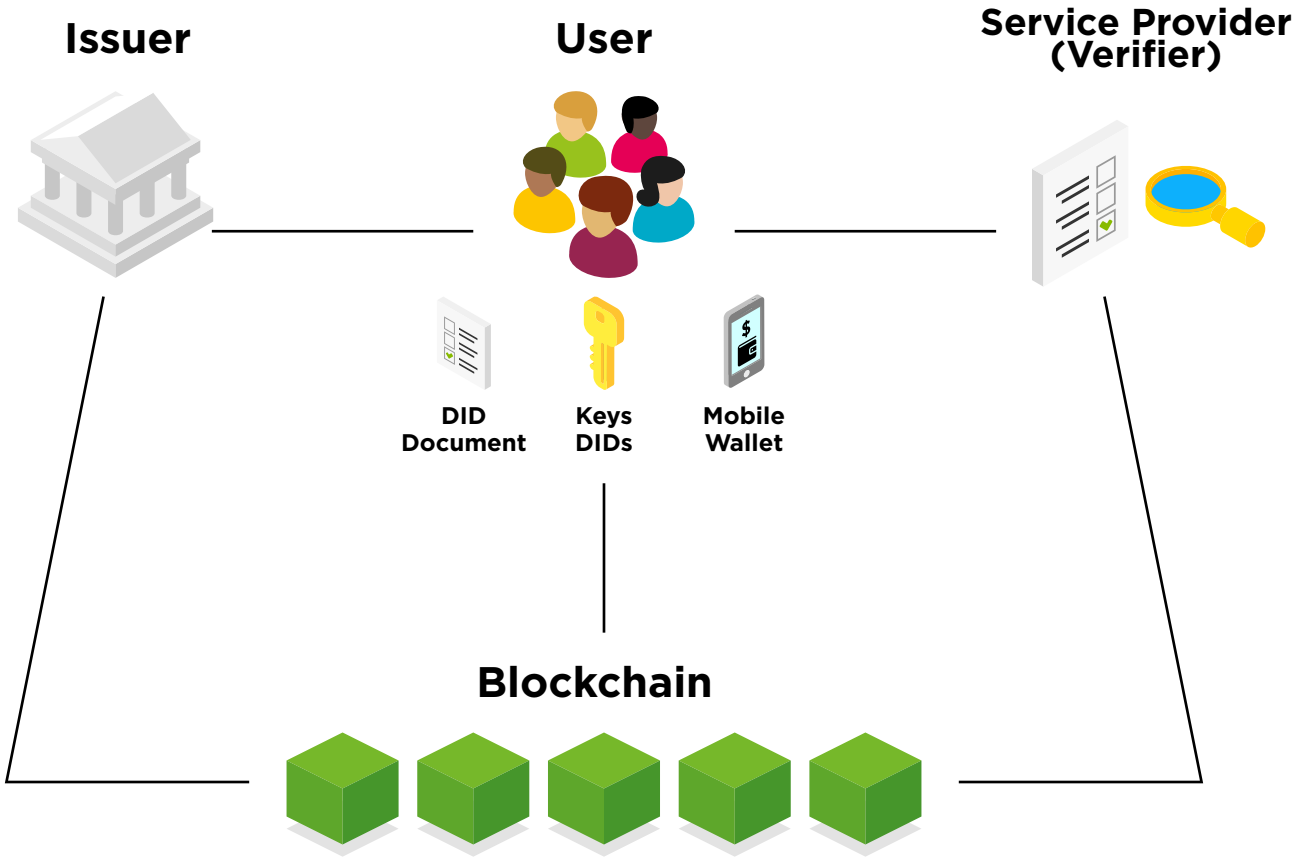
Overall, given the current level of adoption of smart phones, it seems natural to assume they are a suitable option for PADs. In any case, practical implementation of the user centric model in which providers offer digital services to users with maximum levels of assurance, guaranteeing that users are in full control of their authenticators, credentials, and data, a more complete scheme must be developed. This leads us to the self-sovereign identity model.

2.4.5. Self-Sovereign

In the self-sovereign identity (SSI) model, the user is the central administrator of their identity and they have much more control over their data and information than others have, know, or share about them. Unlike centralized, third-party, and federative models, the SSI approach does not require an entity for managing people's identity. Neither an identity provider nor a service provider is needed to manage one's credentials and authenticators on their behalf. The role of the identity provider is now limited to an identity issuer.

Self-sovereign identity is built on two new standards under development by the World Wide Web Consortium, the Decentralized Identifiers (DIDs) (W3C-DID, 2019) and the Verifiable Credentials (VCs) (W3C-VC, 2019). DIDs propose a way for each individual to generate its own unique identifiers to interact in the digital world. VCs are digital credentials, owned by individuals, that contain information or attributes (e.g. name, date of birth, place of residence, etc.) about them. These credentials can be self-issued or third-party-issued.

Image 7. Simplified schema of the self-sovereign identity model.



When the issuers are trusted authorities (e.g. a government or a financial institution), these credentials can be used by the subject to prove those attributes to others (e.g. a digital passport issued by a government). These others are usually called "verifiers" in the SSI model because their role is to receive a credential presented by an individual and verify it. In Section 7.3.5 we introduce the 6 steps of the LACChain ID Verification Process.

SSI leverages two essential elements for identity management: decentralized registers of information and digital wallets.

Decentralized ledgers: The SSI model relies on decentralized registers of information, in which the proofs of ownership of decentralized identifiers and the verifiable credentials are stored within a decentralized ledger. Unlike the centralized, third-party, federated, and user-centric models, which require the verifying entity to somehow reach out to the issuer to verify digital credentials presented to them by the subjects, the SSI model allows the issuer to leave all necessary proofs (cryptographic proofs such as digital signatures and timestamps) in a decentralized public ledger so that anyone can verify them against it. In Section 7.7 we will cover the topic of decentralized ledgers in more detail.

Digital wallets: Digital wallets are portable and secure personal repositories. Ideally in the form of a mobile app, they allow us to manage our identifiers, authenticators, data, and verifiable credentials within our phones, which are completely protected and under our control. We decide what information we disclose to whom in the form of verifiable presentations. In Section 6.5 we will cover the topic of digital wallets further.

2.5. Comparison Between Different Digital Identity Management Systems

In order to compare the digital identity models introduced in Section 2.4, a high-level analysis is presented in Table 3.

In order to evaluate pros and cons of the different schemes of digital identity, it is crucial to examine the financial models of each scheme to assess their sustainability. We have classified costs into five categories:

- User verification and authentication: The identity issuer verifies the identity of the subject.
- Issuance of credentials: The identity issuer generates the credentials and sends them to the holder.
- Management of credential: The holder stores and manages the credentials.
- Back-ups of keys and credentials: The authenticators, private keys, and credentials have back-ups located somewhere to enable recovery.
- Presentation and verification of credentials: The credentials are presented by the holder to the verifier, and the verifier verifies them.

Table 4 identifies who assumes each cost in each of the digital identity models discussed thus far.

Table 3. Comparison between different digital identity models.

	Centralized	Third party IIPs & Federations	User centric	Self-sovereign
Individuals can generate their own identifiers	N	N	N	Y
Individuals are in control of their own authenticators (i.e. private keys)	N	N	Y	Y
Individuals are in control of their own digital credentials and certificates	N	N	Y	Y
Individuals can have control over their identifiers in case of loss or theft of their keys	Y	Y	N	Y
Individuals can retrieve their credentials and certificates in case of loss or theft of their keys	Y	Y	N	Y
Individuals can access the data associated with their digital identity	U	U	U	Y
Enabled zero-knowledge proofs	N	N	N	Y
Personal identifiable information (PII) is minimized	N	N	N	Y
Right to be forgotten can be easily guaranteed	U	N	N	Y
Repositories of authenticators and credentials are portable*	N	N	Y	Y
Identity providers do not keep centralized databases with user's data	N	N	N	Y
Identity providers do not have access to information about people's access to services or interactions with others	N	Y	Y	Y
Implementations comply with regulatory policies	Y	Y	Y	Y
Trust frameworks are developed to allow the definition of identity providers and levels of assurance	Y	Y	Y	Y
Identity is easily retrievable in the case of a natural disaster	Y	Y	N	Y
Data breaches less likely	N	N	N	Y

Y: Yes, N: No, U: Unclear

* We are referring to the current status.

Table 4. Costs and payer in the different identity management systems.

	Centralized	Third party IIPs & Federations	User centric	Self-sovereign
User verification and authentication (prior to the issuance)	The company acting as SP[4]=IdP assumes the costs	For the higher LOAs, users might be asked by the IdP[5] for a fee	Same as third party IdP & federations	Same as third party IdP & federations
Issuance of credentials	Issuance of credentials is part of the verification and authentication process. No additional cost	Same as centralized	Same as centralized	As self-sovereign identity might require DLT, the issuance of credentials might incur in transaction fees to write on those ledgers. Users would assume this fee
Management of credentials	High costs assumed by the SP=IdP in order to protect central databases	Same as centralized, but only by IdPs as they are now different from SPs	Users would decide which PAD to use to manage their credentials. Users would assume the costs	Users would decide which digital wallet they want to manage their credentials.[6] Users would assume the costs
Back-ups for keys and credentials	High costs assumed by the SP=IdP in order to guarantee back-ups and recovery of information	Same as centralized, but only by IdPs as they are now different from SPs	Users would decide which back-up options they want (either provided by the wallet provider, or external). Users would assume the costs	Same as user centric
Presentation and verification of credentials	No cost because credentials are already in control of SP=IdP	The required agreements and connections between IdPs and SP systems might incur in additional costs for them	The provision of technologies to interact with the PAD might incur costs to the SP	Presentation and verification should not incur any costs, as suitable implementations do not generate transactions when verifying credentials against DLTs

4 Service provider.

5 Identity provider.

6 The business model of the digital wallets is not clear yet, as the first solutions are emerging now. Some of the potential revenue models might be in charging fees for (i) the generation of multiple and uncorrelatable DIDs for different electronic interactions, (ii) the provision of cloud storage for back-ups, (iii) the generation of customized verifiable presentations from one or several credentials, and (iv) the generation of qualified electronic signatures.

SELF-SOVEREIGN IDENTITY

Block 3
Self-Sovereign Identity (SSI)

3.1. Definition

According to Sovrin, "self-sovereign identity (SSI) is a term used to describe the digital movement that recognizes an individual should own and control their identity without the intervention of administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world." In 2016, Christopher Allen set 10 principles for self-sovereign identity that have become a reference in the field.[7] These are:

Access: Users must have access to their own data
Consent: Users must agree to the use of their identity
Control: Users must control their identities
Existence: Users must have an independent existence
Interoperability: Identities should be as widely usable as possible
Minimalization: Disclosure of claims must be minimized
Persistence: Identities must be long-lived
Protection: The rights of users must be protected
Portability: Information and services about identity must be transportable
Transparency: Systems and algorithms must be transparent

We consider a digital identity model to be self-sovereign as long as it complies with the 16 following principles:

- Individuals can generate their own unique identifiers[8] (control, existencia)
- Individuals are in control of their authenticators[9] (access, control, existence)
- Individuals are in control of their digital credentials and certificates[10] (access, control, existence)
- Individuals can retrieve the credentials and certificates in case of loss or theft of their authenticators (access, control, existence, persistence, protection,)
- Individuals manage and control the data associated with their digital identity (access, control)
- Individuals can make selective disclosures of data (consent, control, minimalization, protection)
- Individuals' personal identifiable information (PII) is minimized (minimalization, protection)
- Cryptographic proofs of ownership of identifiers can be found in a public decentralized network (persistence, transparency)
- Cryptographic proofs of the ownership and validity of the credentials can be found in a public decentralized network (interoperability, persistence, transparency)
- Right to be forgotten is guaranteed[11] (protection)
- Identity management units[12] (digital wallets) are portable (portability)
- Digital wallet providers do not have access to individuals' information stored in the wallets (access, control, protection)
- Digital wallet providers do not have access to information about individuals' access to services or interactions with others (access, control, protection)
- Back-ups guarantee maximum levels of security and privacy (persistence, protection)
- Implementations comply with regulatory policies (protection)
- Implementations rely on public and/or private trust frameworks that define and specify trust identity providers and levels of assurance (persistence, protection)

7 http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

8 E.g. public keys

9 E.g. private keys

10 E.g. digital passport, digital diploma

11 With self-sovereign identity, enabling tracking of digital information (i.e. where it goes; who has it) and requests to erase it becomes easier because individuals are in control of their identifiers, which are linked to their digital information.

12 Software, hardware, or a combination of both that allows storage and management of personal keys and credentials.

3.2. The Vision of SSI

The general vision of self-sovereign identity is based on personal portable devices that we can use to store and manage all our private keys, authenticators, digital tokens, and credentials safely and in a user-friendly manner. These repositories are called digital wallets, and the first implementations are already available. For example, there are specific mobile apps that can be downloaded to our smartphones from the app store that already have these functionalities. In these apps, we can see all of our digital tokens and digital credentials, and can decide when to use and present them to others. We make these decisions with sovereignty, without having to rely on any third party for any of it.

An example of a digital token is the electronic representation of the digital dollar or euro that today we store in our bank accounts. Additionally, digital tokens include cryptocurrencies, virtual currencies, and others. Examples of digital credentials are digital passports, digital diplomas, digital titles of property, and digital corporate badges, among others.

Today, when we present a credential or a certificate to a verifier (an entity that intends to determine the validity of that credential or certificate) or when we send a digital token to someone else in an electronic transaction, the verifier needs to establish if that certificate or asset is valid. In order to do so, the verifier demands information associated to what is being sent that has been attested by a third party playing the role of an authority that the verifier trusts.

For example, if I present a digital diploma (e.g. a PDF) for a job application, the HR department of the entity posting the job will verify that the certificate is issued by a trusted academic institution. Ideally, if processes are digitalized, the verifier will be able to trigger an automatic electronic process to access a digital service exposed by the issuer and make a query to verify the information presented by the subject. Unfortunately, things very rarely work out this smoothly and efficiently. At present, verifications may take days, months, or years for processes similar to this.

In the SSI model, there is no need for the verifier to directly ask the issuer(s) for information or the trusted authorities for assurance. This is a significant advantage over the centralized, third-party, federated, and even user-centric, models. In the self-sovereign approach, the validity of all our digital assets, including our legitimate ownership of them, can be verified against a decentralized and trusted registry of information. Every time these assets (e.g. digital tokens and credentials) are issued, the issuer registers a cryptographic proof of the issuance as well as a timestamp signed with their electronic signature into a decentralized ledger or network (e.g. a blockchain). The issuer also registers the status of the asset, which either they or any entity authorized by them can change at any time, according to certain public and transparent rules.

These ledgers are also immutable. It is possible to modify or update information, such as the status of the digital credential (e.g. from active to revoked), but all modifications are immutably registered and electronically signed by the entity modifying it, which also needs to be authorized to it, and every change is immutably registered in the decentralized ledger. Therefore, if an issued asset is later revoked, all parties can track changes in the status of the digital credential in the decentralized ledger, which is accessible to everyone. The digital assets can live both in the network or outside of it[13], in our digital wallet. In both cases, the assets are under the owner's complete control because their electronic signature is required to perform any management action with them. Any entity that wishes to verify information on the asset that is presented to them can simply go to the decentralized and transparent network to see the cryptographic proofs left by issuers or trusted authorities. In the following sections, we will be introducing all the necessary concepts needed to understand the

13 No personal data or credentials should be ever stored in the ledger, as ledgers are generally public and immutable. Only cryptographic proofs of information and public tokens should live in the decentralized networks. Therefore, while tokens representing assets can live in the blockchain, credentials containing data or attributes must live off-chain.

Image 8. Example of the presentation of a digital diploma for a job application without (up) and with (down) self-sovereign identity.

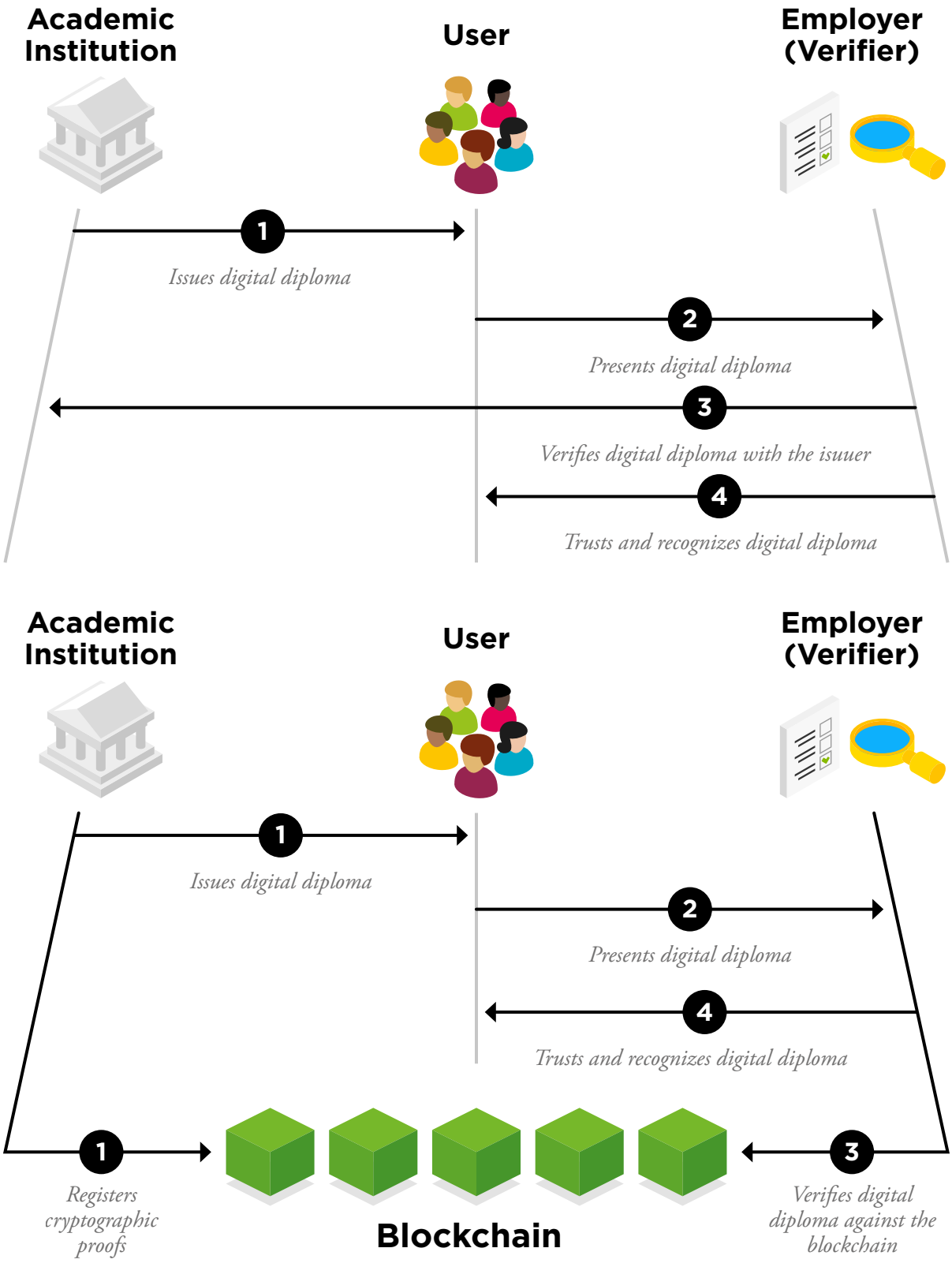
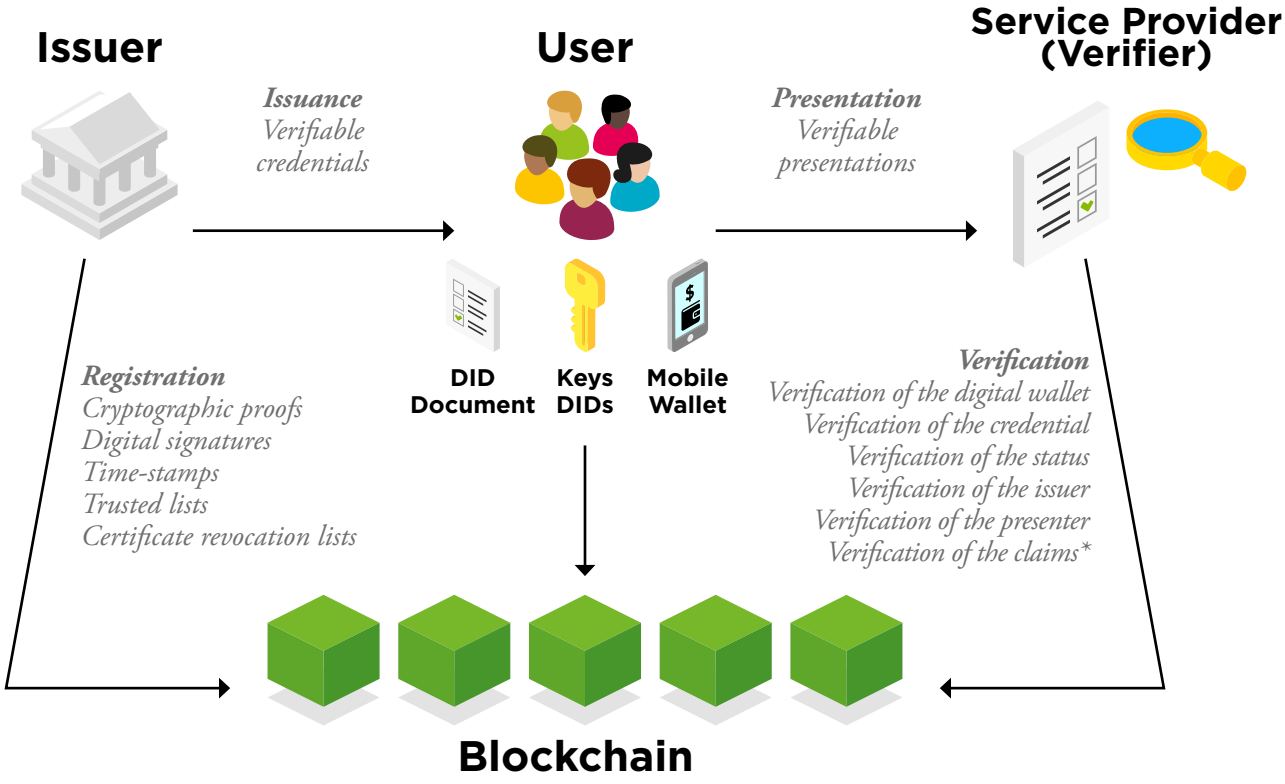


Image 9. Schema of self-sovereign identity.



* For more information, check the LACChain ID Verification Process.

practical implementation of this model. In Section 7.3.5, we present a complete Verification Process.

3.3. Benefits of SSI

There are many substantial differences between managing all assets in a mobile digital wallet under the SSI model and managing them as we do currently. Some of these differences lie within the issues presented in Section 2.3, many of which may disappear with the SSI approach. Let's illustrate these issues and solutions with specific examples:

Interoperability: by using decentralized technology and personal and portable management units, the adoption of global SSI protocols and standards allow private and public entities to store proofs of information within the same accessible decentralized networks. It also enables individuals to manage all their credentials with a single secure and portable device, no matter who issued them or their purpose. Again, in terms of scalability, proper regulation and trust frameworks are essential in complementing the technological tools.

Ownership: currently, we own our cash, but we do not have full ownership of our electronic money (e-money) stored in our bank accounts. When we want to check our balances and transactions, we must access a portal provided by our bank which then exposes the balances and transactions from the bank's database to us. If the bank files for bankruptcy or if the government decides to expropriate the bank, we lose our money. When we make a payment with our credit or debit card, there are several intermediaries, including our card provider, our bank, and the recipient's bank. These intermediaries all communicate with one another, make some validations, and execute the payment by modifying the sender and recipient's balances in their centralized databases. In the SSI model, our balance can be resolved directly from the decentralized ledger (ensuring

the preservation of privacy) and there is no need for any intermediate validation in a transaction, as its rules are automated in the blockchain using computational processes called smart contracts. Financial institutions are still essential in this scheme, as they are the issuers of the digital tokens representing our e-money that we can own and transfer without intermediaries. The difference is that the financial institutions no longer need to play a direct role in the transference of the money. They play an indirect role in this process by being the entity that issued the tokens in the first place.[14] The trust is now held within the decentralized ledger. More than a dozen central banks have already piloted the issuance of central bank digital currencies (CBDCs), and Visa has already submitted a patent for requesting and generating digital currency on blockchain networks[15], suggesting the explosion of this new digital economy is just around the corner.

Pseudonymity: in the SSI model, individuals generate their own identifiers. Individuals are allowed to generate as many identifiers as needed in order to interact with various services in such a way that does not allow these entities to associate the individual with their various other identities. Additionally, SSI protocols allow selective disclosure of information and zero-knowledge proofs. For example, an individual can prove to someone that they are over 21 years old without revealing their real age. Today, in order for an individual to prove they are over a certain age, they must typically show a physical ID document that not only reveals our age, but also discloses additional non-required information, such as our legal name, our nationality, and/or height and weight. We will cover this issue further in Section 7.3.7.

Portability: currently, in order to prove who we are or what we have achieved to another entity, several physical documents are needed, such as passports, national IDs, driver's licenses, property titles, birth certificates, diplomas, among many others. With SSI, all of our documents can be digital, allowing for storage and management within a single digital wallet. This is far more portable than the management units proposed in the other identity models presented in the previous sections. The other models require X.509 certificates, which are typically stored in a computer, or chip cards, which can be easily lost.

Recovery: today, it is quite easy to lose physical documents and chip cards. Almost everyone has lost a physical ID in their lives and thus, consequent difficulties and costs to get new ones are well known. With SSI, on the other hand, if were to lose control over our digital wallet, we could retrieve all of our information from secure and encrypted cloud back-ups. We can also create personal off-line copies using hard drives.

Scalability: by using international standards and protocols and universal technologies, solutions can be replicated across countries. Decentralized ledgers can be joined from anywhere in the world because the internet and digital wallets are available on any smartphone. Obviously, as we will discuss in Blocks 6 and 8, regulations and trust frameworks are necessary to complement the technological components.

Security: digital wallets are able to meet the maximum standards of security. With different layers of identification, authentication, and authorization, SSI protocols ensure that no one but the identity's owner can access it. Additionally, the cryptography and immutability of the decentralized ledgers guarantees that the proofs of information cannot be tampered with. As discussed in Section 2.3.3, billions of data records are hacked each year due to centralized information silos. The SSI approach makes hacking much more difficult because personal data is encrypted and protected within the owner's personal device.

14 This is indeed doing things electronically in a way that is much more similar to how the physical world works. In the physical world, financial institutions mint cash that we can therefore transfer and exchange without any financial institution explicitly validating it. In the digital world, each electronic payments is explicitly validated and executed by financial institutions, making them more expensive and slow. With a decentralized ledger and SSI, individuals will be able transfer money and any other asset instantly, in a peer to peer way, and with no fees.

15 https://cointelegraph.com/news/visa-files-patent-application-for-digital-currency

Table 5. Analysis of the eight weaknesses of traditional digital identity models presented by Gartner (Gartner, 2020) in the self-sovereign identity model.

Traditional digital identity	Self-sovereign identity
Expensive to build and maintain. Each centralized system typically requires its own infrastructure.	As there is a decentralized core infrastructure, some of the costs are shared. Costs of identity management for users might vary depending on the digital wallet they choose to manage their identity.[16]
Inefficient to establish and sustain real trust via identity proofing.	Easier to issue, manage, and present verifiable IDs with digital wallets. This allows for better identity proofing across all kinds of services, not only for those provided by government and financial institutions, as is the case today.
Prone to data proliferation and privacy abuse by way of data aggregation.	As individuals are in control of their data, and differing and unassociated pseudonymous identifiers can be used to interact with various digital services, privacy abuse and data aggregation is much less likely.
Exposed to privacy regulations due to the collection, storage, and analysis of sensitive data.	It is private by design. Identity issuers do not need to keep and expose users' data and service providers can maintain private databases using pseudonymous identifiers. Regulations, however, must continue to improve and adapt, and must always be respected.
The cause of myriad data quality issues due to information silos.	Silos disappear as users are in control of their identifiers, authenticators, data, and credentials.
Vulnerable to security attacks with major data loss exposure (due to centralized repositories).	Centralized repositories are minimized and hacks to decentralized repositories become much more difficult.
Susceptible to identify theft due to a lack of control by the identity owner.	The owner is now in control and can easily revoke credentials and identifiers as soon as they are aware of theft.
Not censorship-resistant because identity providers can suspend accounts at their discretion.	Identity issuers can still revoke credentials but traceability of issuance and revocation is provided by the decentralized ledger or blockchain network. Injustices can be pursued and resolved.

16 Digital wallets are not yet mature products today. The economics of it is still uncertain. Some of the per-pay functionalities might be the generation of uncorrelatable identifiers, the advance electronic signature, or the cloud back-ups. Prices are undefined yet.

Usability: usability comes with portability, recovery, security, interoperability, and pseudonymity. For SSI to have a purpose, public and private services must be available under the SSI framework. The current status, main challenges, and roadmaps for public and private sector with regards to SSI are discussed in Block 5.

The SSI model significantly improves upon the weaknesses of traditional digital identity systems that were pointed out by Gartner and presented in Section 3.3 of this document:

As we will explore in Block 4, not only are there direct benefits of SSI compared to other digital identity management systems, but there are also indirect benefits of SSI on international development, social inclusion, and financial inclusion, making SSI a total game changer across sectors.

3.4. Taxonomy, Basic Concepts, and Clarifications

As a broader and more complex identity management system model, the self-sovereign approach introduces new definitions and contexts that need to be defined. The following taxonomic list of words used in the context of SSI is completely aligned with ISO/IEC 24760-1 (ISO, 2019). Most of the definitions are a merge between the taxonomy provided by the World Wide Web Consortium (W3C) (W3C-VC, 2019) and the National Institute for Standards in Technology (NIST) (NIST-TA, 2020). The purpose of this list is not to replace any list of definitions provided by an organization of standards, but to present consistent and standardized concepts used in this paper.

I. Attribute: characteristic of a *subject*.

II. Authenticator: token, such as a private key or biometric information, used to authenticate a digital service.

III. Claim: characteristic or statement about a *subject* made by an *issuer* as part of a *credential*.

IV. Credential: representation of an *identity* for use in authentication.

Note 1 to entry: a credential is a set of one or more *claims* made by an *issuer* about a *subject*. A *credential* is associated with an *identifier*.

V. Data minimization: act of limiting the amount of shared data strictly to the minimum necessary to successfully accomplish a task or goal.

Note 1 to entry: an example of a task or goal is the provision of a digital service.

VI. Decentralized identifier: portable URL-based *identifier* associated with an *entity*.

Note 1 to entry: also known as a *DID*.

Note 2 to entry: these *identifiers* are most often used in a *verifiable credential* and are associated with *subjects* such that a *verifiable credential* itself can be easily transported from one *repository* to another without the need to reissue the *credential*.

Note 3 to entry: an example of a DID is did:example:123456abcdef.

VII. Decentralized identifier document: document that is accessible using a *verifiable data registry* and contains information related to a specific *decentralized identifier*.

Note 1 to entry: also referred to as a *DID document*.

Note 2 to entry: typical information contained in a *DID document* are the authentication mechanisms and endpoints.

VIII. Derived predicate: *verifiable* boolean assertion about the value of another attribute in a *verifiable credential*.

Note 1 to entry: derivate predicates are useful in zero-knowledge-proof-style verifiable *presentations* because they can limit information disclosure.

Note 2 to entry: if a verifiable credential contains an attribute for expressing a specific height in centimeters, a derived predicate might reference the height attribute in the *verifiable credential* demonstrating that the issuer attests to a height value meeting the minimum height requirement, without actually disclosing the specific height value. For example, the subject is taller than 150 centimeters.

IX. Digital signature: mathematical scheme for demonstrating the authenticity of a digital message.

X. Decentralized ledger: registry of information that is consensually shared and synchronized across multiple sites or computers.

XI. Entity: relevant item for the operation of a domain that has a recognizably distinct existence.
Note 1 to entry: an *entity* can have either a physical or logical embodiment.
Note 2 to entry: an *entity* can be a person, organization, or device that performs one or more roles in the ecosystem.

XII. Graph: network of information composed of *subjects* and their relationship to other *subjects* or data.

XIII. Holder: role an entity might perform by possessing one or more *verifiable credentials* and generating *presentations* from them.
Note 1 to entry: a *holder* is usually, but not always, a *subject* of the *verifiable credentials* they are *holding*. *Holders* store their *credentials* in *credential repositories*.

XIV. Identifier: *attribute* or a set of *attributes* that uniquely characterizes an *identity* in a domain.
Note 1 to entry: an *identifier* can be a specifically created attribute with a value assigned to be unique within the domain.
Note 2 to entry: *identifiers* are typically unique alphanumeric codes that are associated to an *entity*.
Note 3 to entry: an *identifier* can be a blockchain address.

XV. Identity: set of attributes related to an entity.
Note 1 to entry: digital *identities* enable tracking and customization of *entity* interactions across digital contexts, typically using *identifiers* and *attributes*.
Note 2 to entry: unintended distribution or use of *identity* information can compromise privacy.
Note 3 to entry: collection and use of such information should follow the principle of *data minimization*.

XVI. Identity provider: *entity* that makes available *identity* information.
Note 1 to entry: an *identity provider* is an *entity* and/or a system for creating *identity* and maintaining and managing credentials for individuals, while providing authentication services to service providers or *relying party* applications.

XVII. Issuer: *entity* that issues a *credential* about a *subject* on behalf of a *requester*.

XVIII. Presentation: information derived from one or more *credentials*, issued by one or more *issuers*, that a *holder* discloses to a *verifier* to communicate some quality about a *subject*.

XIX. Presenter: *entity* that generates and discloses *presentation*.

XX. Relying Party: *entity* that relies on the *verification* of *identity* information for a particular *entity*.

XXI. Requester: *entity* that makes a request to an *issuer* to issue a *credential* containing *claims* about a *subject*.[17]

XXII. Repository: program, such as a storage vault or *personal verifiable* credential wallet, that stores and protects access to *holders' verifiable credentials*.

XXIII. Selective disclosure: ability of a *presenter* to make fine-grained decisions about what information to share.

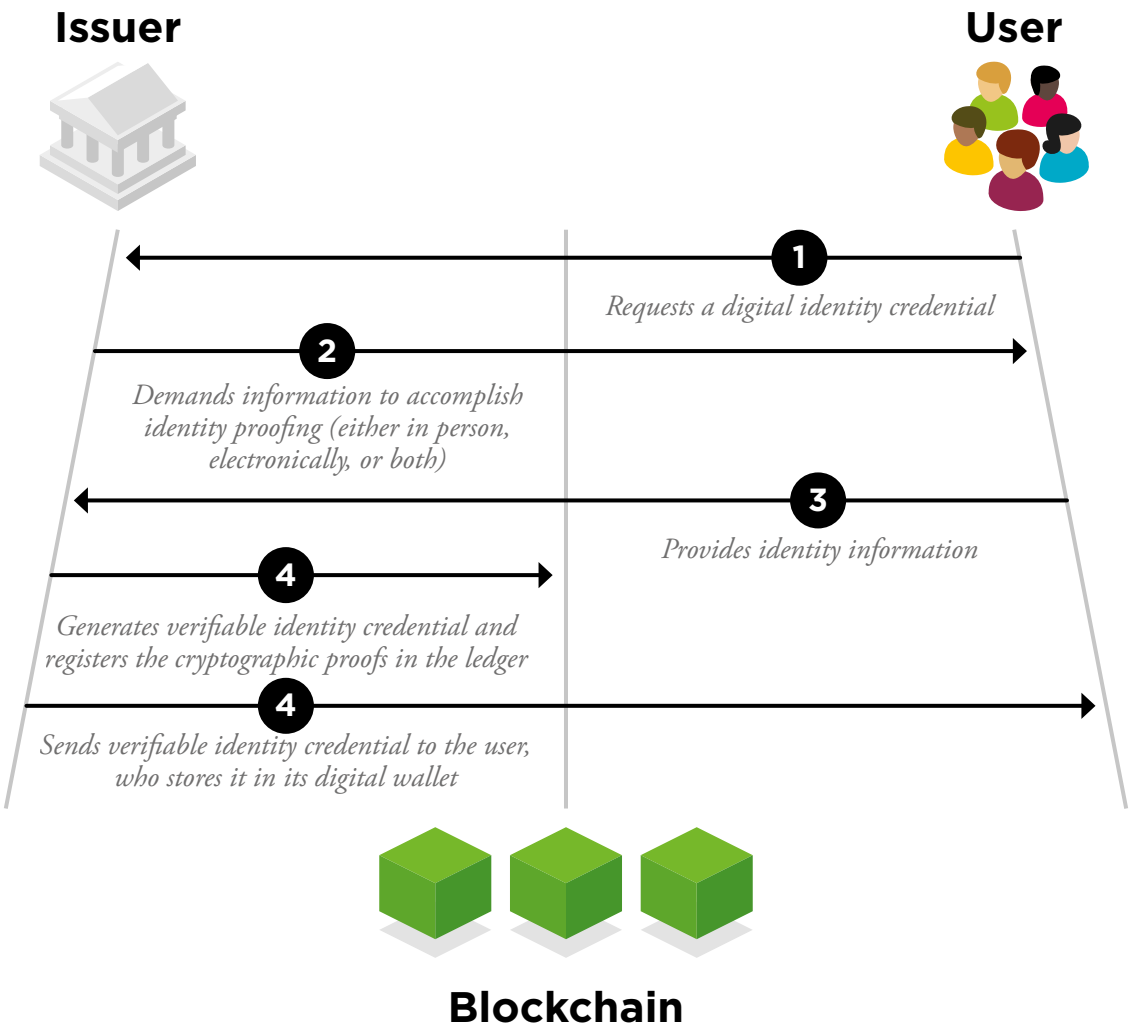
XXIV. Subject: *entity* in which *identity* information is stored and managed by an *identity* management system.
Note 1 to entry: in SSI, identity management systems are typically personal digital wallets.

XXV. System owner: *entity* that owns a given *identity* management system.

XXVI. URI: a Uniform Resource Identifier, as defined by [RFC3986].

17 Requester, subject, and holder can be the same entity, two different entities, or even three different entities. For example, when an entity requests credentials about itself and then manages them, it acts as the requester, holder, and subject at the same time. When an entity, such as a school, asks the government to issue a digital diploma for one of their students and this credential has to be managed by the parent because the student is underage, the requester is the school, the subject is the student, and the holder is the parent.

Image 10. Requesting a digital identity credential.



XXVII. User agent: program, such as a browser or other web client, that mediates the communication between *holders*, *issuers*, and *verifiers*.

XXVIII. UUID: identifier, as defined by [RFC4122].

XXIX. Validation: guarantee or assurance of *verification*.
Note 1 to entry: an example is the assurance that a *verifiable credential* or a *verifiable presentation* meets the needs of a *verifier* and other dependent stakeholders.

XXX. Verifiable credential: a tamper-evident *credential* that has authorship and can be cryptographically *verified*.

XXXI. Verifiable data registry: *role* a system might perform by mediating the creation and verification of *identifiers*, keys, and other relevant data.
Note 1 to entry: example are smart contracts or blockchain networks.
Note 2 to entry: an example of a use case is a certificate revocation registry (CRL).
Note 3 to entry: some configurations might require correlatable *identifiers* for *subjects*.
Note 4 to entry: some registries, such as ones for *UUIDs* and public keys, may just act as namespaces for *identifiers*.

XXXII. Verifiable presentation: tamper-evident *presentation* encoded in such a way that authorship

of the data can be trusted after a process of cryptographic *verification*.

Note 1 to entry: certain types of *verifiable presentations* might contain data that is synthesized from, but does not contain, the original *verifiable credentials* (for example, zero-knowledge proofs).

XXXIII. Verification: process of establishing that the identity information associated with a particular entity is correct.

Note 1 to entry: this ISO definition is more focused on traditional digital identity. SSI is broader as SSI includes not only the identity information layer, but also other attributes that are not explicit identity information (e.g. a university diploma).

Note 2 to entry: This also includes the evaluation of whether a *verifiable credential* or a *verifiable presentation* is an authentic and timely statement of the *issuer* or *presenter*, respectively.

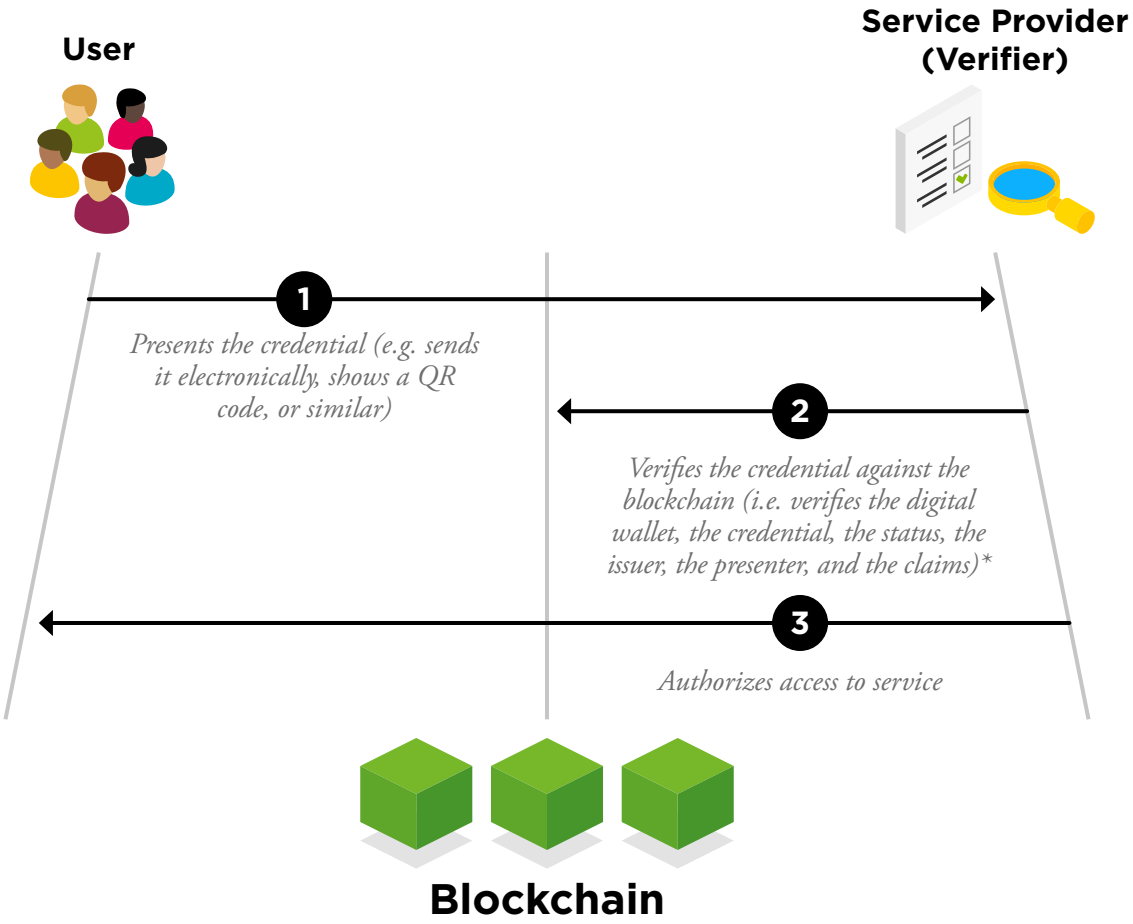
Note 3 to entry: *verification* of a *credential* includes *validating* that the *credential* (or presentation) conforms to the specification, the proof mechanism is satisfied, the *presenter* is authorized, and, if applicable, that the status check succeeds.

XXXIV. Verifier: *entity* that performs *verification*.

Note 1 to entry: an example is an *entity* that verifies the *validity* of a *presentation* (could be on behalf of a *relying* party).

In order not to get lost in this taxonomy, it is important to clarify and emphasize a few concepts:

Image 11. Presenting a digital identity credential (also applies to any other verifiable digital credential).



* For more information, check the LACChain ID Verification Process.

- As mentioned in Section 2.4.5, identity providers do not exist anymore in ideal implementations of the SSI model. In the SSI scheme, the entities that issue digital credentials are no longer the ones that manage them on behalf of the individuals to provide authentication to service providers or relying party applications. Now, the IdPs have become entities that only issue the identity.
- In SSI, users manage their credentials, typically using digital wallets, and the service providers can verify credentials via cryptography when presented to them.
- In the centralized and third-party models, the holders are always the IdP. In the SSI model, the holders are the individuals, subjects of the identity.
- An attribute is called a claim when stated in a credential or a presentation.
- This taxonomy is not only exclusively used to describe schemes of digital identity for people. Subjects can also be animals, plants, objects, or processes.

3.5. SSI and Blockchain Technology

Blockchain and SSI are natural complements, making the perfect symbiosis. SSI solutions need decentralized and immutable registries of information to be able to store proofs of ownership of identifiers and digital credentials. Decentralized and immutable registries of information are also useful for storing lists of decentralized identifiers, certificate authorities (CA), and other public registries necessary for SSI solutions. The other way around, in order to create blockchain networks in which any physical asset can be tokenized and transferred, identity is mandatory.[18] Without identity, most of blockchain-based applications, such as those used in supply chains, trade, notarization, land registries, and digital diplomas, among many others, would never be legally compliant. Some benefits of blockchain networks for SSI solutions are as follows:

Automated delegation: Smart contracts can be used to set dates that enable automatic transference of responsibility, such as when an individual turns a certain age, making them legally responsible for themselves (e.g. 18 years old in the United States).

Blockchain addresses as DID: Blockchain addresses are unique alphanumeric codes that can be naturally used as decentralized identifiers. This will be discussed in detail in Section 7.1.3.

Certificate revocation lists: Instead of requiring each identity issuer to maintain centralized certificate revocation lists (CRLs), they can deploy their own smart contracts in the blockchain to serve as decentralized CRLs, which are still controlled and maintained by themselves. This makes it easier, faster, and cheaper to verify whether a credential was revoked by any verifier. This is discussed further in Section 7.2.6.

DID registries: Smart contracts deployed in a blockchain network can be used naturally as DID registries, in a similar way to the certificate revocation lists. This allows for replacement of centralized registries. This will be discussed in detail in Section 7.1.3.

Digital wallets as repositories: Digital wallets are digital repositories that allow individuals to store and manage keys, and to generate verifiable presentations and share them with others. There are different types of wallets that can naturally connect to blockchain registries. This will be discussed in detail in Section 7.5.

Notarization of credentials: Blockchain ledgers allow any credential to be notarized[19], which means the existence of digital evidence can be sufficiently proved at anytime afterwards.

18 Achieving this is the aim of the LACChain program. In the LACChain Blockchain Architecture, recognized by ITU as one of the fourteen blockchain architectures of reference in the world (ITU, 2019), SSI is a native layer of the infrastructure (layer 2).

19 By notarizing we understand registering the hash of the credential in the blockchain.

Source of cryptographic verification: DIDs and digital credentials are cryptographically verified when they are presented to any entity. Because of their immutability and decentralization, blockchain networks are ideal to store the cryptographic proofs required for this verifications.

Trusted lists: Trust frameworks specify who can issue which credentials to comply with a certain level of assurance. Smart contracts can also be used by authorized entities to maintain trusted lists. At present, trusted lists for digital certificates are usually maintained by certificate authorities (CAs) and public administrations centrally. This will be discussed in detail in Section 8.2.

The huge potential for blockchain technology, or more broadly, decentralized ledgers to leverage the self-sovereign identity model has been widely acknowledged:

"For digital identity applications, there is greater use of permissioned ledgers among trusted parties, as this approach provides increased transaction speeds and improved data privacy. Many proposed blockchain-backed digital identity systems are examples of accumulated IDs, whereby blockchain technology can be used to record transactions between an individual (potentially with no other formal digital identity document) and a peer, service provider, or authority." OIX – OIX (OIX-TOOLS, 2019)

"Thanks to a combination of advances in hardware, including the increasing sophistication smartphones, as well as advances in cryptography and the advent of the blockchain, it is now possible to build new identity frameworks based on the concept of decentralized identities – potentially including an interesting subset of decentralized identity known as self-sovereign identity (SSI)." EU – (EU-BDID, 2019)

"Blockchain technology has the potential to support novel data ownership and governance models with built-in control and consent mechanisms, which may benefit both users and businesses by alleviating these concerns; as a result, blockchain-based IDMSs are beginning to proliferate." – NIST (NIST-TA, 2020)

"Distributed ledgers might represent a future alternative architecture for identity management, and is certainly worthy of evaluation by governments looking to establish a National Digital Identity Framework. This architecture accommodates multiple Identity Providers interacting with multiple Service Providers, as in other architecture models, the difference being in what is called the process of 'identity attestation'. In practice this means that identity credentials are attested by users and third-parties via a decentralized database." – ITU (ITU, 2018)

"It is common to implement identity trust fabric (ITF) using a distributed ledger technology, which is typically built on a blockchain platform (see "Guidance for Assessing Blockchain Platforms"), to enable a decentralized identity network. In fact, ITF is the digital representation of the decentralized governance framework that encompasses the rules of the decentralized identity ecosystem. While some argue that ITF can be implemented using a centralized DBMS technology, Gartner believes that blockchain is a more viable option due to its decentralized property." – Gartner (Garner, 2020)

SELF-SOVEREIGN IDENTITY

Block 4

Potential for Social and Financial Inclusion

The development and implementation of sustainable SSI solutions opens up a new world of opportunities and use cases across sectors. Below, we have provided some examples of these opportunities with a focus on international development and social and financial inclusion.

Access to first identity: according to estimates by the World Bank ID4D Dataset, as of February 2016, some 1 billion individuals around the world lack proof of identity (WB-ID4D, 2018). One of the main causes for having not registered an average of 1 out of 10 children between 0 and 4 years old in Latin America and the Caribbean is the lack of registration points close to rural areas. (IDB, 2013) Having individually managed portable digital identity wallets would allow governments to develop programs in which representatives acting as official birth notarizers could travel to rural and undeveloped areas to issue digital identity certificates that would be managed by the individuals using these digital wallets. This would allow to identify these individuals in this vulnerable and rural populations with an acceptable degree of accuracy and provide them with all kinds of services, such as education or healthcare.

Conditional cash transfers: since the 1990s, most countries in Latin America and the Caribbean have developed conditional cash transfer programs. By 2015, these programs have benefited 88.2% and 76.9% of the national population in Uruguay and Bolivia, respectively (IDB, 2016). Today, these programs face many challenges, including the identification and verification of the target population, the delivery of conditional transfers, and the traceability of money to verify it was used for its conditioned purpose, among others (IDB, 2017). SSI enables individuals that own digital wallets to store both their identity credentials and electronic money themselves. This allows for real-time and zero-cost verification of the target population (provided that an initial identity onboarding has been carried out), real-time and zero-cost delivery of cash transfers, and full traceability of the usage of transfers. This is all thanks to the immutable blockchain, which can also be leveraged to create smart contracts with rules that only allow money spending for conditioned purposes.

Data breaches: more than 2.8 billion consumer data records were exposed in 342 breaches at an estimated total cost of more than $654 billion (ForgeRock, 2019) in 2018 alone. Large data breaches occur because information is centralized through identity providers and service providers, who do not protect the information well enough. With the SSI approach, identity providers no longer manage user's credentials and solely become identity issuers. This helps eliminate information hacking. Service providers, on the other hand, must still manage some customer information. However, as subjects are identified by pseudonymous identifiers in self-sovereign schemes, service providers can maintain pseudonymous information, thus minimizing the amount of PII. In ideal implementations of SSI, with each individual acting as the sole manager of their own credentials and personal data, only individual hacks are possible. This exponentially increases the time and effort required for hacking.

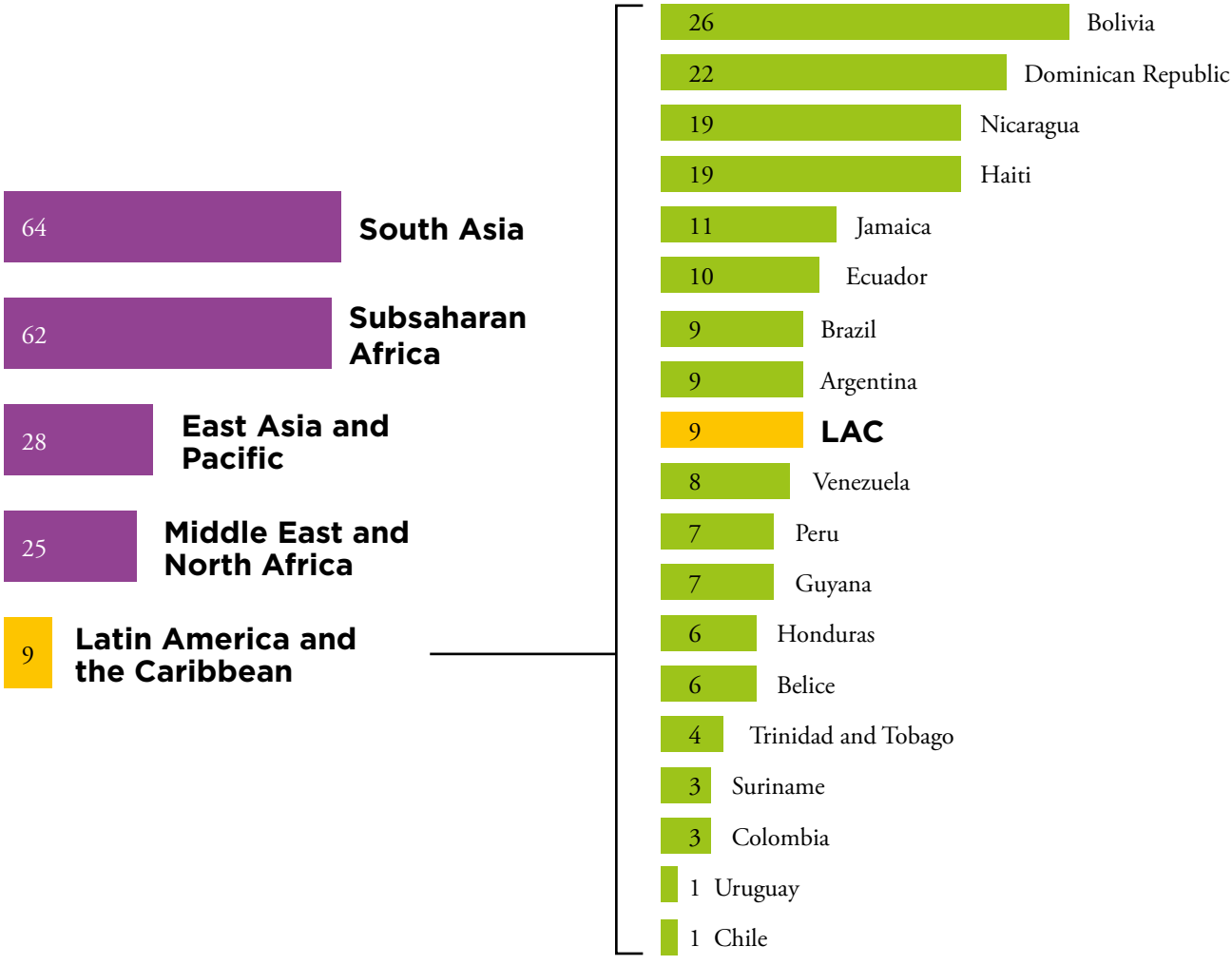
Data privacy: the SSI approach bolsters data privacy in several ways. SSI mitigates the risk of privacy abuse by data aggregation and eliminates information silos. It also makes major attacks more difficult because centralized repositories are no longer needed. Ideal SSI implementations also guarantee the right to be forgotten, the right of consent, the right of pseudonymization, data portability, and the minimization of PII. The topic of data privacy is covered in Section 6.2.

Digital diplomas: the issuance, management, translation, foreign validation, and verification of diplomas is a substantial issue internationally. Some countries take several years to issue an official university diploma. Often, when attempting to present a university diploma abroad for employment or secondary education, an original version or a certified copy must be presented physically. When diplomas are lost or stolen, re-issuance may even be impossible. All of these issues cost significant amounts of both time and money for individuals. These issues have to do with the existing processes and

available technology in addition to normalization and standardization of the issuance and verification of diplomas. SSI promotes the issuance of digital verifiable credentials that are portable, do not need translation, follow international standards, and can be cryptographically verified in real time. Issuance times are also reduced, as there is no need to print physical copies and pass them along to be signed by different institutions manually. The digital credentials can be digitally issued and signed in real time. Even more, students' academic histories can be digitized, with the cryptographic proofs stored in the blockchain, and smart contracts could be developed to generate automatic diplomas signed by the issuers after graduation.[20]

Education: according to IDB's research, children without registration across Latin America and the Caribbean are up to 17.7% less likely to be enrolled in school compared to their documented peers.

Image 12. Percentage of under-registered children between 0 and 4 years from 2000 to 2012. (IDB, 2013)



20 An illustrative example of a project that leverages self-sovereign identity to issue digital diplomas is one led by the Caribbean Examinations Council (CXC) and the Inter-American Development Bank (IDB). This project issued digital diplomas to 24,000 students in a first pilot phase and is now in the process of developing a second phase which uses the LACChain Blockchain Network to issue digital diplomas in Barbados, Jamaica, and Trinidad & Tobago.

This contributes to a 25.3% lower probability of having access to primary education and up to 19.5% of having access to secondary school (IDB, 2013). Easier access to identities and management of identification and authentication processes provided by SSI can help reduce these numbers.

Financial inclusion: according to the IDB's research, approximately 185 million people in Latin America and the Caribbean did not have access to formal financial services in 2015. In countries such as Bolivia, Colombia, El Salvador, Honduras, Mexico, Nicaragua, Panama, and Peru, access to financial services for those living in rural areas is below 40%. One of the reasons why is because the development of sustainable and scalable digital platforms has been weak. Despite the existence of 37 mobile money services in 19 countries throughout Latin America and the Caribbean, in 2015 there were only 15 million existing accounts, with 60% of these accounts inactive. (IDB, 2015) SSI solutions enable easier, faster, and cheaper digitalization and bankarization by providing more reliable information for KYC and AML processes. Additionally, SSI contributes to financial inclusion indirectly too, as it enables the provision of many digital services, such as the ones described in this section, which encourages and motivates individuals to embrace digitalization and use electronic services which allows them to generate a credit history. In the United States, for those who do not have bank accounts, 30.2% do not because they do not trust banks, 28.2% have privacy concerns, and 13.1% claim they have no interest in the services provided by banks. (FDIC, 2017) These same concerns, among others, are most likely also applicable to Latin American and the Caribbean citizens and could be mitigated with both direct and indirect SSI solutions.

Government services: some countries already utilize advanced national digital ID schemes to allow citizens to access some government services. Estonia is the most widely known example and is generally presented as a model for other countries. According to data provided by the Estonian government, 98% of Estonians have a national ID-card and use it to travel, access bank accounts, generate digital signatures, check medical records, or vote electronically.[21] The Estonian case example illustrates that there are many advantages to having a national government-issued ID but that even the best implementations of national government-issued IDs are limited due to the previously discussed problems with centralized digital identity models. As we will discuss in detail in Section 5.3, the SSI model will allow governments with existing national ID solutions to upgrade to a more secure and scalable approach, and also provides a leapfrogging opportunity to those without it.

Healthcare: the healthcare industry can benefit greatly from the use of SSI. As presented in Section 2.3.3, the healthcare sector was most vulnerable to data breaches, with this industry falling victim to 48% of all breaches in 2018. Date of birth and/or Social Security Numbers were the most frequently compromised personal identifiable information (PII) in 2018, with 54% of total breaches exposing this type of data. Giving individuals control of their medical records would significantly help address problem. Medical centers could minimize the PII they retain from their users, going from identifying individuals with their pseudonymous identifiers to eventually fully erasing medical records from their databases. If this were the case, doctors would have access to a patient's medical records only when patients allow them to authenticate with their self-managed authenticators. Another impact on healthcare enabled by SSI implementations would be an increase in the number of individuals that would get access to care. By being identified more easily, they can qualify for the provision of necessary medical services, such as vaccines. At present, in Latin America and the Caribbean, children without a birth certificate are administered 13.9% fewer vaccines against dangerous or life-threatening diseases compared to their documented counterparts on average (IDB, 2013).

Migrants and refugees: SSI solutions has potential to facilitate multilateral and nongovernmental (NGO) organizations help refugees and forced migrants. According to the United Nations, at present

21 https://e-estonia.com/solutions/e-identity/id-card/

there are 30 million refugees around the world.[22] Not only is it often difficult for them to prove their identities, but it is also often difficult to prove their professional skills or experiences. The existence of SSI solutions and decentralized and immutable blockchain networks provides new ways for NGOs and multilaterals to issue verifiable digital identity credentials and professional digital certificates[23].

Natural disasters: natural disasters are also a threat to entities' and individuals' essential information. Digitalization of documents (for identity, healthcare, or diplomas, among others) is the easiest solution for reducing the impact of natural disasters on loss of information. However, some approaches for digitalization are better than others. Centralized registries of digital information, such as data centers, can also be damaged in natural disasters. Decentralized registries and SSI solutions allow users to be in control of their digital identifiers and documents by giving them stronger ability to retrieve them in case of loss or theft is the best approach to mitigate these impacts. In 2015, the US Federal Emergency Management Agency (FEMA) began an initiative to transform the way the agency administers grants and disaster relief funds. They claimed that "in addition to validation of assets, FEMA can use blockchain identity management to issue e-identities to individuals seeking aid and assistance. A blockchain e-identity can help ensure that FEMA has a unique record of every person and issue relief payments in a manner that is secure and transparent." (FEMA, 2019)

Public safety and gender equality: Having SSI and immutable blockchain networks can help increase public safety, through real time notification of law infringements and personal violence or abuse. In the case of domestic violence against women, which is a particular public health concern, action protocols could be implemented into smart contracts, such that the actions are triggered as soon as the contract is notified that abuse has occurred.[24]

Remittances: In 2014, a research paper showed that more than $60 billion in remittances enter Latin America and the Caribbean every year (FOMIN-I, 2014). In countries such as Haiti, Honduras, El Salvador, Jamaica, Guatemala, and Nicaragua, income due to remittances represented between 10% to 34% of GDP in 2017. (IDB-REM, 2017) An important component of cost of remittances are in the final stages, as most of the recipients do not have bank accounts. Additionally, research from FOMIN revealed that senders send money at greater amounts more frequently when the recipients have bank accounts. (FOMIN-II, 2014) As explored in the previous paragraphs on easier access to identity and financial inclusion, SSI has the potential to indirectly facilitate and lower the price of remittances. By leveraging blockchain technology, it can allow for digital money transfers from one digital identity to another in real time, reducing times and costs, as one on side bankarization of individuals from vulnerable and poor populations is encouraged, and on the other side the number of intermediaries needed for cross border payments is reduced.

22 https://www.un.org/es/sections/issues-depth/refugees/index.html

23 UNICEF has been exploring applications of blockchain technology since 2015

24 LACChain have launched the challenge "Blockchangels", a call for solutions to confront violence, harassment, and abuse to women, children and elderly. https://blockchangel.webintra.net/

SELF-SOVEREIGN IDENTITY

Block 5
The Road to Adoption

5.1. The Current Status of SSI

At present, self-sovereign identity is still at an early stage. However, there is already broad recognition of its enormous potential, as is clear from the many quotations provided in the previous sections by the International Telecommunications Union (ITU), the National Institute of Standards and Technology (NIST), the European Union (EU), or the Open Identity Exchange (OIX). In order for SSI solutions to proliferate, it is necessary to keep making progress across the three layers of the techno-legal framework that will be presented in the second block of this paper: regulation, technology, and trust frameworks. The aim of this section is to present a general overview of the status of the development of these three layers.

Any electronic service of trust needs to be compliant with regulation. In the case of SSI, the two big areas of regulation involved are the regulations of electronic signatures and transactions, and the regulations in data protection. Electronic signatures and transactions are already regulated in many countries, including most of the countries in Latin America and the Caribbean. However, several countries do not currently have data protection regulations in place. Clear and modern regulations on data protection are essential to ensure that digital solutions and services respect individuals' data, rights, and privacy. The most acknowledged regulatory policies on electronic signatures and data protection come from the European Union: Electronic Identification, Authentication and Trust Services (eIDAS) and General Data Protection Regulation (GDPR). In Sections 6.1.1 and 6.2.1 we present the state of regulation on electronic signatures and data protection in Latin America and the Caribbean. In Sections 6.1.2 and 6.2.2 we explore how eIDAS and GDPR apply to SSI.

Regarding technology, different working groups and standardization agencies have been working over the past few years to develop new standards and protocols that are the base of the SSI model. Some of these efforts come from Alastria, the Decentralized Identity Foundation (DIF), the European Blockchain Services Infrastructure (EBSI), the Internet Engineering Task Force (IETF), LACChain, NIST, Sovrin, OASIS, the OpenID Foundation (ODIF), and the World Wide Web Consortium (W3C). There are two fundamental standards for SSI: the decentralized identifiers (DIDs) and the verifiable credentials (VCs). Both DID and VC standards are in the very beginning stages and propose a data model for unique identifiers in self-sovereign solutions and a data model for the issuance, storage, presentation, and verification of digital credentials, respectively. There are also a few existing solutions on the market which leverage new standards and protocols for SSI, including Evernym, Hyperledger Indy, KayTrust (by Everis), Rem (by World Data), Sovrin, and uPort. In the Block 7 of this paper, we will cover in detail the different layers of technological components that we consider necessary for the success of self-sovereign identity solutions.

Trust frameworks consist of legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose. In the case of SSI, the purpose is to enable trusted electronic interactions using self-sovereign identity for the identification, authentication and authorization of individuals. Trust frameworks can be public or private, and can have a local, national, or regional scope. Unfortunately, there are not many trust frameworks tailored for SSI yet. However, a very good reference of a regional framework for electronic identification that is unique in the world is eIDAS. The eIDAS regulation establishes the rules for members of the European Union to define governing bodies and maintain trusted lists. It also establishes standard and secure ways of communicating information between Member States using certificate authorities, identity issuers, and certificate revocation lists. Finally, it requires non-discrimination of credentials by public entities of the Member States when those credentials meet assurance requirements. In other parts of the world, there is currently a lack of both national and regional trust frameworks. In Section 8.3, we present the OIX, eIDAS, and Sovrin approaches.

5.2. Challenges

There are several challenges facing the widespread adaptation of self-sovereign identity, some of which have been pointed out in the previous section. They are the following:

Adaptation of current information and digital systems: Current IT must transition in order to enable the issuance and verification of SSI credentials for accessing digital services.

Back-ups: Flexible integrations between digital wallets and back-up services are necessary to guarantee the recovery of credentials and information under user control.

Comprehension of the technology by jurists, notaries, and regulators: A clear understanding of technology by jurists, notaries, and regulators is necessary in order for regulation to keep up with technology.

Data protection: Stronger and more modern data protection regulations are needed to protect people's data, rights, and privacy.

Digital wallets: Digital wallets are an essential interface between end-users and the decentralized SSI infrastructure, playing a main role in identification, authentication, and authorization. The first digital wallets are already available but they are not very robust yet. There is a need and an opportunity for a bigger and more competitive ecosystem of digital wallets.

Individual's adoption: Proposing user-friendly solutions to individuals, either from the private sector or from governments, is necessary for broad adoption. Additionally, it is very important to develop a marketplace of SSI-friendly applications.

Involvement of governments and policy makers: Governments would need to transition to the SSI scheme for the provision of SSI-compatible national ID documents and the establishment of techno-legal frameworks.

Key recovery: Currently, key recovery is not independent, fast, or robust enough. More work in this area is necessary.

Privacy: SSI can solve many existing privacy issues but can also create new ones. As SSI relies on an immutable and decentralized registry of information for storing the cryptographic proofs of the information, privacy can be violated if not only the proofs but also the data and information itself is stored in this public registry. Decentralized ledgers and blockchain networks must not be used as traditional databases to store documents and sensitive data. Only their proofs and in a non-correlatable way.

Pseudonymity: The use of public, decentralized, and immutable registries of information demands essential efforts to guarantee the pseudonymity of information and identifiers. PII must not be registered in public registries.

Recognition of standards: Standards, such as DIDs and VCs, must continue to evolve in order to be accepted and recommended by Standards Developing Organizations (SDO) such as the IEEE, ISO, ITU, or NIST.

Regulatory policies: Regulation of electronic signatures and transactions and recognition of verifiable credentials such as electronic documents are needed.

Right to be forgotten: The right to be forgotten must be guaranteed. As defined in Article 17 of GDPR[25], "the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her" under certain conditions. The self-sovereign identity approach can facilitate this. Because individuals are in control of their identifiers, which are linked to their digital information, it can be easier to enable tracking of digital information, and request certain parties

25 https://gdpr-info.eu/art-17-gdpr/

to destroy it. However, the fact that immutable blockchain networks are used to store cryptography proofs also presents a challenge, and it is necessary to ensure that the registration of personal data or PII in the ledger is avoided.

Robust decentralized registries: Mature and robust decentralized registries are necessary for scalable SSI solutions. This includes requires high transactionability to allow the generation of identifiers and proofs of credentials, and solid regulatory frameworks. The current fragmented ecosystem of non-interoperable, non-regulated, and with limited transactionability decentralized ledgers and blockchain networks is far from ideal. Regional efforts to develop public-permissioned regional networks, such as EBSI in Europe and LACChain in Latin America and the Caribbean, have been acknowledged as promising.

Trust frameworks: It is necessary to develop national and regional public and private frameworks in order to establish levels of assurance for electronic services, and the certification of qualified identity providers, such as eIDAS in the European Union.

Use of biometrics: The use of biometrics in self-sovereign identity for identity proofing and authentication has tremendous potential and needs to be explored more in depth.

Zero knowledge proofs: Zero knowledge proof solutions are still at an early stage and need more time to keep evolving.

These challenges are not insurmountable, nor should they be discouraging. They are worth contributing significant time and effort to overcome as self-sovereign identity is a disruptive tool that will bring greater convenience, more reduction of costs, stronger inclusion, higher security, better user experience, greater service delivery, more commercial opportunities, higher reachability, and greater verification, among many others benefits. It will also enable multiple solutions that target social and financial inclusion, as discussed in Section 4.

5.3. Steps for Adoption

Currently, there exists some interesting material providing guidelines for government agencies to develop digital identity frameworks. Some references are ITU (ITU, 2018), FATF (FATF, 2020), the European Union (EU, 2018), and OIX (OIX, 2019). Although these guidelines are not specific to self-sovereign identity, they are perfectly applicable.

According to OIX, identity frameworks and solutions can be classified into three groups or levels depending on the source of rules governing liability (OIX, 2014). At level one, the digital identity scheme is based on general public law that applies to every digital identity solution and every natural and legal person. Level two also relies on public law but, the law only applies to specific jurisdictions. Level three consists of contract-based rules that several entities agree to be bound by. In the next sections we analyze how the self-sovereign identity approach applies to solutions based on public frameworks versus solutions based on private agreements.

5.3.1. Opportunities for Governments

Some governments have already enabled digital identity for individuals at the national level. Estonia, for example, has a national ID card system that provides access to all Estonian e-services and is used by 98% of the population.[26] In Latin America and the Caribbean, Peru has the most advanced national electronic ID card (DNIe in Spanish), which is issued by the National Registry of Identification and Civil Status (RENIEC in Spanish). However, most countries, including most of the ones in Latin American and the Caribbean, lack national digital identity schemes. Identity proofing, authentication, and authorization are conditioned to the level of assurance (LOA) required by each use case, and enabling strong digital identities equivalent to the LOA of a passport requires very significant efforts.

26 https://e-estonia.com/solutions/e-identity/id-card/

Additionally, even in countries that currently utilize digital IDs, they are only used to provide individuals access to some government services, so they cannot be used to access private services. Thus, there are not currently national ecosystems whereby a citizen can access a broad variety of public and private digital services with their government-based digital identity.

One of the reasons why current government-based digital identity solutions have a limited scope is the digital identity management systems behind them. As we have previously discussed in this paper, these systems have either governments themselves or a few designated entities acting as identity providers, which represents the centralized model presented in Section 2.4.1. This means all authenticators and user data is centralized either directly or indirectly in the government's infrastructure. This model works well when individuals want to access services provided by the government. However, individuals cannot use their government-based digital IDs to access services that are not provided by the government. It seems very unlikely that the government or the entities designated by the government as identify providers could be willing to offer services to authenticate citizens not only against government services but also against any kind of national and international third-party digital service. This would entail very high-cost infrastructure and a big responsibility.

However, we believe that the adoption of the self-sovereign identity approach has the potential to allow governments to issue digital IDs to individuals that can be used to access any kind of digital services (i.e. public and private) without large investments in infrastructure nor additional responsibilities associated. In the self-sovereign identity approach, governments issue identity credentials which proofs are recorded in a blockchain ledger as well as in trusted lists. This changes completely the situation, as the government does not need to provide and maintain any kind of service for the verification of credentials or the authentication of individuals. In the SSI scheme, the government only needs to issue digital credentials that the individual will manage, and register its cryptographic proofs in a public and decentralized

Table 6. Types of digital identity schemes based on the source of rules governing liability, according to OIX.

Source of rules governing liability	General Law	ID-Specific Law	Contract-based rules
Level	1	2	3
Type of rule	Public Law	Public Law	Private Law
Applicability	Everyone in jurisdiction	ID system participants in the jurisdiction covered by the statute	Entities that agree to be bound by contract

network which the government does not need to maintain (even though it could if wished), which eliminates the need for additional infrastructure costs. Additionally, as the individual is in possession of the digital credentials, the individual is now fully responsible for sharing their information and data with others. Also, as service providers do not verify credentials directly with the government but against the decentralized network, it could be understood that the government is not offering an authentication service and therefore is not responsible nor liable for the identification, authentication, and authorization to digital services that third parties grant to citizens that present government IDs for these purposes.

For governments that already have national digital identity schemes, the transition to self-sovereign identity will be easy. However, it may require modifications to regulations, which we will address in Block 6, and incorporation of technological elements, which we will introduce in Block 7. For governments without an existing digital identity scheme, there is a leapfrogging opportunity to be at the forefront of the electronic identification and authentication of the future. ITU highlights four areas to focus on: the governance model, the approaches for fostering adoption, the architectural model, and the sustainability model. (ITU, 2018) In Section 8.1, we will present a disaggregated review of the different layers that require governance models in a self-sovereign identity solution.

5.3.2. Opportunities for the Private Sector

The exchange of identity information of individuals and companies happens frequently between private entities. Generally, these exchanges of sensitive information between pairs or groups of entities are ruled by private agreements. Very often, the exchanges are insecure and inefficient.

SSI standards and protocols are opening a door for a safer, more standardized, and efficient exchange of information, that can lead to the development of private platforms and digital services much more interoperable, secure, and reliable, compliant with national and international regulations.

As discussed in Sections 2.3 and 2.4, centralized and third-party provider digital identity models consist of silos of information, centralized databases, different types of identifiers for the same users, a lack of standards and protocols, lack of suitable data protection regulations and rules, and many other disadvantages that make it very difficult for different parties to develop common private frameworks for digital identity solutions. Therefore, if a group of entities from the same sector want to develop common platforms that require individual identification, such as single windows or settlement networks, several challenges have to be addressed. However, self-sovereign identity provides a new process of digital identification. It proposes several advantages, including the use of 1) common, public, and decentralized registries of information; 2) decentralized identifiers following the same rules for all users; and 3) common standards and protocols for the issuance, storage, presentation, and verification of digital credentials, among many others.

Having a single trusted registry, such as a regional blockchain network, and following common protocols and standards, such as the decentralized identifiers and verifiable credentials, would be a big first step in the development of private frameworks and agreements that are scalable, secure, and robust, and at lower costs and effort than before. One successful example of this approach is an initiative carried out by the international customs administrations of Chile, Colombia, Costa Rica, Mexico, and Peru: Proyecto Cadena. This project, financed by the Inter-American Development Bank, consists of the development and implementation of a joint solution using LACChain regional blockchain network to exchange sensitive information between these five countries' custom administrations. Each country updated their bilateral mutual recognition agreements (MRA) agreeing to recognize each other's self-issued identities within the blockchain network and the electronically signed information in the form of blockchain transactions.

With privacy rules defined at the blockchain level, which limits customs agencies' access to sensitive information that are part of the MRA, the five customs from five different countries in Latin America and the Caribbean were able to create a common solution based on a private implementation of the self-sovereign identity scheme even though they do not share common regulations for electronic signatures or data protection. This agreement allowed them to exchange secure and reliable information in real time without having to maintain a centralized platform, interconnect centralized databases, or integrate silos of information. Building a common platform with shared data, accesses, authentication schemes, integrations, maintenance, and many other requirements allowed for an alternative and efficient way of exchanging information that would have been impossible with traditional technology.

Self-sovereign identity opens the door to a new identity ecosystem independent of governments' direct supervision and approval. NGOs, financial institutions, multilaterals, private insurance companies, and other large institutions could become identity issuers and provide digital credentials to individuals that they have the capacity to identify, in some cases because they are already doing it as they are providing services to them. There is also potential for lucrative business models around it. These credentials would be under the control of the individuals which they could present electronically to anybody that can verify them against a public registry. Other entities could then trust those credentials with a high level of assurance as they have been issued by large institutions that they trust.

5.3.3. Comparison Between Higher and Lower Involvement of the Government

There are several steps required to develop a full, scalable, and operative self-sovereign identity ecosystem that is focused on end-users. These steps may differ depending on how much government is involved. In Table 7, we present a hypothetical overview of two approaches: one with a fully hands-on and one with a fully hands-off government. These examples are not intended to act as guidelines and they assume that the appropriate regulations and technology are readily available.

The first step for any SSI solution is choosing a decentralized network to serve as the trusted registry. Currently, there are two regional blockchain ledgers: one in Europe and one in Latin America and the Caribbean. These ledgers are positioning themselves to serve as the regional reference in their respective areas.

The European Blockchain Services Infrastructure (EBSI) is a "joint initiative from the European Commission and the European Blockchain Partnership (EBP) to deliver EU-wide cross-border public services using blockchain technology. The EBSI will be materialized as a network of distributed nodes across Europe (the blockchain), leveraging an increasing number of applications focused on specific use cases. In 2020, EBSI will become a CEF[27] Building Block, providing reusable software, specifications and services to support adoption by EU institutions and European public administrations."[28] The European governments will be testing this blockchain infrastructure with four use cases in 2020: notarization, diplomas, self-sovereign identity, and data exchange. This is the only government-based regional effort to develop a self-sovereign identity solution in the world. The EU is utilizing regional regulatory policies, such as eIDAS and GDPR, to build this regional blockchain infrastructure that can support the SSI model.

The SSI eIDAS bridge, a pilot focusing on providing cross-border identity solutions compliant with the eIDAS trust framework, outlines scenarios for short-, mid-, and long-term implementation, which are reviewed in more detail in Section 6.1.2. Briefly, it suggests recommendations in which changes to

27 CEF stands for "common European framework".

28 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

Table 7. Two hypothetical frameworks depending on the involvement of the government.

	Government-based	Non-government-based
Development of the trusted registry	The government develops and maintains the public and decentralized registry. If using a blockchain network, they would also define the rules regarding permission for others to be part of the network	Private entities, typically consortia, would develop and maintain networks
Development of reliable digital wallets	The government designates certain service providers as trusted providers of digital wallets	There would be a marketplace of digital wallets that users can trust to manage their authenticators and credentials, which provide pseudonymity, security, and guarantees for recovery. Different vendors would compete for spots in this market.
Attraction of users	The government makes it mandatory for citizens to use a digital ID for government-based services	There would be interesting applications for natural and legal persons to encourage the use of digital wallets and to generate and manage DIDs. The development of a marketplace of service providers accepting SSI would be fundamental.
Generation of DIDs	The government would either develop or choose one existing DID method and require wallet providers to use those as well.	The open community contributes to the effort of proposing safer and more scalable DID methods. Different wallet providers will choose which method(s) to use.
Recognition of standards	In order to be accepted and implemented worldwide, standards, such as decentralized identifiers and verifiable credentials, have to be recognized by international agencies of standards, such us IEEE, ISO, ITU, or NIST	In order to be accepted and implemented worldwide, standards such as decentralized identifiers and verifiable credentials have to be recognized by international agencies of standards, such us IEEE, ISO, ITU, or NIST
Issuance of verifiable credentials	The government could develop infrastructure and protocols to issue verifiable credentials such as digital ID documents (e.g. a digital passport)	Organizations need to develop mechanisms to issue SSI-based digital credentials, so that a market of identity issuers would emerge
Acceptance by service providers	For service providers, government-issued digital ID documents compliant with SSI are very convenient because it provides them with higher user reachability, allowing them to verify customers' identities more easily, quickly, and with higher levels of assurance before providing them with the digital service	Service providers would start accepting SSI solutions to authenticate to their services. Some service providers would become identity issuers of SSI digital verifiable credentials

regulations are not necessary in the short-term. However, in the mid- and long-term, it calls for major changes in regulations to comply with the SSI design principles.[29]

In Latin America and the Caribbean, the LACChain[30] program led by the IDB Lab is already enabling SSI solutions by providing a free network with international standards and protocols, technical support, and a large group of international experts and advisors. It has been recognized by the International Telecommunications Union (ITU) as one of the fourteen architectures of reference in the world (ITU, 2019). In contrast to the EBSI approach, this initiative is non-government-based. It is not a government or set of governments, but rather the IDB and their partners, that maintain the infrastructure. However, LACChain is also advising governments on how to use LACChain's infrastructure, protocols, and standards and on how governments can build their own, exemplifying a complementary government-based approach. LACChain has already supported solutions that leverage self-sovereign identity, such as Proyecto Cadena[31], which was presented in the previous section.[32]

29 https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report-flyer

30 https://www.lacchain.net/

31 https://www.lacchain.net/projects/CADENA

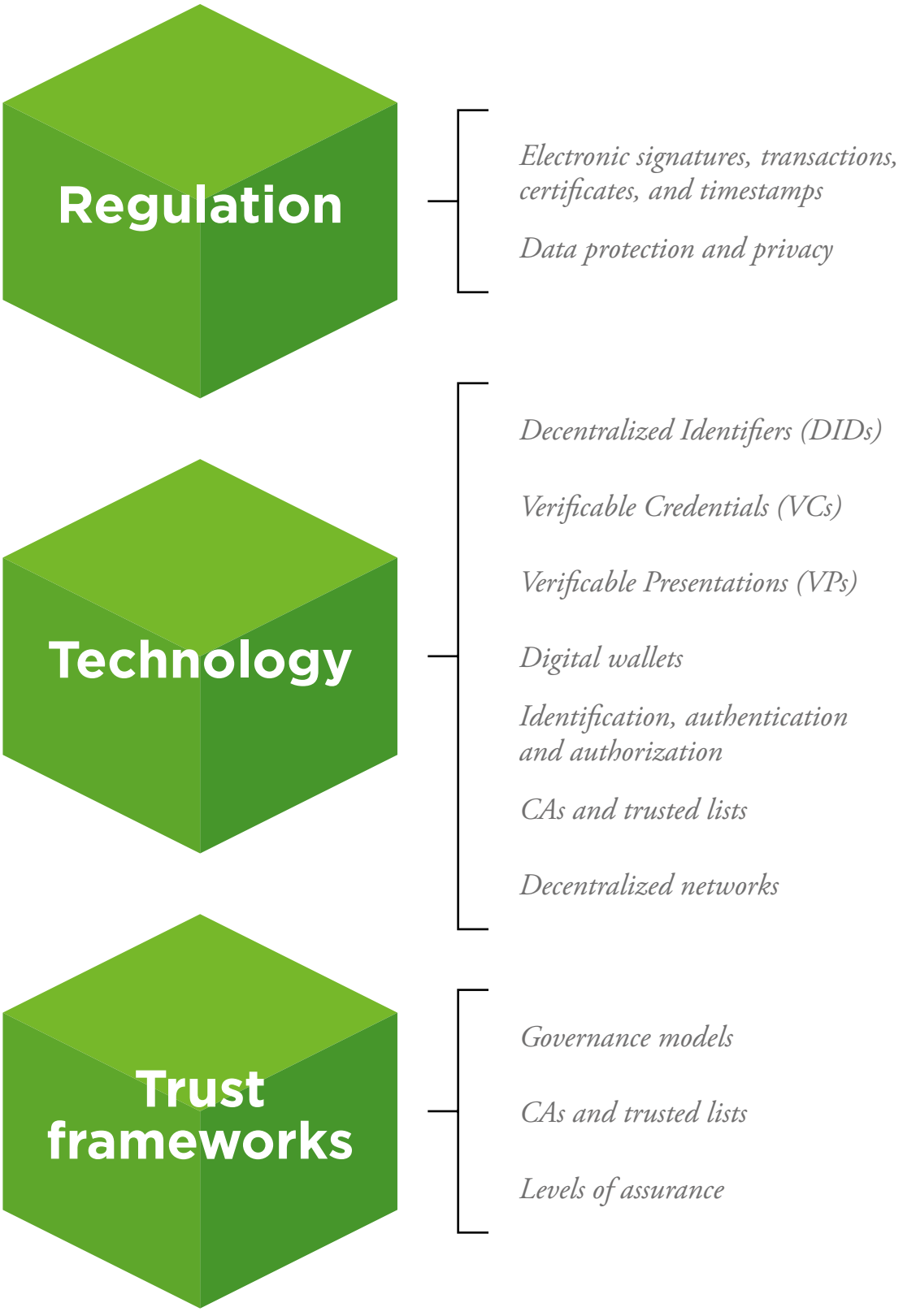
32 The LACChain blockchain network and the EBSI blockchain network use the same technology, standards, and protocols, so these two infrastructures could interoperate. The two initiatives are inspired and collaborating also with Alastria, the pioneer effort led by a big community of associated entities in Spain.

SELF-SOVEREIGN IDENTITY

Chapter II
The Three Necessary Layers for SSI

Regulation, Technology, and Trust Frameworks

IDB | IDB LAB | LACCHAIN


Regulation
Electronic signatures, transactions, certificates, and timestamps
Data protection and privacy
Technology
Decentralized Identifiers (DIDs)
Verifiable Credentials (VCs)
Verifiable Presentations (VPs)
Digital wallets
Identification, authentication and authorization
CAs and trusted lists
Decentralized networks
Trust frameworks
Governance models
CAs and trusted lists
Levels of assurance

We believe there are three complementary layers to be considered when developing robust, scalable, and compliant SSI solutions.

The first layer is regulation. The SSI model relies on the cryptography of the immutable and decentralized ledgers, the electronic signatures of the transactions and the credentials, and the timestamps. Additionally, in order to guarantee the protection of people's data and information, modern data protection regulations are also required. Unfortunately, there are a number of countries without regulations on electronic signatures and transactions, and a bigger number without regulations on data protection and privacy.

The second layer is technology. At present, there are several new emerging technologies, concepts, standards, and protocols necessary to design and build SSI solutions. First, the SSI identity model requires decentralized ledgers of information. Second, it requires a new set of standards for the generation of the unique identifiers, the verifiable digital credentials, and the verifiable digital presentations. Third, it needs a new generation of digital repositories to allow individuals to store, manage, present, and recover personal data in an easy and secure way. Last but not least, all of these components require new protocols for electronic identification, authentication, and authorization.

The third layer consists of trust frameworks. In a digital identity ecosystem, a trust framework defines the governance model, certificate authorities, identity providers, levels of assurance, and communication channels, among other things. This allows for the establishment of roots of trust, trusted lists, revocation lists, and many other necessary trust elements for the recognition of identities and authorization for access services and information.

SELF-SOVEREIGN IDENTITY

Block 6
Regulation

Regulation is the first layer within the framework of all identity models, including the self-sovereign (SSI). Within the regulation layer we consider regulations on data privacy and protection, and regulations on electronic signatures, transactions, certificates, timestamps, and others.

6.1. Regulatory Policies

The SSI model relies on the cryptography of immutable and decentralized ledgers, digital signatures of transactions and digital credentials, and timestamps. Fortunately, from a regulatory perspective, these topics are not new. However, the proliferation of SSI depends on the recognition of the legal value of elements such as blockchain networks, decentralized identifiers, verifiable credentials, and digital wallets, which will be discussed in more detail in Block 7. The necessary steps to move from current regulations on electronic identification and authentication to enhanced versions that recognize the new elements introduced by SSI need to be analyzed for every particular regulation. Countries that currently lack these regulatory policies have the opportunity to leapfrog up to speed.

These new elements present new challenges, as decentralized technologies have not been widely used for identity management before. Additionally, registering data in international networks also demands new trust frameworks that can build on the national regulatory frameworks, which is discussed in Block 8. In order to overcome these challenges, we can start by answering the following questions:

- If an entity broadcasts a transaction in a blockchain network that might violate the law, and the other blockchain nodes incorporate this transaction into their copy of the ledger, is the entity breaking the law? Are the block generators responsible in any way if they only applied the logical rules for validation of transactions, which typically do not include reviewing data content?
- What are an entity's requirements for compliance with the law if the entity provides services in one or several countries and registers data in a decentralized ledger where some of the copies are maintained in another set of countries when all of these countries have different regulatory policies?
- Is the hash of a personal data also personal data?

It is not the aim of this paper to answer these questions. Instead, the purpose of this chapter is to present an overview of the current state of regulations and highlight the need to update them in order to make sure they can be leveraged to guarantee scalability, interoperability, and data privacy in SSI solutions.

6.1.1. Regulation of Electronic Transactions, Signatures, and Documents in Latin America and the Caribbean

Since 1999, most countries in Latin America and the Caribbean have passed regulations on electronic transactions, signatures, and documents. Table 8 collates the updated information of the regulations on electronic transactions of the 42 Latin American and the Caribbean countries. We have tried to be as accurate as possible and we have left the references to the regulations in the Section References.

Table 8 shows that most countries in Latin America and the Caribbean already have regulations for electronic transactions. All 7 Central American countries and Mexico have regulations; all 13 South American countries except Guiana and French Guiana have regulations too; only in the Caribbean there is a higher number of countries, most of them small islands, that lack regulation, adding up to 9 out of 21 without it. In total, 31 out of the 42 Latin American and the Caribbean countries have regulation on electronic transactions, which represents a 74%.

This is a minimum necessary step to be able to provide a regulatory framework for digital identity, and particularly self-sovereign identity. An analysis of each of these regulations is necessary to determine if and which modifications would need to be accomplished to allow for SSI solutions that are fully endorsed by the law.

Table 8. National regulations on electronic transactions, singatures, and documents in Latin America and the Caribbean.

Country	Region	Regulation	Year
Antigua and Barbuda	Caribbean	Electronic Transactions (Ammendment) Act	2016
Argentina	South America	Law No. 25506	2001
Aruba	Caribbean	-	-
Bahamas	Caribbean	Electronic Communications and Transactions Act	2003
Barbados	Caribbean	Electronic Transactions (Ammended) Act	2014
Belize	Central America	Electronic Transactions (Ammended) Act	2003
Bolivia	South America	Law No. 164	2011
Brazil	South America	Law No. 25506	2001
Cayman Islands	Caribbean	Law No. 4	2000
Chile	South America	Law No. 19.799	2002
Colombia	South America	Law No. 527	1999
Costa Rica	Central America	Law No. 8454	2005
Cuba	Caribbean	Lack of law. Multiple norms	-
Dominica	Caribbean	No legal precedents	-
Dominican Republic	Caribbean	Law No. 126	2002
Ecuador	South America	Law No. 2002-67 (2002) Decree No. 3496 (2018)	2018
El Salvador	Central America	Decree No. 133	2015
French Guiana	South America	No legal precedents	-
Grenada	Caribbean	Electronic Transactions Act	2008
Guadalupe	Caribbean	No legal precedents	-
Guatemala	Central America	Decree No. 47-2008	2008
Guiana	South America	No legal precedents	-
Haiti	Caribbean	Bill on electronic signature	2014
Honduras	Central America	Law No. 35217	2020
Jamaica	Caribbean	Electronic Transactions Act	2007
Martinica	Caribbean	-	-
Mexico	North America	Law Advanced Electronic Signature	2012
Nicaragua	Central America	Law No. 729	2011

Country	Region	Regulation	Year
Panama	Central America	Law No. 51 (2008) Law No. 82 (2012)	2012
Paraguay	South America	Law No. 4017/10 Decree 7369	2001
Peru	South America	Law No. 27269	2000
Puerto Rico	Caribbean	Law No. 148 (2006) Law No. 155 (2010) Law No. 75 (2019)	2019
Saint Barthélemy Island	Caribbean	-	-
Saint Christopher and Nevis	Caribbean	-	-
Saint Vincent and the Grenadines	Caribbean	Electronic Transactions Act	2007
Saint Lucia	Caribbean	Electronic Transactions Act	2007
Suriname	South America	Draft on Electronic Transactions Act	2017
Trinidad and Tobago	Caribbean	Electronic Transactions Act	2011
Turks and Caicos Islands	Caribbean	-	-
Uruguay	South America	Law No. 18600	2009
Venezuela	South America	Law on Data Messages and Electronic Signatures	2014
Virgin Islands	Caribbean	-	-

In order for local and national solutions for digital identity to scale and be interoperable across countries in the region, it is essential to have regional regulations on electronic transactions, signatures, and documents that enable recognition and guarantee non-discrimination. This is both a challenge and an opportunity, and we believe that the decentralization and interoperability that the foundation of self-sovereign identity provides can help facilitate these regional efforts.

6.1.2. The eIDAS Regulation, SSI, and Blockchain

The European Union (EU) has the most advanced and globally recognized regional regulation on electronic transactions, signatures, and documents to date. Adopted on the July 23, 2014,[33] the regulation

33 https://www.boe.es/doue/2014/257/L00073-00114.

910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) "provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities"[34] (EU-eIDAS, 2014). The eIDAS Regulation (EU, 2019):

- Ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available.
- Creates a European internal market for electronic trust services by ensuring that they will work across borders and have the same legal status as traditional paper-based processes.

eIDAS recognizes different electronic elements defined in Article 3. We are particularly interest in the following:

Electronic document: any content stored in electronic form, in particular text or sound, visual or audiovisual recording.

Electronic identification: the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.

Electronic signature: data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

Electronic time stamp: data in electronic form which binds other data in electronic form to a particular time, establishing evidence that the latter data existed at that time.

Electronic seal: data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

eIDAS also distinguishes 3 types of degrees of confidence:

- Simple
- Advanced
- Qualified

Annexes I, II, III, and IV of eIDAS specify requirements for qualified certificates for electronic signatures, qualified electronic signature creation devices, qualified certificates for electronic seals, and qualified certificates for website authentication, respectively. Qualified electronic signatures have the same legal effect as hand-written signatures.

In regard to legal recognition, any electronic signature or seal, regardless of its classification as "ordinary" or "simple", or "advanced" or "qualified," serve the same objective of attributing the content of the document to the natural or legal person, and therefore are potentially valid and, depending on the case, perfectly acceptable. (Alamillo, 2020)

The new technological elements introduced in the SSI schema shall not be considered different from the electronic elements already defined and regulated by eIDAS. Instead, they shall be classified using the existing taxonomy. For instance, smart contracts could be considered electronic documents and electronic signatures used to sign blockchain transactions could be considered electronic signatures, with all the legal consequences it implies.

34 eIDAS oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online, including electronic funds transfers or transactions with public services. This enables both the signatory and the recipient more convenience and security in the electronic transactions. Instead of relying on traditional methods, such as mail or facsimile, or appearing in person to submit paper-based documents, they may now perform cross border transactions. The eIDAS regulation has defined the standards for which electronic signatures, qualified digital certificates, electronic seals, timestamps, and other proof for authentication mechanisms enable electronic transactions with the same legal standing as paper-based transactions.

The major question to be asked in this context is: Is eIDAS, the most advanced regulation on electronic transactions, signatures, and documents, already suitable for SSI and blockchain technology? The eIDAS Bridge[35], an initiative to promote eIDAS as a trust framework for the SSI ecosystem, and EBSI ESSIF[36], the European Self-Sovereign Identity Framework, have identified legal considerations and scenarios with respect to SSI and the eIDAS Regulation[37]:

Very Short-Term Scenarios – No Need of Legal Changes in eIDAS

- Use of notified eIDAS eID means and qualified certificates to issue verifiable credentials
- eIDASBridge: increasing verifiable credentials' legal value and cross-border recognition
- Use current eID nodes to issue a SAML assertion based in verifiable credentials/presentations.
- Short-term scenarios – Mild technological changes and slight modifications of eIDAS
- Use of Verifiable IDs as eIDAS electronic identification means.
- Issuance of qualified certificates based on a specific DID method and verifiable credentials

Mid- to Long-Term Scenarios – Stronger Modification of eIDAS

- Extend the eIDAS notification mechanism to Verifiable Attestations: enhanced Trusted Issuers management.
- Regulate the issuance of Verifiable Attestations as a new trust service.
- Regulate Identity Hubs as a new trust service in support of SSI-based TOOP.
- Regulate delegated key management as an independent trust service.
- Regulate a specific type of DLT/node as a trust service.

Therefore, the eIDAS Regulation will need some modifications to become the legal and trust framework for self-sovereign identity in the European Union. This is a reasonable conclusion, as the eIDAS Regulation was created as a legal framework supporting a digital identity metasystem mainly based in delegated authentication, which is more limited than the self-sovereign approach that enables, among other things, pseudonymity and selective disclosure mechanisms, presented in Section 7.3.7 of this paper. Additionally, it will be necessary an effort from both the regulators and the developers to allow blockchain networks and nodes, and digital wallets to qualify and be certified as trust services.

Aligned with this, after analyzing the compatibility between eIDAS and verifiable credentials, Alamillo makes two key points (Alamillo, 2020)[38]:

- Verifiable credentials must be considered as electronic documents and thus, should not be denied legal effect and admissibility as evidence in legal proceedings, prohibiting its denial just because it is in electronic form.
- There should be defined classes of verifiable credentials with well-defined semantics according to a specific governance framework (e.g. a Verifiable ID or a Verifiable Diploma). This would enable specific recognition for particular purposes.

As a trust framework, eIDAS also establishes communication channels that have been proved vulnerable and could be replaced by the decentralized ledger. This is discussed in Section 8.3.2.

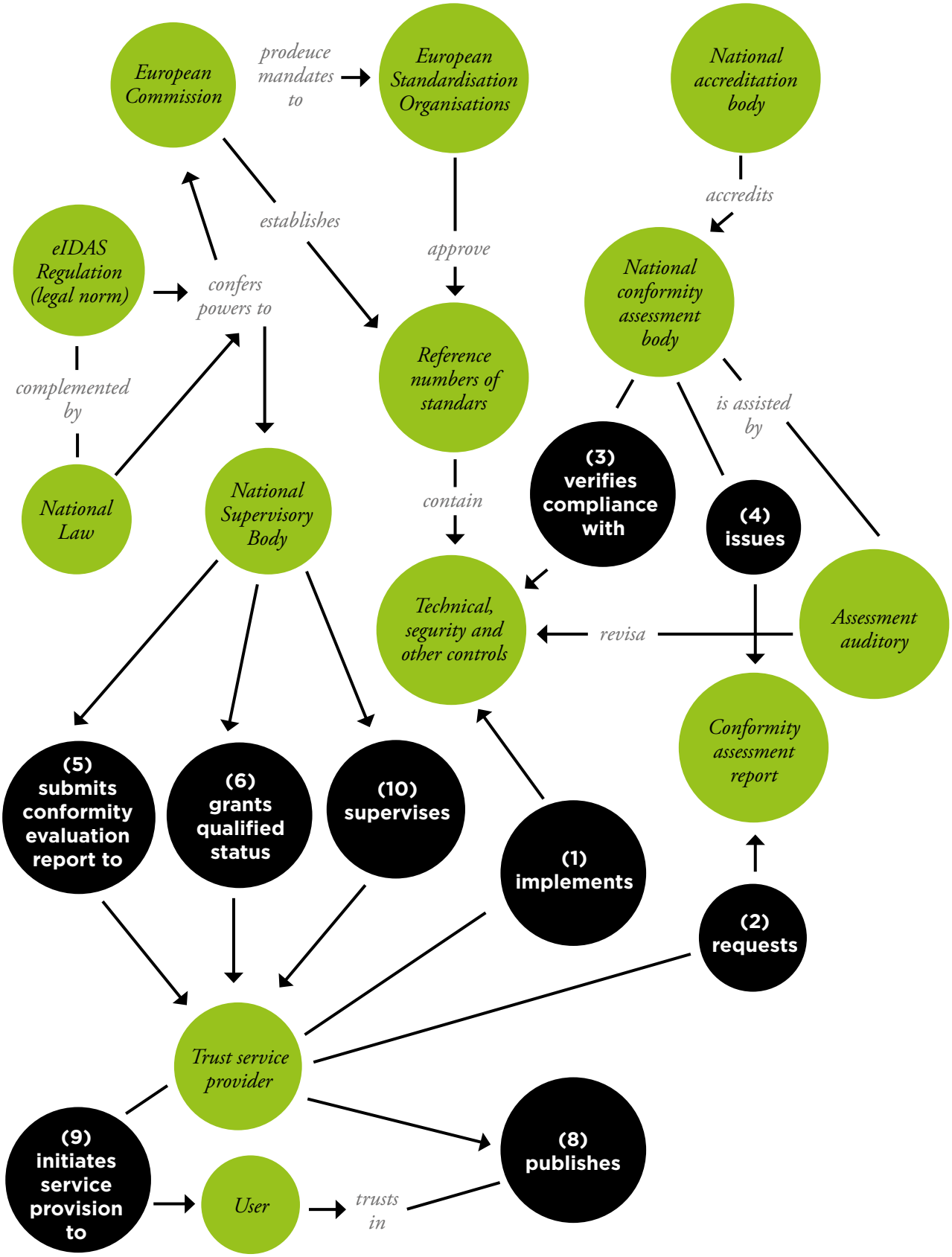
35 https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about

36 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/12/16/EBSI+-+ESSIF+-+Stakeholder+meeting

37 https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report-flyer

38 This publication by Nacho Alamillo, one of the most recognized experts in the eIDAS Regulation and SSI that advices the European Commission, is a mandatory reading on SSI and regulation.

Image 13. Conceptural regulatory model of eIDAS Regulation (Alamillo, 2019).



6.2. Data Protection

In an increasingly digital world, it is essential to protect people's data and privacy. The best way to enforce these protections is through regulations. Unfortunately, many countries either lack or have outdated data protection regulations, including many countries in Latin America and the Caribbean.

6.2.1. Data Protection Regulations in Latin America and the Caribbean

Less than half of the countries of Latin America and the Caribbean have passed regulations on data privacy and protection. Table 9 collates the updated information of these regulations in the 42 Latin American and the Caribbean countries. We have tried to be as accurate as possible and we have left the references to the regulations in the References section.

Table 9 shows that most countries in Latin America and the Caribbean do not have regulations on data privacy and protection. According to our research, South America is the most advanced region with 8 out of 13 countries having regulations. In Central America we found that only 3 out of 7 countries have regulations, which is much worse than the number of regulations on electronic transactions that we presented in Section 6.1.1, where we showed that all the Central American countries have already passed regulations on that matter. In North America, Mexico has regulations. In the Caribbean, only 5 out of 21 countries have regulations. This adds up to a total of only 17 out of the 42 Latin American and Caribbean countries having regulations on data privacy and protection, representing only 40%.

6.2.2. GDPR, SSI, and Blockchain

The most advanced international regulation on data privacy is the General Data Privacy Regulation (GDPR). This is a European regulation, in effect as of May 25th, 2018, to all states that are members of the European Union, put in place in order to "harmonize data privacy laws across Europe". (EU-GDPR, 2016) GDPR has been acknowledged worldwide for many reasons:

- It is the most advanced and complete regulation on data privacy to date.
- It applies to entities outside the EU that use European citizens' data, making it a global solution. This inspires motivation for non-European countries to develop regulations that are compliant with GDPR that enable data with European countries.
- Interestingly, it is a regional effort, making it unique. For example, in the US there is no common regulation for data protection for all states; rather, there are several laws at both the federal and state levels. An example of a state-level law is the California Consumer Privacy Act (California, 2018).

We believe that if SSI solutions are implemented in alignment with recommendations made in this paper, they can be completely compliant with GDPR. To further make this point evident, we will focus on six of the main areas of convergence between GDPR and SSI:

Consent: SSI, as introduced in Section 2.4.5, presents a change of paradigm for digital identity. In traditional identity schemes, such as centralized or third-party provider, the subject of an identity is not in control of their keys, credentials, or data. In SSI, the subject of the identity is in control of these aspects and decides when to share them with others in the form of verifiable presentations (defined in Section 7.3). Therefore, developing solutions that comply with consent is efficient because (i) it is not necessary for third parties to exchange identity subject information, and (ii) it is much easier to reach out to and ask the identity subject for consent.

Data portability: Data portability is provided by digital wallets, where an individual can store their keys, credentials, and data. As we will present in Section 7.5.2, cloud and mobile wallets are the most portable options to date.

Table 9. Data protection regulations in Latin America and the Caribbean.

Country	Region	Regulation	Year
Antigua and Barbuda	Caribbean	Data Protection Act	2013
Argentina	South America	Law No. 25325	2000
Aruba	Caribbean	-	-
Bahamas	Caribbean	Data Protection Act	2008
Barbados	Caribbean	Data Protection Bill	2019
Belize	Central America	Lack of regulation. Protected by the Freedom of Information Act (2000)	-
Bolivia	South America	Lack of regulation. Constitutional right to privacy in personal communications Draft No. 185-2019	-
Brazil	South America	Law No. 13709/2018 (LGPD)	2018
Cayman Islands	Caribbean	-	-
Chile	South America	Law No. 19628 (1999) and No. 20575 (2012)	2012
Colombia	South America	Law No. 1581 (2012)	2017
Costa Rica	Central America	Law No. 8968	2011
Cuba	Caribbean	Lack of regulation. New constitution recognizing personal data rights in Articles 48 and 97 (2019)	-
Dominica	Caribbean	-	-
Dominican Republic	Caribbean	Law No. 172-13	2013
Ecuador	South America	Protection of privacy and personal data Bill	2016
El Salvador	Central America	In development in 2020	-
French Guiana	South America	No legal precedents	-
Grenada	Caribbean	-	-
Guadalupe	Caribbean	-	-
Guatemala	Central America	-	-
Guiana	South America	-	-
Haiti	Caribbean	-	-
Honduras	Central America	Under development	-
Jamaica	Caribbean	Data protection act	2017

Country	Region	Regulation	Year
Martinica	Caribbean	-	-
Mexico	North America	Federal Mexican Law on Data Protection	2010
Nicaragua	Central America	Law No. 787	2012
Panama	Central America	Law No. 81 of 2019	2019
Paraguay	South America	Law No. 1862/01 and Law 1969/02	2001
Peru	South America	Law No. 29733	2011
Puerto Rico	Caribbean	-	-
Saint Barthélemy Island	Caribbean	-	-
Saint Christopher and Nevis	Caribbean	-	-
Saint Vincent and the Grenadines	Caribbean	-	-
Saint Lucia	Caribbean	-	-
Suriname	South America	-	-
Trinidad and Tobago	Caribbean	-	-
Turks and Caicos Islands	Caribbean	-	-
Uruguay	South America	Law No. 18331	2008
Venezuela	South America	-	-
Virgin Islands	Caribbean	-	-

Data protection by design and by default: All aspects of the SSI model presented in this paper, including DIDs, verifiable credentials, verifiable presentations, identification, authentication and authorization, digital repositories and wallets, and a decentralized registry, are designed to protect data by default.

Pseudonymization: As pointed out in Section 3.3, pseudonymization is a direct benefit of SSI. In order to guarantee pseudonymization, suitable DID registries and DID methods must be used (see Sections 7.1.3 and 7.1.4). These will allow for an identity holder to manage as many pseudonymous identifiers as desired so that they can interact with various services securely. They can authenticate without revealing more data or PII than desired. Pseudonymity is also one of the main advantages of DID documents and verifiable presentations over the traditional X.509 for electronic identification. Additionally, the SSI model enables functionalities such as selective disclosure mechanisms and ZKP, which will be presented in Section 7.3.7.

Records of processing activities: As data is connected to identifiers, and individuals are responsible for sharing their own credentials, digital wallets should be able to keep a private record of processing activities, which will be addressed in Section 7.5. Additionally, public and decentralized blockchain registries allows for more pseudonymous traceable data; nobody will be able to correlate identifiers if suitable solutions are developed, as we will discuss in Sections 7.1.3 and 7.1.4. In all cases, data privacy must be preserved, including the PII that could be derived from exchanges and verifications.

Right to erasure (right to be forgotten): The right to erasure is always challenging as it implies that one must (i) know exactly where the data is, (ii) be able to authenticate themselves to those who own their data so they can ask them to erase it, and (iii) not have personal data in immutable and decentralized registries. SSI enables the achievement of the first two goals with much more ease than other digital identity models, but the third goal must be carefully taken care of. Bad implementations of SSI and blockchain very easily could violate data privacy. However, by following the guidelines of this paper, this problem can be avoided. Additionally, digital wallets should provide easy ways to track where one's identifiers have been used and for what purposes, allowing request for erasure. On the service providers' side, the mechanism to guarantee the right to erasure should also be enabled proactively.

SELF-SOVEREIGN IDENTITY

Block 7
Technology

The self-sovereign identity model requires new technological components, standards, and protocols. At present, these three elements are at different levels of maturity. We have classified technological components into seven categories: decentralized identifiers (DIDs); verifiable credentials (VPs); verifiable presentations (VPs); authentication, authorization, and identification; digital wallets; certificate authorities (CAs) and trusted lists (TLs); and distributed ledger technology (DLTs).

7.1. Decentralized Identifiers (DIDs)

7.1.1. Definition

A working group with the World Wide Web Consortium (W3C) is currently developing the Decentralized Identifiers (DIDs) standard (W3C-DID, 2019). A DID is "a new type of identifier that enables verifiable and decentralized digital identity. A DID identifies any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) that the controller of the DID decides that it identifies." The different realizations of the DID standard are referred to as DID methods.

7.1.2. DID Documents

A DID should point to a DID document that contains information about the authentication methods to prove ownership of that DID, endpoints, and other attributes. As sorted by NIST, a DID document is comprised of the following standard elements (NIST-TA, 2020):

- A Uniform Resource Identifier (URI) to uniquely identify terminology and protocols that allow parties to read the DID document
- A DID that identifies the subject of the DID document
- A set of authenticators (i.e. public keys) used for authentication, authorization, and communication mechanisms
- A set of authentication methods used for the DID subject to prove ownership of the DID to another entity
- A set of authorization and delegation methods for allowing other entities to operate on behalf

Image 14. Example of a basic DID Document (W3C-VC, 2019).

EXAMPLE 14: Authentication field containing three verification methods

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  ...
  "authentication": [
    // this method can be used to authenticate as did:...fghi
    "did:example:123456789abcdefghi#keys-1",
    // this method can be used to authenticate as did:...fghi
    "did:example:123456789abcdefghi#biometric-1",
    // this method is *only* authorized for authentication, it may not
    // be used for any other proof purpose, so its full description is
    // embedded here rather than using only a reference
    {
      "id": "did:example:123456789abcdefghi#keys-2",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    }
  ],
  ...
}
```

of the DID subject (i.e. holders different from the subject).
- A set of service endpoints to describe where and how to interact with the DID subject
- A timestamp for when the document was created
- A timestamp for when the document was last updated
- Cryptographic proof of identity (e.g. digital signature)

Additionally, we believe that DID documents should also contain an element that indicates the status of the DID document (active, suspended, or revoked). This would allow the holder to revoke it in case they do not want to use it anymore. By doing that, all the digital documents associated to the DID would no longer accomplish successful verifications, as the verification of the DID subject would fail.

In the simplest model, a DID would be a public key generated from a private key using asymmetric cryptographic algorithms such as RSA, elliptic curves (EC), or discrete logarithms. In the case of public keys, the authentication mechanism requires solving a cryptographic challenge, using the private key associated with the public key that constitutes the DID. However, this should be avoided for security and privacy reasons. DID documents should contain more than one authentication mechanism and the private key used to generate the DID should not be used as one of them. More specifications on this are provided in Section 7.1.4.

The most widely adopted elliptic curve and hash function in the DLT space are secp256k1 and keccak-256, respectively. Unfortunately, neither are endorsed in SP 800-186 (NIST-ECDM, 2019) and FIPS 186-5 (NIST-DSS, 2019). A joint effort between Consensys, the Decentralized Identity Foundation (DIF), the Enterprise Ethereum Alliance (EEA), the World Wide Web Consortium (W3C) Credentials Community Group, Hyperledger, and individual W3C member companies submitted a request for NIST to "include the secp256k1 curve as part of the endorsed ECDSA schemes, and the use of keccak-256 in the secp256k1 signature schemes," arguing that "there are no significant security differences between for example the NIST endorsed secp256r1 and secp256k1 or the sha3-256 hash versus keccak-256". They claim that this would "minimize the damage to innovation and markets caused by the difference between the standards being adopted by the world and those currently endorsed by NIST". (Consensys et al, 2019)

As emphasized in Section 5 of this paper, it is very important for protocols and standards used in blockchain and self-sovereign identity to be recognized by international standards organizations. This includes cryptographic algorithms as well. Additionally, it is essential that the blockchain community does not underestimate the need to start testing quantum-safe algorithms too. Any cryptography based on RSA, elliptic curves, or discrete logarithms will be broken by quantum computers when they are large enough, which NSA (NSA, 2016), NIST (NIST-Q, 2016), and ETSI (ETSI, 2015) warned back in 2015 and 2016.

The DIF maintains an interface for JavaScript applications to resolve DID documents from Decentralized Identifiers[39], and LACChain also provides a service to resolve DIDs[40].

7.1.3. DID Registries

In Section 3.5, we explained some benefits of using blockchain technology for SSI. Some of these benefits are actually requirements for scalable implementations of DIDs. For example, when working with DIDs, it is necessary to have DID registries. Because any entity can generate their own DIDs, having centralized and independent databases used as DID registries would not work. DIDs are expected to serve as identifiers for many different applications. For each of these applications to know where the registry is and how to verify the ownership of the DID against it, would

39 https://uniresolver.io/

40 https://didresolver.lacchain.net/

Table 10. Types of DID registries in Ethereum-based blockchain networks based on NIST (NIST-TA, 2020).

		Description	Standards	Pros	Cons
On-chain	**Credential registry acting as identifier**	Each identifier has a dedicated smart contract	ERC-725 (Proxy Account) ERC-734 (Key manager)	Decentralization: Very decentralized Maintenance and sovereignty: Easy to maintain (modify logic, update, or destroy)	Scalability: Very expensive in terms of transactions
	Global identifiers registry	A single monolithic smart contract, or set of integrated contracts, act as a global registry for storing and managing all identifiers.	Hyperledger Fabric	Scalability: Cheaper in terms of transactions	Maintenance: Challenging to define reliable governance models Single point of failure
	Anchors registry	A single monolithic smart contract acts as a global registry that registers the hashes of identifier management operations that are grouped together into bundles, or "anchors."	did:element[41]	Interoperability: External storage systems Scalability: Cheap in terms of transactions Data protection: Metadata of the DID document is not registered in the blockchain. Just the hash	Integrity: If one of the two layers is compromised, it might be challenging to reconcile
Off-chain	**Bringing your own blockchain address**	Any blockchain address is a valid identifier and can be immediately used without having to be registered beforehand.	ERC-1056 Lightweight Identity	Scalability: Identifier creation takes place offline without any gatekeeper and at no cost. Privacy: DIDs are not identifiable by default	On-chain logic may be necessary to implement additional functionalities, such as identifier management and verification capabilities

41 https://github.com/decentralized-identity/element

be unpractical. This is similar to the issue with the centralized identity model. With centralized registries we would keep having dependency of centralized entities, which facilitates hacks and attacks and limits accessibility and scalability. Instead, decentralized ledgers that all entities know and have a copy of seem to be the most suitable "databases" for DID registries.

NIST has proposed a classification model for the types of DID registries when using blockchain networks, especially Ethereum-based, which allows for leveraging smart-contract-based functionalities. (NIST-TA, 2020) Table 10 shows the description of each type, the related standards and implementations, and pros and cons.

In the case of the global identifiers registry, "governance models can range from the entity deploying the contract having complete control of the system, having only limited control of it, or having no control of it. In the case of no control, the governance of the contract would be run by participating users (e.g., with a DAO)."

In the case of the anchors registry, "the bundling (grouping) of identifier management operations is executed by a second layer protocol that sits on top of the blockchain to which the anchors registry is located. The protocol then adds the hashes of those anchors in the registry, and uses decentralized storage systems such as the Inter-Planetary File System (IPFS)."

In the case of bringing one's own blockchain address, "the identifier creation and storage is usually done locally in the identity wallet. Resolving a DID to its DID document consists in iterating over the DID operations that may have been posted."

7.1.4. DID Methods

Realizations of the DID standard are called DID methods. DID methods may vary in terms of the mechanism proposed for the generation of DIDs, the authentication methods, or the decentralized ledgers used as registries. There are no official lists of DID methods. However, the W3C[42] and the DIF[43] maintain informal lists.

DID methods should comply with the following requirements:

- Allow responsible use of biometrics (by wallets and applications used to operate these DIDs)
- Contain all the elements listed in Section 7.1.2, including the status of the DID document.
- Have more than one authentication method (i.e. RSA, EC, post-quantum keys, and biometrics)
- Use quantum-safe cryptography for the authentication, encryption, and signature
- Destroy the seed of the DID so it cannot be re-generated by a hacker in case of theft
- Do not disclose any personal data or information in the DID documents
- Guarantee privacy and pseudonymity in the use of the DIDs.
- Have more than one authenticator for each authentication method (e.g. several RSA public keys).
- If the DID was generated from a private key, do not use the associated public key for authentication, encryption, or signature.
- Register the DIDs in a smart contract with a well-defined governance (an on-chain DID registry)
- Be scalable enough to economically afford the generation of the required amount of DID for the specific use case in the chosen network.
- Set different functionalities for the different keys, so that some primary keys can be used for authentication, some secondary keys can be used for temporary delegation, and some tertiary keys can be used for retrieving primary and secondary keys
- Store the DID documents in the blockchain so that issuers or verifiers that must resolve specific DID can easily find them

42 https://w3c-ccg.github.io/did-method-registry/

43 https://github.com/decentralized-identity/universal-resolver/

The standardization of this basic structure is, in fact, revolutionary. As presented in Sections 2.4.5 and 3.1, the self-sovereign identity model starts with unique identifiers that entities can self-generate, manage, and prove ownership of. Establishing the rules for their use and getting them recognized internationally is essential.

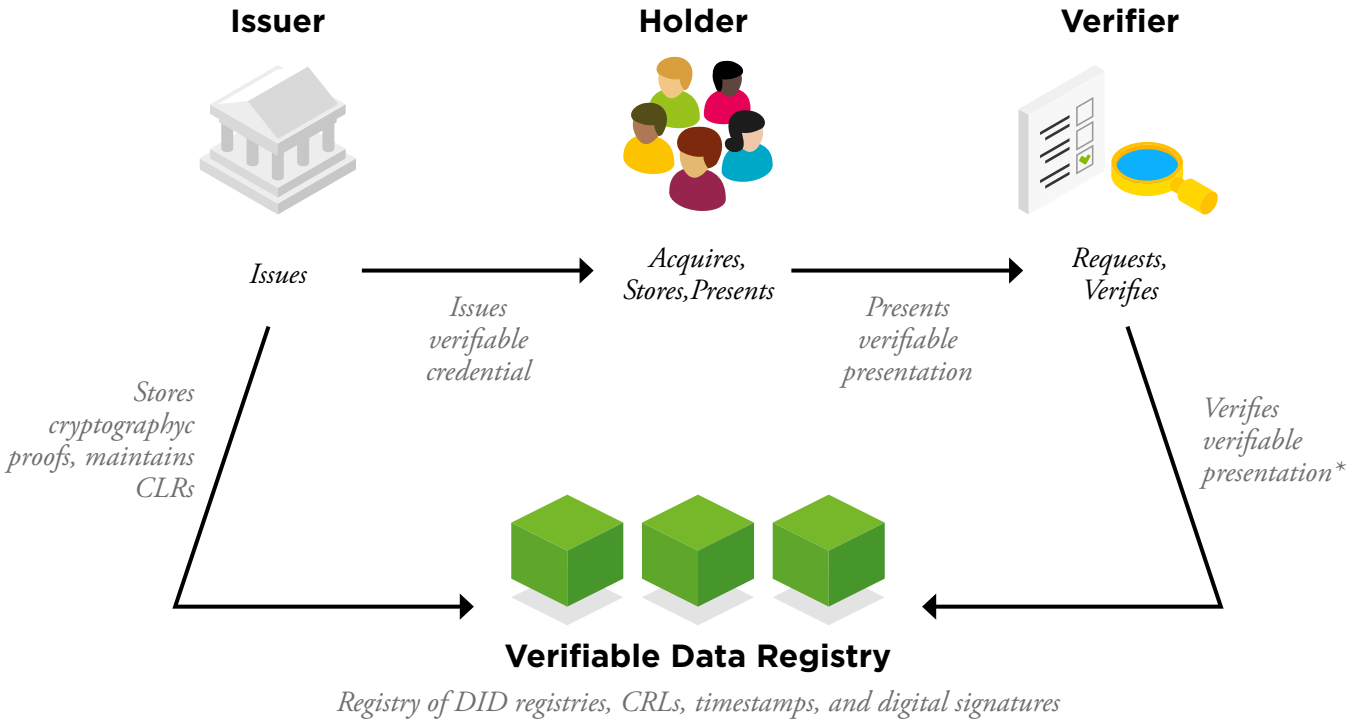
One could argue that traditional standards, such as X.509 certificates, could play the role of a DID document in the SSI model. However, they cannot offer the minimum requirements needed for solutions that are scalable, reliable, and guarantee data privacy. In fact, in the SSI model, X.509 certificates are replaced by the combination of a decentralized identifier and a verifiable credential issued by a trusted entity. However, in the short-term, it is very possible that existing X.509 certificates will be used to generate verifiable credentials.

7.2. Verifiable Credentials (VCs)

7.2.1. Definition

In order to build a self-sovereign identity solution, the second step after having a mechanism to generate unique identifiers is to have trusted issuers issuing verifiable credentials. A verifiable credential is a digital file that contains one or more key-value claims (e.g. birth date, name, qualifications, gender, citizenships, etc.) about an entity (the subject), issued by another entity (the issuer), and verifiable by any entity (the verifier). A Working Group with the W3C is working on defining the Verifiable Credentials (VC) standard. A Verifiable Credential contains claims, metadata, and proofs. Proofs are what make the credential verifiable. The VC specification by W3C does not

Image 15. Simplest flow of the lifecycle of a verifiable credential.



* Check the LACChan Verification Proccess for more information

enforce a specific proof algorithm but does describe the articulation between a credential and a specific proof method. Implementers are free to come up with their own proof method or to follow someone else's.

The subject of the credential is the decentralized identifier of the entity that the attributes in the credential are about. The verifier can always decide whether they trust the issuer of the credential or not.

7.2.2. Structure and Format

As noted by NIST, a Verifiable Credential is a file that is comprised of the following standard elements (NIST-TA, 2020):

- URI to uniquely identify the credential and/or the subject of the credential (e.g. DIDs)
- URI to identify the issuer (e.g. a DID)
- URI to identify the credential type
- URI to identify terminology and protocols that allow parties to read the credential
- Cryptographic proof of the issuer
- Claims data or metadata
- Issuance date
- Expiration conditions
- Location of the credential status (e.g. a smart contract in a blockchain network)

Additionally, we recommend the following:

- The subject and issuer DID can be found and resolved in the blockchain
- Claims data or metadata from the credential are never registered in the blockchain
- Expiration conditions can be automatically checked from the credential
- Credential status can be verified against a smart contract living in the blockchain and nobody but the issuer should be able to change it[44]

Some of the preferred formats are JWT, JWS, and JSON-LD.

44 This eliminates the need of external and/or centralized CRL or OCSP

7.2.3. Registry

NIST has outlined a classification of the types of credential registries when using decentralized ledgers that allow for the deployment of smart contracts. (NIST-TA, 2020) Table 11 highlights the description of each type, as well as their pros and cons.

For credential registries, we recommend the off-chain option because it is the only one scalable in terms of transactionability and storage, and the only one that allows to meet data protection requirements. When the off-chain option is chosen, the blockchain is queried for verification of credentials. In most blockchain networks these queries do not generate transactions. Therefore, they do not leave any track nor consume any blockchain resource. In ideal implementations:

- The DID of the subject and the issuer can be found in blockchain registries
- Claims data or metadata from the credential are never registered in the blockchain in a readable way
- Expiration conditions can be automatically checked from the credential and verified against the blockchain
- Credential status can be verified against a smart contract living in the blockchain, and nobody but the issuer should be able to change it. This eliminates the need for external and/or centralized CRL or OCSP

7.2.4. Storage

As introduced in Section 3.1, holders use private repositories to store and manage credentials. These repositories are typically digital wallets which also allow for the generation of verifiable presentations to be shared with others. In the off-chain model presented in Section 7.2.3, credentials are stored in and protected by the software and/or hardware chosen by the user. The use of mobile apps as digital wallets seems the most reasonable option in terms of security and convenience. In Sections 7.4 and 7.5, we provide guidelines for repositories related to identification, authentication, authorization, security, and key recovery, among others.

Table 11. Different types of credential registries in blockchain networks, according to NIST (NIST-TA, 2019).

		Description	Pros	Cons
On-chain	**Per-identifier credentials registry**	Credentials are managed as entries in a per-identifier smart contract that acts as a container	-	Scalability: Very expensive in terms of transactions and storage Data privacy: Very hard to guarantee data privacy requirements
	Global credentials registry	All credentials corresponding to different entities are registered and managed as entries in a single smart contract	-	Scalability: Very expensive in terms of transactions Data privacy: Very hard to guarantee data privacy requirements Governance: The ownership of the smart contract belongs to the entity that deployed it
	Non-fungible token registry	Credentials take the form of a non-fungible token (NFT)[45]. Minting and management of the tokens are performed through an NFT factory smart contract (acts as a registry that manages the NFTs)	-	Scalability: Very expensive in terms of transactions Governance: Very centralized management of the NFT smart contract
	Entitlement to a user-mintable non-fungible Token	A credential takes the form of an entitlement to let a user mint a pre-defined and pre-assigned NFT at a future date or condition	-	Governance: Very centralized management of the NFT smart contract
Off-chain	**Off-chain objects**	Credentials take the form of an off-chain object that acts as a self-contained vehicle for transmitting information directly between parties	Scalable: Cheap in terms of transactions Storage: No blockchain storage is used Data privacy: Can meet data privacy requirements because issuance, storage, and verification are off-chain Verification: Verification is against the blockchain but does not necessarily generate transactions	Traceability: Less traceability (could also be a pro)

45 An NFT is a unique, not interchangeable token that is owned and may be managed and traded.

7.2.5. Exchange

There are at least three types of credential exchanges.

Issuance: The credential is sent from an issuer to the requester, holder, or subject.

Delegation/Transference: The credential is exchanged between requester, holder, and subject.

Presentation: The credential is sent from a holder to a verifier.

For all three types of credential exchanges, the digital channels between the repository where the credential is stored (i.e. the digital wallet) and the service that generates or consumes the credential must be secure and protected.

7.2.6. Revocation

As indicated in Section 7.2, credentials must have a field indicating status, whose value can be changed between active, suspended, and revoked. **Clear revocation rules should be defined for each credential so that it is clear who and under which conditions someone can modify the status.** Some examples are:

- Status is automatically set as active when the credential is issued by the issuer.
- Issuers can change the status to "revoked" when the subject ceases meeting the claims attested in the credential.
- Issuers can change the status to "suspended" when the subject reports that the credential, authenticators, or associated proofs have been compromised.
- Issuers can change the status to "revoked" when the user reports that they do not want to use the credential anymore.
- Subject or holder can change the status to "suspended" when the credential or their keys have been compromised.
- Subject or holder can change the status to "revoked" when they no longer want to use the credential.
- The status of the credential is automatically changed after the expiration date.

In order to register the status of the credential, we encourage the use of smart contracts. In a smart contract, the issuer registers the URI of the credential when it is issued. Then, depending on the revocation rules, authorized entities can change the status directly in the smart contract. The credential should contain the address of the smart contract in the field status, so that in Step 2 of the Verification Process, detailed in Section 7.3.5, it easily can be checked.

7.3. Verifiable Presentations (VPs)

7.3.1. Definition

The W3C introduces the concept of Verifiable Presentations (VP) (W3C-VC, 2019) in the Verifiable Credentials specification. As stated in the specification, "a verifiable presentation expresses data from one or more verifiable credentials, and is packaged in such a way that the authorship of the data is verifiable. If verifiable credentials are presented directly[46], they become verifiable presentations."

7.3.2. Structure and Format

All verifiable presentations should include the following fields:[47]

46 By directly, we mean that we take the credential as issued by the issuer and we present it without any modification or combination with other credentials.

47 This list of requirements assumes that the verifiable presentation is an encapsulation of different verifiable credentials. This is why fields such as the cryptographic proof of the issuer, the expiration conditions, and the status are not specified as required in the presentations because it is assumed that they are present in the credentials that the presentations are encapsulating. As indicated in Section 7.2.2, these fields are required in the verifiable credentials. If a verifiable presentation was a verifiable credential itself, the requirements for verifiable credentials specified in Section 7.2.2 are enough both for the credential and the presentation.

- URI to uniquely identify the presentation
- URI to uniquely identify the type of the object
- One or more verifiable credentials or claims
- URI to identify the entity generating the presentation (e.g. DID)
- Cryptographic proof of the subject (e.g. digital signature)

Verifiable presentations may also include information about a targeted audience or verifier that the credential was issued for.

Some of the preferred formats are JWT, JWS, and JSON-LD.

7.3.3. Storage

Same as for verifiable credentials. See Section 7.2.4.

7.3.4. Exchange

Same as for verifiable credentials. See Section 7.2.5.

7.3.5. Verification Process

The process for the verification of digital credentials is not standardized and, in general, it is not rigorous enough either. We have defined the Verification Process that is presented in this section, which allows any verifier entity to accomplish diligent electronic verifications of digital credentials presented to them by holders.

In any electronic interaction there are two types of verifications: the verification of the electronic information that is exchanged between parties or presented from one party to the other, and the verification of the physical entities behind the digital personas involved in the digital interaction. In the SSI model, individuals store, manage, and present credentials using digital wallets. In general, when a holder presents a credential to a verifier electronically, they first need to establish a communication channel between the holder's digital wallet and the verifier's digital service (e.g. https).

When the verifier receives the credential, they are capable of verfying all the electronic information (i.e. validity of the credential, status, issuer, presenter, and claims) against the blockchain network, as described in Steps 2 to 6. However, the verifier cannot verify directly that the person in control of the device that is sending the digital credential (the presenter) is truly the holder. The verifier needs to trust that the digital wallet used by the presenter accomplishes a diligent authentication process to authenticate users, so no unauthorized user can access other's credentials and present them on their behalf. This is why the Step 1 of out Verification Process consists of the verification of the digital wallet as a trusted service.

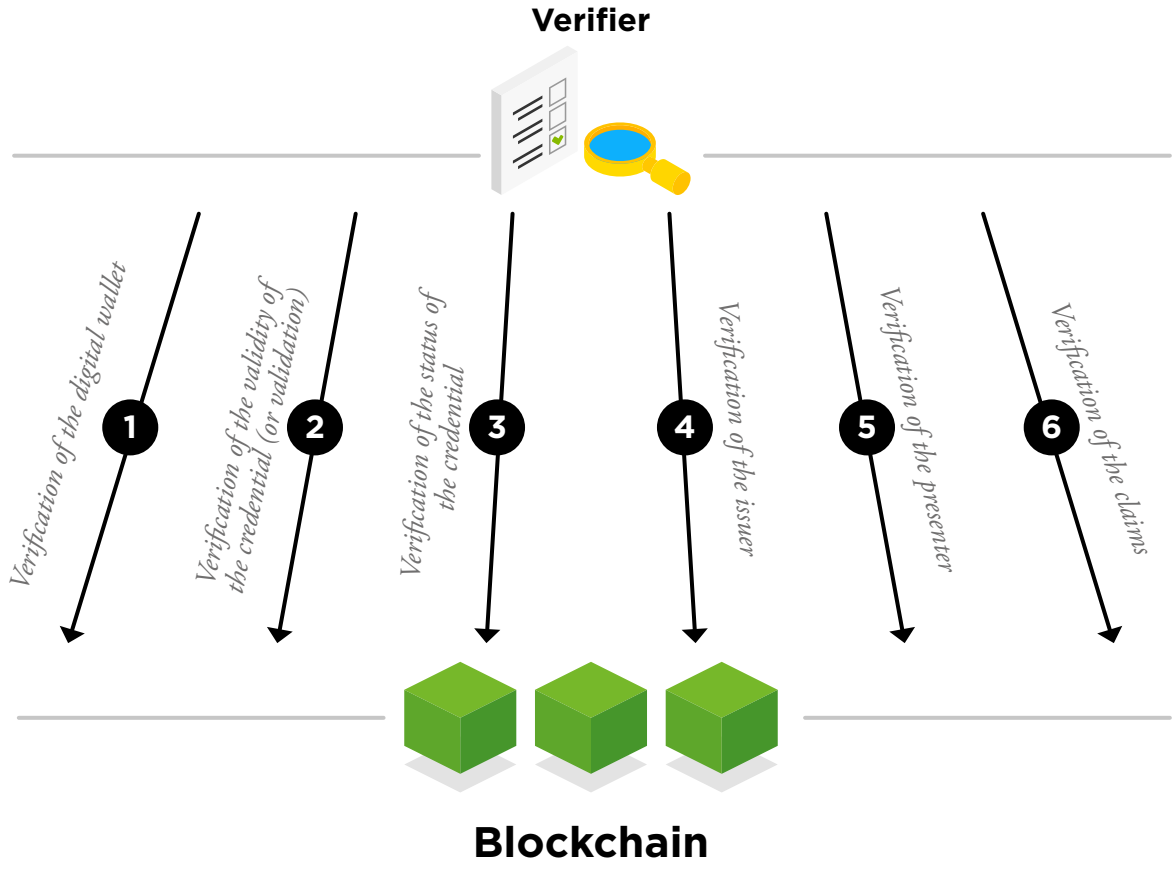
Some regulatory frameworks, such as eIDAS in Europe, introduce the concept of electronic trust services. This allows electronic services that meet specific requirements to be certified and recognized with a certain level of assurance for the provision of electronic services for electronic identification. We believe that it is essential for digital wallets to become some kind of trusted services according to the different regulatory frameworks in order be trusted by verifiers in the authentication of users. This also requires modification of the regulations. The certification of digital wallets as trust services is essential for the scalability of SSI.

Step 1. Verification of the digital wallet: the digital wallet provider guarantees that the presenter of the credential has been authenticated to the wallet with a certain level of assurance. The digital wallet provider assumes a liability for this guarantee.

Step 2. Verification of the validity of the credential (or validation): the verifier verifies that the structure, the format, and the context are correct. All this information is contained in the credential and can be automatically verified by a verification service. Standardization of structure, format, and context will enable worldwide recognition for items such as digital passports, digital diplomas, or digital property titles.

Step 3. Verification of the status of the credential: the verifier verifies that the credential has an active status. As described in Section 7.2.6, we encourage the use of smart contracts for CRLs, maintained by the credential issuers. In this case, credentials would

Image 16. The LACChain ID Verification Process.



contain a field that indicates the address of the smart contract where the identifier of the credential is associated with a dynamic status whose value can be changed by the issuer between "active", "suspended", and "revoked". Step 2 of the verification should only be considered successful when the status is active.[48]

Step 4. Verification of the issuer: the verifier verifies the identity (i.e. the digital signature) of the issuer, and the chain of trust behind their identity, if applicable. To trust the issuer, the verifier must know their real identity. In principle, the credential presented by the holder only contains the DID and digital signature of the issuer, but not additional information about their identity. That digital signature might be unknown or untrusted by the verifier. In that case, in order to verify the issuer's real identity, the verifier must have the ability to know how to access the root of trust behind it. That requires roots of trust that end in a root certificate authority (CA) that is trusted by the verifier.[49] In Section 7.6, we present a blockchain-based approach for

48 At present, in order to enter certain countries, people are required to have a passport is both valid and does not have an expiration date within the following six months. It is our understanding that these conditions may not be necessary in an SSI model where the issuance, presentation, verification, and revocation of credentials can happen it real time. However, if necessary, this could be easily added as an additional condition of the verification process.

49 In order to verify the root of trust behind a DID, we ideally want to be able to end up finding a root CA that is registered in an on-chain DNS, which would be another smart contract recognized by all or some participants of the network. LACChain has enabled an on-chain DNS where the LACChain Permissioning Committee assumes the responsibility for validating the issuers identity and maintaining the DNS.

certificate authorities, trusted lists, and revocation lists. Additionally, in Block 8 we explore the third layer of the identity model, consisting of the trust frameworks that set the rules and governance models for the previous elements. We recommend the use of on-chain DNS using smart contracts.

Step 5. Verification of the presenter: the verifier verifies that the presenter is authorized to present that credential, either because the presenter is the subject or because the presenter has been authorized to present the credential. In the first case, the presenter will be able to prove that they are in control of the DID by solving a challenge to one of the authentication methods. In the second case, there are at least two options. Option one is that the presenter is given one of the private keys required for the authentication of that DID. Option two is that the credential specifies that a DID different from the subject can present the credential, which would be the presenter DID.

Step 6. Verification of the claims: if all the previous steps are successful, the verifier finally gets the information claimed in the verifiable credential and trusts it.

7.3.6. Revocation

Same as for verifiable credentials. See Section 7.2.6.

7.3.7. Selective Disclosure Mechanisms and Zero Knowledge Proofs (ZKP)

In self-sovereign identity schemes, individuals are in control of both their data and credentials. Therefore, they can decide when, how, and to whom they want to present them to. Individuals can also decide how much information they want to disclose. They can have several verifiable credentials issued by several different issuers and create a unique presentation with specific claims from those credentials in a way that it will not disclose any other claims that are made in them. For example, currently, in the physical world, when we are asked to prove we are over a certain age, we usually show a physical ID that not only contains a verifiable claim about our age, but also discloses additional and non-requested information, such as our name, nationality, gender, date of birth, and others. Another example is when we are asked to prove that our income is greater than a certain amount in order to access services such as renting an apartment. This often requires us to reveal the exact amount of income, rather than only proving we make enough.

When working with elements such as blockchain registries and digital signatures in the digital world, there is a more sophisticated way of proving that something is true without the need to reveal any information at all. These claims are known as zero-knowledge proofs (ZKP). According to NIST, the main types of claims are the following (NIST-TA, 2020):

- **Equality or non-equality:** The value of a magnitude is equal or non-equal to a given value.
- **Inequality:** The value of a magnitude is higher or lower than a given value.
- **Membership:** A subject is in a list.
- **Range:** The value of a magnitude is within a given interval [a, b] or not.

In the context of having a prover (the entity trying to prove the veracity of claim) and a verifier (the entity trying to verify whether a claim is true), zero-knowledge proofs should satisfy the following three properties:

- **Completeness:** if the claim is true, an honest verifier will be convinced.
- **Soundness:** if the claim is false, a cheating prover will not be able to convince the verifier.
- **Zero-knowledge:** if the claim is true, the verifier learns nothing other than the fact that it is true.

There are also two types of zero-knowledge proof processes, according to the type of interaction between the prover and the verifier:

- **Interactive:** The prover and the verifier engage in different rounds, in which the prover is required by the verifier to solve challenges.

Table 12. Definition and examples of ZKP.

	Definition	Example
Equality or non-equality	The value of a magnitude is equal or non-equal to a given value	A person is a certain age
Inequality	The value of a magnitude is higher or lower than a given value	An account balance is over a certain amount
Membership	A subject is in a list	A person is a member of a club
Range	The value of a magnitude is within a given interval [a, b] or not	The number of people in a certain population is between 1 and 2 million

- **Non-interactive:** The verifier can verify the veracity of the claim without any further interaction with the prover after the presentation of the proof. In some cases, this requires previous engagements or additional computation assumptions. (Lum et al, 1988)(Wu & Hang, 2014)

7.3.8. Traceability and Monitoring

When the off-chain storage of credentials recommended in Sections 7.2.3 and 7.2.4 is adopted:

- The exchange of credentials also happens off-chain, so it does not leave any tracks in the registry.
- The verification of credentials queries the registry without generating transactions which guarantees there is no traceability.

This helps meet data privacy requirements. However, in some cases the exchange and verification of credentials is intended to be known. This may be the case when measuring the impact of and providing feedback for the solution is important. If that is the case, then the following apply:

- Scalable approaches should be designed for each solution so that transactions can be registered in the ledger when the credentials are presented and verified.
- Data privacy should be preserved, including the PII derived from exchanges and verifications. Only quantitative data should be registered in the ledger and only aggregated data should be collected.

7.4. Digital Repositories and Wallets

7.4.1. Definition

In the context of self-sovereign identity, a digital wallet is a private repository that allows its owner to store, manage, and present keys and identity credentials. A digital wallet should:

- Provide secure access to the holder, by guaranteeing that only authorized entities can access it.
- Ensure security and strong data encryption.
- Provide recovery of keys and credentials.
- Be connected to the ledgers where the DID registries, the trusted lists, and the cryptographic proofs of the DID documents and credentials are stored.
- Provide mechanisms for subjects and issuers to change the status of their credentials.

- Provide mechanisms for the owner to erase all the data associated with them.

A digital wallet may:

- Keep transactional information about the entities, if authorized to it.
- Provide dashboards of activity.
- Provide mechanisms for reducing PII of the entities' activities by combining the use of different DIDs for different interactions.
- Be certified and/or audited to be acknowledged as trusted services.

7.4.2. Types

There can be different types of digital wallets:

- Desktop wallets (installed onto a particular computer)
- Browser wallets (browser extensions installed in a particular computer)
- Hardware wallets (physical devices such as a hard drive or an USB)
- Cloud wallets (based in cloud-storage)
- Mobile wallets (mobile applications)

Mobile and cloud wallets are the most portable options.

7.4.3. Key Recovery

The first layer of our digital identities are our private keys and authenticators. They allow us to prove ownership of our identifiers and credentials. Therefore, it is essential that digital wallets guarantee key recovery mechanisms in case of loss or theft of digital wallets.

As described in Section 7.1.4, suitable DID methods specify different types of keys, so if one primary keys is compromised, a secondary key can be used to revoke it and/or retrieve control over the identity. The lack of this functionality has been one of the disadvantages of cryptocurrencies living in public permissionless blockchain networks. There are cases of users who lost millions of dollars in crypto assets because they lost the private key associated to their account. When key recovery is not possible, if you lose your key, you will never regain access to your account and you will never be able to sue a thief or claim the tokens and credentials lost because you will not be able to prove you ever owned that account.

There are two types of key management systems that can be leveraged for key recovery: centralized and decentralized.

7.4.3.1. Centralized Key Management Systems (CKMS)

Centralized complementary key repositories can be used by entities to store back-ups of their private keys and credentials, so they can retrieve them in the case that the originals are lost or stolen. The natural option for this type of repository is cloud storage. Wallets should be able to provide private cloud-based solutions for key recovery. A second option is off-line back-ups. Wallets should also be able to provide safe mechanisms for users to export keys to hardware.

Identity wallet providers should define clear rules and inform the entities about how and under which circumstances they can retrieve their keys and credentials. Key recovery must balance usability and security.

7.4.3.2. Decentralized Key Management Systems (DKMS)

Decentralized key repositories consist of relying on several entities, persons, or nodes to store the private keys or seeds of private keys of an individual. An algorithm typically leveraged for this approach is the Shamir Secret Sharing protocol (SSS) which allows for the generation of m key seeds in such a way that a customized number of n seeds, provided $n<m$, are enough to recover the key. There are different alternatives for the guardianships:

- **Social key recovery:** The m seeds are stored in private repositories that belong to friends and relatives.

- **Decentralized ledgers:** The *m* seeds are stored in IFPS nodes or blockchain nodes. These nodes must guarantee availability.

Digital wallets may provide both options or combinations of the two.

7.4.4. Recovery of Credentials

Digital wallets are used to store and manage digital credentials. Therefore, when our wallet is lost or stolen, we lose our credentials. It must be possible for an individual to retrieve their credentials if a digital wallet is compromised. As for key recovery, digital wallets should allow for credential back-ups both in the cloud and in off-line hardware devices.

Cloud back-ups or any other back-up facilitated by the wallet provider should define clear rules and inform entities about how and under which circumstances they can retrieve their credentials. The recovery of credentials must balance usability and security.

In addition to credential recovery provided by digital wallet providers, it could be possible to retrieve the credentials by asking the issuer for a re-issuance. As the issuers would need to keep the original data of the credential generation for their own records, they could re-issue a credential to a subject when the original is lost or stolen. However, this would require the subject to reach out and authenticate to each of the entities that had issued them credentials and may incur long wait-times and large costs.

7.5. Identity Proofing, Authentication, and Authorization

Identity proofing, authentication, and authorization are present in every electronic provision of service by a service provider to a requester. Identity proofing consists of verifying that the requester is who they claim to be. Authentication consists of making sure that the electronic service is provided and consumed safely. Authorization consists of verifying that the requester is authorized to consume the service and then allows them to do so.

7.5.1. Identity Proofing

The identity proofing flow is as follows:

1. The requester entity applies for identity credentials.
2. The identity issuer verifies the real identity of the subject.
3. The identity issuer issues the digital identity credentials and sends them to the holder.[50]
4. The holder stores the identity credentials in a repository.

There can be distinguished three levels of identity proofing (NIST-IDGa, 2017):

IP1: There is no requirement to link the applicant to a specific real-life identity. Claims can be self-asserted and credentials self-issued or issued by others that do not comply with any specific requirements. This is useful when accessing digital services, such as websites that only require you to have a pseudonymous profile. In this case, level 2 is omitted.

IP2: The identity issuer verifies the real identity of the entity. Verification can be digital. Issuers should comply with specific requirements, such as having an IP2 or IP3 level of identity proofing themselves. This is useful to access digital services such as social networks (e.g. Facebook or LinkedIn) that require users to be real and identified people.

IP3: The issuer verifies the real identity of the entity with the maximum level of assurance. Verification requires physical presence. Issuers are identified with credentials that follow a root of trust where the main CA is an entity trusted and recognized at a local, national, regional, or international level. This is necessary to access digital services with the

50 The holder and the subject can be the same entity. Holder, as introduced in Section 3.4, is a more general term that allows to refer to the entity in control of the credential whether it is the subject or not.

maximum level of assurance, such as government or financial services.

7.5.2. Authentication

Authentication is always based on three types of factors:

- Something you know (i.e. a password).
- Something you have (i.e. a mobile phone, ID credential received after accomplishing identity proofing, or a cryptographic key).
- Something you are (i.e. a fingerprint or other biometric data).

In order to access digital services with the credentials that one stores in their digital wallets, they must first authenticate to the digital wallet to access their digital identity and then authenticate to the digital service they want to consume.

7.5.2.1. Authentication to the Digital Wallets

In the SSI model, individuals store their keys and credentials in repositories that they manage themselves. These repositories are known as digital wallets. Preventing non-authorized users from accessing digital wallets is critical. If a non-authorized person has access to another person's digital wallet, they would be able to control that person's identity credentials, digital money, cryptocurrencies, digital diplomas, digital property titles, and any other data stored there. In order to have reliable and secure self-sovereign identity solutions, authentication to digital wallets must be extremely secure.

In a robust implementation of a self-sovereign identity framework, the wallets are the weakest point of security by far. Wallet providers must develop solutions that do not require any level of technical or technological skills for the user to ensure their protection. We believe that wallet providers should develop different mechanisms to authenticate the user at the time of accessing the digital wallet, at the time of accessing credentials stored in the digital wallet, and at the time of presenting these credentials to others. These stages can be broken down as follows:

1. **Set up the digital wallet:** The digital wallet should require a minimum set of authenticator factors for the user. Once the user passes the sign-up process, they can start creating DIDs, generating and receiving verifiable credentials, and presenting information to others (i.e. in order to access digital or physical services).
2. **Log in to the digital wallet:** Digital wallets should ensure that authentication factors allow verification of the user's identity with a high level of assurance, combining factors that the user knows, has, and is.
3. **Access digital credentials:** Once the user is logged in, the digital wallet should restrict the user's sensitive information such as their digital credentials and request additional real-time verifications, such as biometrics or security questions, when trying to access this information.
4. **Present digital credentials from the digital wallet to others:** Digital wallets should also require users to pass additional verifications when attempting to share sensitive information to others or when using it to access services. In some cases, the service provider itself could indicate to the wallet that a service requires a high level of assurance in the verification of the subject. For instance, when using a digital passport to access services identified by the service provider as high level of assurance, such as take a flight or to make a financial operation.

As discussed in Section 7.3.5, when a person attempts to use a digital credential from their digital wallet to access a digital service, the first step of the Verification Process is the verification of the digital wallet from which the credential is being presented. If the service provider does not trust the digital wallet, then it will not authorize the access. Service providers will trust digital wallets as long as they know and trust the mechanisms they use to authenticate the individuals. We expect the most advanced digital wallets will get certified as trusted services with various

regulations in order to be recognized and trusted nationally and internationally.

7.5.2.2. Authentication to Services

In order to access a digital service, the holder presents a credential from their digital wallet to the service provider. When receiving the verifiable credential, the service provider has to be able to accomplish the steps in the Verification Process described in Section 7.3.5. This includes the verification of 1) the digital wallet, 2) the structure, format, and context of the credential, 3) the status of the credential, 4) the issuer, 5) the presenter, and 6) the claims.

If the service provider cannot verify all of the previous factors, the authentication process will fail and the individual will not be authorized to access the service. The service provider will not be able to recognize a credential as being valid if they do not trust the digital wallet from which the credential is presented, they do not recognize the syntax of the credential, or they do not trust the issuer. In a self-sovereign ecosystem completely aligned with regulatory policies, non-discrimination of certain authentications coming from qualified digital wallets and standardized credentials issued by qualified and trusted issuers (e.g. a digital passport issued by a government) can be enforced.

7.5.3. Authorization

As introduced in the Verification Process presented in Section 7.3.5, when the credential is presented in order to receive a service (digital or physical), the service provider verifies that the digital wallet presenting the credential (if applicable) is trusted, the credential is valid, the issuer is known, and the presenter is authorized to be presenting that credential. There are two types of authorizations that can be checked when a verifiable credential is presented.

7.5.3.1. Authorization of the Presenter

When a credential is presented in step 5 of the Verification Process, the verifier verifies that the presenter is authorized to present that credential, either because they are a legitimate subject or they have been authorized to present that credential. In the first case, the presenter will be able to prove that they are in control of the DID by solving a challenge to one of the authentication methods. In the second case, there are at least two options. Option one is that the presenter is given one of the private keys required for the authentication of that DID. Option two is that the credential specifies that a DID different from the subject can present the credential, which would be the presenter DID.

If DID documents have different types of authentication methods, as introduced in Section 7.1.4, such that they are used for different purposes (i.e. full control, temporary delegation, and key recovery), then the entity in control of the DID can share some private keys associated with some of the authentication methods with other entities. This way of proceeding can be used by the subject to generate verifiable credentials which indicate that only a specific set of authentication methods associated to the subject DID can be used to prove ownership of that specific credential.

In the case where the credential subject is underage and therefore not authorized to present the credential without approval from a legal representative, the verifier would not accept the credential unless it has the approval of its representative (i.e. by signing the presentation with its digital signature, or by issuing an additional credential of consent). This can be achieved with multi-sign schemes.

7.5.3.2. Authorization of Purpose

When an issuer issues a credential, the issuer can aim to restrict the use of identity information attested in that credential to a specific purpose or service (e.g. an academic identity credential to authenticate the subject first access to digital services provided by a group of universities that have private agreements for the recognition of that credential). In this case, the credential would include a field specifying its purpose.

7.6. Certificate Authorities (CAs) and Trusted Lists (TLs)

In a digital identity model based on PKI, certificate authorities (CAs) are entities that issue identity credentials that are recognized by others with a certain degree of assurance. As presented in Block 5, in government-based solutions, the government designates the root CAs, and in non-government-based solutions, which have the potential to proliferate much faster in the SSI model in the short-term, different private and multilateral entities can become trusted by others as CAs for various reasons.

There are at least a couple of essential trusted lists (TLs). The first trusted list is the list of identity providers or CAs designated by a trusted authority. The second trust list is the list of certificates that each CA has issued to other entities and each of their statuses. This allows us to create roots of trusts to see whether a digital certificate issued by an entity that we do not know or trust is certified by an entity that we do know and trust.

At present, every browser has a user agent that recognizes the signatures of some internationally acknowledged root CAs. Therefore, when any service or site presents to us their X.509 certificate, our browser is capable of tracking the chain of certificates behind it and verifying in real time if it ends in a root CA that the browser knows and trusts. In self-sovereign identity, the mechanism will be exactly the same, but with minimal modifications of protocols that allow, among other things, to replace current X.509 certificates for verifiable credentials.

Today, CAs maintain certificate trusted lists and certificate revocation lists (CRLs). Protocols such as the Online Certificate Status Protocol (OCSP) are applied to these lists to verify whether a certificate is valid. Blockchain technology makes leveraging smart contracts to serve as public and decentralized trusted lists and CRLs possible. With blockchain, instead of having each CA maintaining external databases that are not interconnected, certificate authorities can simply deploy a smart contract in the network and register the URI of each certificate they issue together with their status and additional metadata of interest. As discussed in Section 7.2.2, digital verifiable credentials should contain a field that specifies the location of the information about the status of the credential. If that location is the address of a smart contract, when the credential is presented to others they can automatically verify if the credential has an active status. As is the case with X.509 certificates, the verification is not manual; each application or service has an agent that knows how to conduct verification.

Using blockchain registries and smart contracts reduces costs for CAs as they do not need to maintain and expose centralized databases anymore. This also allows for a transparent traceability because every change in the credential status or list of CAs is registered in the blockchain. Additionally, using these blockchain registries and smart contracts provides more accessibility to information because it is in each copy of the blockchain owned by each node. This also guarantees availability even if the CA's IT infrastructure goes down or the CA disappears because the certificate trust/revocation lists remain in the blockchain ledger and not in a centralized digital repository exposed by the CA.

In the short-term, we expect a combination of the current electronic certificates and blockchain technology in which traditional X.509 will be used to sign blockchain transactions. In the mid-term, we foresee a new generation of credentials that follow the SSI model with DIDs, verifiable credentials, verifiable presentations, and digital wallets substituting the current X.509 certificates and repositories.

7.7. Distributed Ledger Technology (DLT)

As pointed out repeatedly in the previous sections and discussed explicitly in Section 3.6, it is es-

sential for SSI to rely on decentralized ledgers for the storage of the cryptographic proofs of DIDs, the cryptographic proofs and status of verifiable credentials and presentations, the DNS, and the trusted lists, among others. Using blockchain networks provides SSI with the security and the scalability that this digital identity management system pursues. Blockchain networks are specific types of decentralized ledgers characterized by their use of smart contracts to automate processes and represent digital assets. Blockchain networks also contain consensus protocols to generate new blocks and all nodes maintain the same copy of information. Blockchain networks are more suitable for self-sovereign identity than other types of decentralized ledgers because blockchain addresses can be used as DIDs, smart contracts can be used as trusted lists, and they do not require various versions or siloes of information be used between different entities in the network.

According to the International Standards Organization (ISO), there are three types of blockchain networks (ISO, 2018):

Permissionless: Permissionless networks are those that anyone can join at any time, such as Bitcoin or Ethereum. Most of these networks are generally crypto-based[51]. They are open and transparent, but generally have high transaction fees, no privacy[52], and all users are pseudonymous. Additionally, as participants are not identified, transactions and applications can hardly be forced to be compliant with regulation.

Permissioned private: Permissioned private networks consist of a consortium of finite and well-defined entities that deploy, run, and maintain all the nodes. Generally, these networks are developed, and even maintained, by a blockchain service provider. In general, private networks, do not have transaction fees (although there might be a fixed cost charged by the service provider if applicable), and allow for high levels of privacy. However, these networks are not decentralized nor transparent and the scalability is very limited. In addition, they are usually designed for a single use case or application. Examples of permissioned private networks include the hundreds of private blockchain networks behind specific blockchain applications, the IBM FoodTrust,[53] and the blockchain network of the Energy Web Chain by the Energy Web Foundation (EWF) consortium (EWF, 2018).

Permissioned public: With permissioned public network, a consortium initiates a network and allows everyone to join, provided that they meet certain requirements, such as being authenticated and compliant with regulations. In these networks, the consortium is self-sufficient and does not need to rely on a vendor. Permissioned public networks are open, transparent, decentralized, and in general do not have transaction fees. At the same time, every participant is identified so both privacy and compliance with regulation are enabled. Examples of these networks are Alastria in Spain, led by an association of over 500 members; EBSI in Europe led by the European Union; and LACChain in Latin America and the Caribbean, led by the Inter-American Development and its partners in the program.

The self-sovereign identity model can leverage different types of blockchain networks in addition to other decentralized ledgers. However, permissioned public networks are most suitable. Permissionless networks are designed to be anonymous and permissioned private networks are designed to be small and limited to specific use cases. Alternatively, permissioned public

51 Linked to a cryptocurrency.

52 Permissionless networks are not private because all information registered to them is public. However, in principle it is not possible to know who is behind each transaction because accounts are pseudonymous. In practice, pseudonymity does not guarantee privacy because identity can be disclosed in various ways.

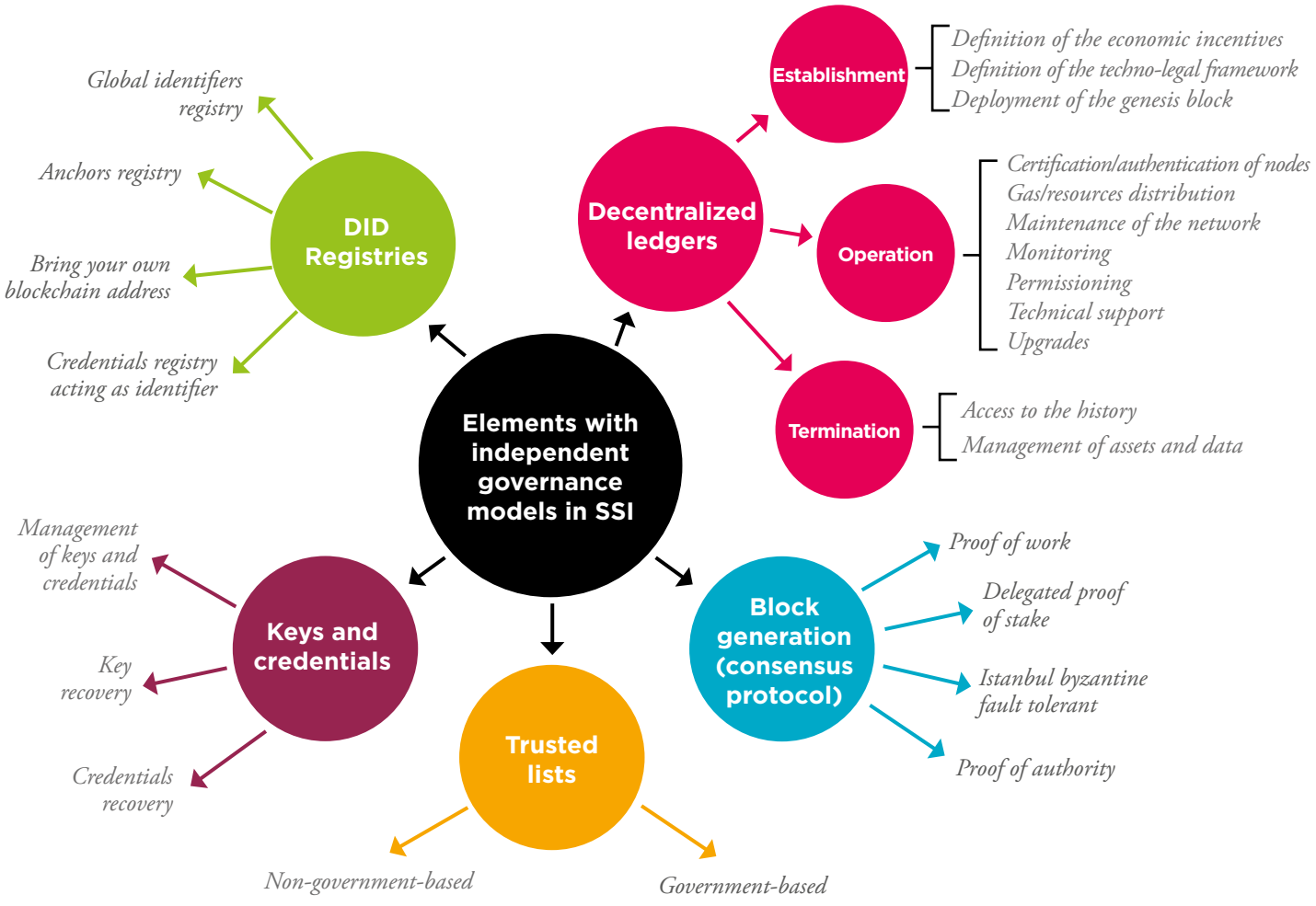
53 https://www.ibm.com/blockchain/solutions/food-trust

networks often have zero transaction fees, are compliant with regulations, and are designed to be multipurpose, making them a perfect fit for the decentralized ledger that self-sovereign identity demands. It is not a coincidence that the three public-permissioned ledgers mentioned in the previous paragraph are leading the SSI initiatives in their respective regions: the Alastria ID framework, the European blockchain-based digital passport, and the LACChain ID framework.

SELF-SOVEREIGN IDENTITY

Block 8
Trust Frameworks

Image 17. Elements with independent governance models in implementations of self-sovereign identity.



According to the Open Identity Exchange (OIX), a trust framework is a "generic term often used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements. […] They are referred to as operating regulations, scheme rules, or operating policies in contexts different from digital identity." The Open Identity Exchange (OIX) is a leader in the SSI field and will be presented further in Section 8.3.1. (OIX-TF, 2010)

The scope of a trust framework[54] spans from recognition within single organizations or groups of entities, to regional, sectorial, and international agreements. An example of a national trust framework is the national ID, which establishes government sovereignty for the issuance of identity credentials. An example of a regional framework is the international recognition of national passports that follow standards dictated

54 There is also a good reference by MIST that can be retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf

by the International Civil Aviation Organization (ICAO). Examples of sectorial frameworks include the mutual recognition agreements (MRA) between customs, the settlement networks between financial institutions, and the recognition of certifications between universities.

In a digital identity ecosystem, self-sovereign or not, a trust framework defines the governance model, the certificate authorities[55], the identity providers, the levels of assurance, and the communication channels, among others. This allows for the establishment of roots of trust, trusted lists, certificate revocation lists, and many other necessary trust elements.

8.1. Governance Models

A governance model establishes principles, policies, terminology, standards, and responsibilities. Metaphorically, frameworks establish the agreements and rules of the game, and governance models define the roles and responsibilities of the players in that game. In current implementations of digital identity schemes, the governance model establishes who the certificate authorities are and where the trusted lists and CRLs can be found. In self-sovereign identity, however, the governance model is more complex because there are new elements that need to be governed, such as the decentralized ledger. We are not aware of any existing classifications of governance layers particular to self-sovereign identity and thus, we propose a structure that is presented in Image 17 and explained in more detail in the following sections.

8.1.1. Governance of the Decentralized Registries and Blockchain Networks

According to ISO/TC "DLT and blockchain systems governance is an approach that comprises elements of central and decentral decision rights, where the accountability is situated within the network and where incentives are provided to reach consensus […]. The governance of a DLT & blockchain systems oversees several key functions during the operational stage of the DLT & blockchain system, such as the enrolment of participatory rights for participants in the DLT & blockchain system and the contracting rules associated with participation in the DLT & blockchain system. All DLT & blockchain systems shall operate within the broader context of external legal and regulatory frameworks; in some case DLT & blockchain systems may provide guidance and on-chain mechanisms for managing the operation […]. The DLT and blockchain systems governance lifecycle view addresses both the risks inherent to and the interests of DLT participants and broader stakeholders during the establishment, operation, and termination of the DLT system" (ISO, 2020).

We believe the essential tasks that comprise governance of a decentralized registry or blockchain network can be divided into the three phases of the lifecycle: establishment, operation, and termination. These essential tasks are:

Establishment

Definition of the economic incentives: definition of the economic incentives in order to guarantee the sustainability of the blockchain.

Definition of the techno-legal framework: definition of the framework that sets the rules and allows the establishment of the technical, legal, and other bodies of the blockchain.

Deployment of the genesis block: designing and deploying of the first block of the network that contains both soft (e.g. the initial validator nodes) and hard rules (e.g. the consensus protocol). Setting the first nodes.

Operation

Certification/authentication of nodes: accomplishing identity proofing and certifying nodes in the network in a way that others can trust.

55 The concept of certificate authority is equivalent to the concept of credential service provider.

Table 13. Comparison between the governance of the tree types of blockchain networks introduced in Section 7.7.

	Permissionless	Permissioned private	Permissioned public
Definition of the economic incentives	Open community	Consortium	Underlying orchestration entity
Definition of the techno-legal framework	Unclear - Might be provided by the software designer	Consortium	Underlying orchestration entity
Deployment of the genesis block	Open community	Consortium	Underlying orchestration entity
Certification/authentication	Does not apply	Consortium	Underlying orchestration entity
Gas/resources distribution	Nobody	Consortium	Underlying orchestration entity
Maintenance	Open community	Consortium	Underlying orchestration entity
Monitoring	Open community	Consortium	Underlying orchestration entity
Permissioning	Does not apply	Consortium	Underlying orchestration entity
Technical support	Open community	Vendor / Technology provider	Underlying orchestration entity
Upgrades	Open community	Vendor / Technology provider	Underlying orchestration entity
Access to the history after termination	Any entity that had a node	Consortium	Any entity that had a node
Management of data and assets after termination	Service and application providers	Consortium	Service and application providers

Gas/resources distribution: managing the distribution of network resources between different users. Guaranteeing the correct operation of the network.

Maintenance of the network: supervising the network and performing maintenance tasks to guarantee that it runs without issues and does not fail, collapse, or die.

Monitoring: providing and maintaining dashboards and monitoring tools, and performing monitoring tasks.

Permissioning: allowing nodes and accounts to join the network (i.e. whitelisting) and removing them (i.e. blacklisting) when they violate the agreements.[56]

Technical support: providing technical assistance in case something fails in the deployment or performance of nodes or applications on top of the network.

Upgrades: accomplishing proactive research and developments in the network to improve security, efficiency, scalability, performance, and interoperability.

Termination

Access to the history: guaranteeing access to the history of transactions.

Management of assets and data: determining of how data or assets (e.g. smart contracts, tokens, proofs of certificates) are transferred, destroyed, or disposed.[57]

Depending of the type of decentralized registry or blockchain network, some of these tasks are accomplished by different entities, while others do not apply. An overview is presented in Table 13.

8.1.2. Governance of the Block Generation (Consensus Protocol)

The process of block generation in a blockchain network is known as *consensus protocol*. The governance of the block generation is independent from the governance of the ledgers themselves, which includes everything that was listed in the previous section. For example, in the context of Bitcoin, the open community is responsible for governing the network, but only a small number of entities govern the block generation. In permissioned networks, an orchestration legal vehicle (representing a consortia) governs the network but any entity is allowed to participate in the consensus protocol[58], whether they are part of the legal vehicle or not. Some of the most mainstream consensus protocols are:

Proof of work: any node in the network can compete with computational power to win a lottery that allows them to generate a new block (known as mining) and be rewarded for it, typically with a native cryptocurrency from the network. This may seem very decentralized in theory; however, in practice with Bitcoin (the largest network that

56 The conditions under which a user is given access to a blockchain network (in permissioned networks) is based on the acceptance of a network's terms of use. These access rules are entirely determined by an underlying orchestration entity. All parties behind the system are known and identifiable

57 We understand that the transference of all smart contracts, tokens, proofs of certificates, and any other data registered in the blockchain is under the responsibility of the entity that registered it. Therefore, it will be also their responsibility to guarantee its availability by transferring it to a different network if a blockchain dies. However, in the case of public-permissioned networks, the underlying orchestration entity should commit to giving advance notice about the termination of the network so that entities can make proper alternative arrangements.

58 Blocks are always generated by the validator nodes, which are constantly listening to new transactions broadcasted by any node in the network. After a certain amount of time, which may vary from seconds to minutes depending on the network, one of the validator nodes is selected to generate a new block that contains the transactions it has been hearing from. This node then verifies the transactions, signs the block, and broadcasts it to the network. The consensus protocol establishes the rules for selecting a validator node for every new block. There are many different consensus protocols.

operates with proof of work), a small group of four mining pools generates 58.7% of the blocks and a slightly bigger group of thirteen mining pools generates 97.6% of the blocks.[59] Additionally, the energy spent by Bitcoin miners is higher than energy consumption in Switzerland, Greece, Israel, or Ireland.[60] This consensus protocol is frequently used in permissionless networks.

Delegated proof of stake: the ability to generate new blocks is delegated to a specific number of nodes. These nodes are then trusted by the others for the generation of new blocks. Between those nodes, proof of stake applies. This consensus protocol is used in both permissionless and permissioned networks.

Istanbul byzantine fault tolerant: validator nodes take turns generating new blocks. An algorithm is applied so the number of validator nodes malfunctioning or trying to tamper with the network in order to cause damage is maximized and the possibility of tampering is minimized. This consensus protocol is used in some permissioned networks.

Proof of authority: the ability to generate new blocks corresponds to a selected group of authorized nodes. These nodes are then trusted by the others for the generation of new blocks. This consensus protocol is used in both permissionless and permissioned networks.

8.1.3. Governance of the DID Registries

As presented in Section 7.1.3, there are at least four types of registries for decentralized identifiers. DID registries can be on-chain or off-chain. In both cases, interactions with a ledger (or chain) are required. Therefore, the governance models for the ledger (or chain) and the block generation presented in Sections 8.1.1 and 8.1.2 affect the governance of the DID registries. Each type of DID registry has a different governance model:

Global identifiers registry: because a single monolithic smart contract is deployed in the ledger to act as a global registry, the governance of the smart contract becomes governance of the DID registry. Different options are possible, including management by a centralized entity, a limited number of accounts, or a DAO.

Anchors registry: same as in the global identifiers registry.

Bring your own blockchain address: in this case, there is no such a thing as an on-chain DID registry. The management and storage of DIDs is done off-chain by the subject and/or holder, and resolving a DID is accomplished through iterations over its registries (transactions) in the ledger.

Credentials registry acting as identifier: each subject deploys a dedicated smart contract to register the DID. The subject is in complete control of the registry.

8.1.4. Governance of the Trusted Lists (TLs)

The establishments of the entities responsible for maintaining the trusted lists corresponds to the trust framework. In alignment with Block 5, we can classify the governance of the trusted lists into two types, depending on whether the government is playing the main role in the trust framework or not.

Government-based: a government either acts as the root CA or designates a list of CAs that become trust anchors. The government also sets the rules for who and how qualified certificates can be issued.

Non-government-based: the government is not the root CA and, through private-agreements, a trust framework emerges so that different entities can decide to trust other entities as root CAs.

59 https://www.buybitcoinworldwide.com/mining/pools/

60 https://www.forbes.com/sites/niallmccarthy/2019/07/08/bitcoin-devours-more-electricity-than-switzerland-infographic/#550986c121c0

8.1.5. Governance of the Keys and Credentials

In the self-sovereign identity model, digital wallets are repositories that store, manage, and present credentials. Ideally, subjects are in full control of their wallets. These wallets should either be in the form of hardware in their possession or software installed in one of their personal devices. The digital identity's subject controls their own identity and decides with whom they will share it. This is precisely what gives this digital identity model it name: sovereignty means that the user controls their own authenticators, credentials, and data. Governance of keys and credentials includes determining the following:

- Who can have access to the subject's keys and credentials
- Who can present a credential to others and under which conditions
- Where the back-ups are located
- Who can facilitate a subject's key recovery
- Who is responsible and liable for loss or theft of keys and credentials

8.2. Certificate Authorities (CAs), Trusted Lists (TLs), and Levels of Assurance (LOAs)

In a digital identity model, certificate authorities (CAs) are entities that issue identity credentials and are recognized by others with a certain level of trust and assurance. As presented in Block 5 and Section 8.1.4, there are two types of trust frameworks, depending on whether the government plays a main role or not. In government-based solutions, the government either plays the role of the root CA or designate an entity to play that role. In non-government-based solutions, which have the potential to proliferate much faster in the SSI model in the short-term, different entities can become trusted as CAs by another through private agreements and social recognition.

As addressed in Section 7.6, there are at least two essential trusted lists. One of these trusted list is a list of CAs designated by a trusted authority. Another trusted list is a list of certificates that each CA has issued to other entities and each of their statuses. This allows for the creation of roots of trusts to verify whether a digital certificate issued by an entity that we do not know or trust is certified by an entity that we do know and trust.

Trust frameworks also allow us to define different certificates' levels of assurance, depending on who issued them and how they were issued. One of the most reputable frameworks for levels of digital identity assurance comes from the International Organization for Standardization (ISO), presented in Image 18 (ISO, 2013).

In Europe, one of the most reputable frameworks for levels of assurance is STORK[61] (Secure Identity Across Borders Linked), a project within the ICT Policy Support Programme under the Competitiveness and Innovation Framework Programme (CIP). STORK's levels of assurances are defined in the Authentication Quality Assurance (QAA) framework. Image 19 shows the level of assurance required depending on the likelihood of the risks and impact of damages.

In the short-term, we expect a combination of traditional off-chain trusted lists, X.509 certificates, and levels of assurance with new blockchain networks, decentralized identifiers, and verifiable credentials. In the mid-term, we foresee a migration from centralized trusted lists to decentralized and smart contracts in public blockchain networks, a replacement of X.509 with verifiable credentials, and adaptations of the levels of assurance, given the slight variations introduced by these new elements.

61 https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu

Image 18. Levels of assurance of ISO/IEC DIS 29115.

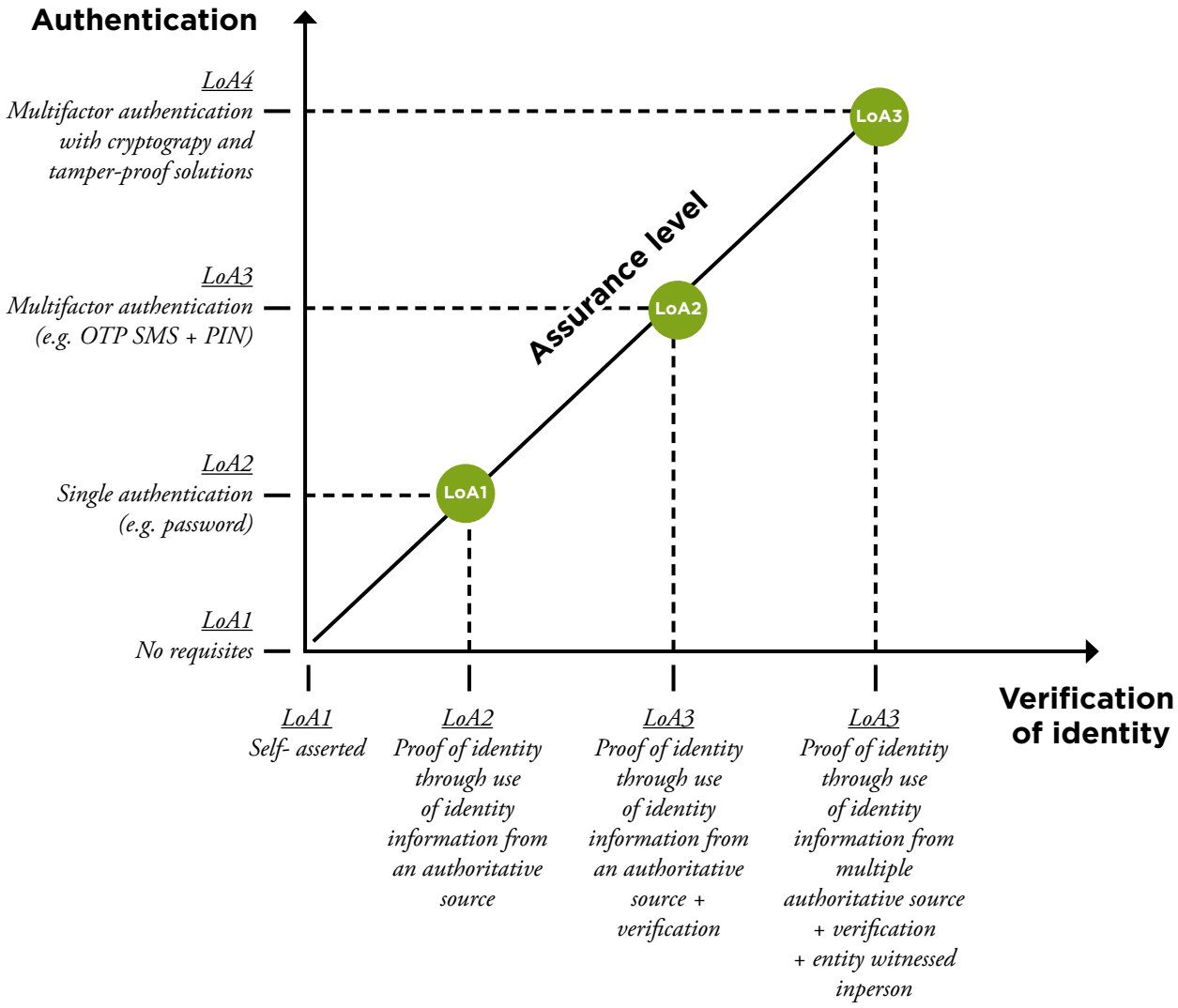


Image 19. Impact of damages defined by STORK (Alamillo, 2020).

		Impact of damages				
	Likelihood	Very High	High	Medium	Low	Negligible
Risk	Almost certain	(1)	(1)	Level 4	Level 3	Level 3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1

(1): Not applicable to remote authentication over open networks

8.3. Leading Initiatives

There are some relevant initiatives working to create trust frameworks for the operation of digital identity that are specifically applicable to self-sovereign identity. Three of the most reputable at this time are the Open Identity Exchange (OIX), eIDAS, and Sovrin.

8.3.1. The Open Identity Exchange (OIX)

OIX is a non-profit, technology agnostic, collaborative cross sector membership organization that aims to accelerate the adoption of digital identity services based on open standards. It is one of the international references in trust frameworks for digital identity. According to OIX (OIX, 2017), for a trust framework to become a set of system rules that enable trust between participants, it must have:

- **Authorship and control:** the authors of the content and the governing body.
- **Content:** roles, functions, and technical, operational, and legal matters.
- **Enforceability:** legally binding, usually through contracts between stakeholders but also through regulation.
- **Form:** in general, a set of documents.
- **Purpose:** the governance of that system.
- **Scope:** the system it governs.

Additionally, they highlight that the goal of a trust framework is to establish:

- **Functionality:** by guaranteeing proper operation and compliance with any applicable law.
- **Trustworthiness:** by addressing and managing risks, legal rights, responsibilities, and liabilities; eliminating uncertainties; and facilitating the accessibility and understanding of the trust frameworks to all participants.

OIX identifies five participating functions that a trust framework typically focuses on, which are completely aligned with the technical requirements presented in this paper. These include 1) identity issuing, 2) identity verification, 3) authentication management, 4) authorization management, and 5) attributes, claims or assertion management. These functions have been addressed and explored in detail in Block 7 of this paper and are presented in Table 14.

OIX also outlines five types of trust frameworks according to the types of entities writing and controlling that trust framework. These are presented in Table 15.

This classification is independent from and compatible with the layers of independent governance proposed in Section 8.1.

8.3.2. The European Trust Framework for Digital Identity: eIDAS

In order for governments to continue playing a central role in the area of digital identity in the upcoming SSI era, they must:

- Define governing bodies at a national level.
- Certify and maintain trusted lists.
- Establish standard and secure ways of communicating information such as certificate authorities, identity issuers, and certificate revocation lists.
- Require acceptance of credentials between different parties when the credentials have been issued meeting assurance requirements.

A clear example of this is eIDAS (EU-eIDAS, 2014). This European regulation, explored in Section 6.1.2, not only provides a regional base for the standardization of electronic services and the recognition between all the European Member States, but also meets the four previous requirements (or at least aims to do so). As stated in Article 17, "each country is responsible for designating a supervisory body to supervise, report to the Commission, and take actions if necessary." Also, every Member State operates an eIDAS node which is a standardized software to communicate with the others. Last but not least, as stated in Article 6, "when an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognized in

Table 14. Comparison between OIX participating functions and LACChain ID technical components.

OIX	LACChain ID
Identity issuing	Decentralized identifiers (Section 7.1) Verifiable credentials (Section 7.2)
Identity verification	Verifiable presentations (Section 7.3) Identification (Section 7.4.1)
Authentication management	Authentication (Section 7.4.2)
Authorization management	Authorization (Section 7.4.3) Digital repositories and wallets (Section 7.5)
Attribute, claims or assertion management	Decentralized identifiers (Section 7.1) Verifiable presentations (Section 7.3) Digital repositories and wallets (Section 7.5)

Table 15. The five types of trust frameworks according to the types of entities writing and controlling those trust frameworks, according to OIX. (OIX, 2017)

Type	Definition	Example
Independent governing entity	An entity designated to develop, maintain, and enforce the trust framework; useful for large-scale identity solutions with several identity issuers and service providers	SAFE-BioPharma identity system managed by SAFE-BioPharma Association[62]
Consortium of participating entities	A group of some or all participating entities; useful for small identity solutions	CA/Browser Forum[63]
Single participant governing entity	A central entity is responsible for the trust framework; common when there is a single identity issuer or service provider, that also becomes the central entity	Identity issuer: Google, Facebook Service provider: Governments (U.S. government's Login.gov; UK's government GOV.UK Verify program)
Non-governing standards or certification organization	An independent entity established to develop and update the trust framework; may also certify identity issuers	Kantara initiative[64] tScheme Approval profiles issued by tCheme[65]
Mutual agreement among participants	Mutual agreements between entities in smaller scale identity solutions; usually though MRA	Proyecto Cadena between the Customs of Chile, Colombia, Costa Rica, Mexico, and Peru

62 https://www.safe-biopharma.org

63 CA/Browser Forum, https://cabforum.org/. This trust framework governs the issuance of EV-SSL server certificates.

64 Kantara Initiative, https://kantarainitiative.org

65 tScheme, www.tscheme.org

the first Member State for the purposes of cross-border authentication for that service online." This holds provided that a minimum set of conditions are met. Therefore, it can be inferred that "the legal effect of cross-border recognition of electronic identification is guaranteed only in relations between individuals and public sector bodies" (Alamillo, 2020), which excludes the private sector.

The introduction of new technological elements also provides new tools for the exchange of information between the Member States. In this sense, there are at least a couple factors that could be reviewed leveraging blockchain networks in SSI implementations.

Communication: in eIDAS, Member States from the UE are responsible for the development of national frameworks. Communication between nodes is currently accomplished through eIDAS nodes (not blockchain nodes but centralized software). These nodes have been proved to be vulnerable, as identified by SEC in October 2019. Decentralized ledgers can be used for safer communication, as each country can run a known blockchain node and known blockchain accounts that can be used to communicate public and private information about trust providers and certificated entities. Additionally, being already part of the ledger that will be leveraged as the registry for SSI makes processes more efficient and secure.[66]

Trusted lists: related to the previous point, blockchain networks can be a suitable registry for trusted lists and certificate revocation lists. Currently, trusted lists are maintained in centralized and independent registries by countries. It would also make them more efficient and secure.

8.3.3. Sovrin

One of the most relevant and recognized governance models for SSI identity is the Sovrin Governance Framework. It "serves as the constitution for the Sovrin Network as well as a foundation for more specialized Domain-Specific Governance Frameworks (DSGFs)" (SOVRIN, 2019). The Sovrin Network is a public-permissioned network that incorporates SSI at the infrastructure level, enabling a decentralized way of exchanging and verifying credentials. Their governance model includes five legal agreements:

- The Sovrin Steward Agreement: the agreement between the Sovrin Foundation and all stewards who operate nodes of the Sovrin ledger.
- The Transaction Author Agreement: the agreement between the Sovrin Foundation and all identity owners writing transactions to the Sovrin ledger networks.
- The Transaction Endorser Agreement: the agreement between the Sovrin Foundation and organizations using permissioned write access.
- The Steward Data Processing Agreement (DPA): the agreement under which stewards serve as data processors from a data protection regulatory standpoint.
- The Transaction Endorser Data Processing Agreement: the DPA that applies to transaction endorsers.

Sovrin's trust framework is designed specifically for their blockchain network, although it could be adapted for other networks. Sovrin has also developed a governance framework composed of several documents that complement the trust framework.[67]

66 https://sec-consult.com/en/blog/2019/10/vulnerability-in-eu-cross-border-authentication-software-eidas-node/

67 https://sovrin.org/library/sovrin-governance-framework/

SELF-SOVEREIGN IDENTITY

Conclusions

Self-sovereign identity introduces a revolutionary and innovative solution for the management of individual digital identities. This model has the potential to solve the problems and inconveniences presented by the current identity management systems in terms of regulation, technology, and security. In doing so, this model combines two innovative technologies: digital wallets and decentralized ledgers. Digital wallets will allow individuals to manage all their digital assets with total independence, sovereignty, and privacy. We will be able to have fast and safe access to digital versions of identity documents, academic diplomas, and property tiles, among other valuable identifying information. We will also be able to manage tokenized fiat currencies such as the dollar, euro, libra, pesos, yuan, and even cryptocurrencies. Decentralized ledgers, such as blockchain networks, allow for storage of cryptographic proofs of the existence and ownership of digital credentials and assets, increasing the trust, interoperability, security and efficiency of electronic transactions while preserving data privacy.

The self-sovereign identity model will require evolution and adaptation of governments and financial entities in order to issue these assets in a digital format that is compatible with the self-sovereign identity standards. These efforts are presently under way. In regard to the adoption of digital verifiable credentials and certificates, the European Union stands out, with initiatives such us the eIDAS Bridge and the EBSI ESSIF for the development of techno-legal frameworks suitable for self-sovereign identity between the country members. These initiatives have already piloted the issuance of digital identity credentials, digital driver licenses, and digital diplomas of which cryptographic proofs are stored in a blockchain network. With respect to digital currencies, several central banks have already started to pilot the issuance of digital currencies using blockchain technology. Some of the most renowned projects thus far are Jasper (Canada), Ubin (Singapur), Khokha (South Africa), RTGS RP (England), Stella (Japan and Europe), LBChain (Lithuania), the Central Bank of Brazil (Brazil), Inthanon (Thailand), and E-Krona (Sweeden).

Some of the benefits of the self-sovereign identity model include the facility to enable interoperability between different solutions, the ownership of the digital assets by the individuals, the full control over the consent, the portability of data, the protection of data by design, pseudonymity, traceability, the right to be forgotten, scalability, security, and usability. Additionally, this identity scheme enables and contributes to a long list of use cases with social and financial impact, such as easier access to first identity, better targeted and tracked conditional cash transfers, reduction of data breaches, increase of data privacy, issuance of digital verifiable diplomas, financial inclusion of unbanked, easier digitalization of government services, reduction of hacks of health information, portability of documents for migrants and refugees, recovery of documents after natural disasters, safe notarization of domestic violence, and cheaper and faster remittances, among others.

We are still in the early days of implementing self-sovereign identity globally, but the current developments have been promising and exciting. As we have discussed throughout this paper, it is necessary to work on three different areas moving forward: regulation, technology, and trust frameworks. Further progress in these three areas will enable the development of complete SSI solutions, both public-based and private-based, in the upcoming years, along with the consolidation of new standards and protocols. We will face several challenges in this process of development, including 1) the adaptation of current infrastructure and data models, 2) lawyers, notaries, and jurists understanding the technology, 3) maturing digital wallets, 4) development of campaigns to attract users, 5) safe back-ups, 6) guarantee of the right to be forgotten, 7) the establishment of trust frameworks, 8) engagement of governments, 9) modification of regulations, 10) guarantee of data protection, 11) enabling of zero-knowledge proofs, 12) easy key recovery, 13) maturing decentralized registries, 14) guarantee of the right to pseudonymity, and 15) use of biometrics for identification and authentication. Although governments will keep having sovereignty over the identification of citizens, we expect that

private-based trust frameworks around SSI will also emerge, and entities such as financial institutions, insurance firms, health entities, and universities, among others, will be issuing digital verifiable credentials to their clients and customers.

In regard to regulations, it is necessary to work on the areas of electronic transactions and signatures as well as data privacy and protection in order to develop and update regulatory policies in countries that lack them. In Latin America and the Caribbean, 31 out of 42 countries (74%) have regulations on electronic signature. However, only 17 out of 42 countries (40%) have regulation on data protection.

With respect to technology, we have presented seven complementary elements that we consider essential: decentralized identifiers; verifiable credentials; verifiable presentations; digital wallets; identification, authentication, and authorization; certificate authorities and trusted lists; and decentralized ledgers. Each of these elements will have to be analyzed and taken into consideration when developing complete SSI solutions, looking at the international standards and protocols to guarantee scalability and interoperability. Finally, regarding trust frameworks, it will be key to define governance and economic models for the operation of networks and the SSI solutions built on top of them, and to establish certification authorities, identity providers, levels of assurance, and communication channels.

As stated by the ISO, ITU, NIST, and the European Union, among others, in the next few years, we will see an intense and rapid growth in activity surrounding self-sovereign identity. It is possible that in a short period of time, we will be managing all of our digital assets with a mobile wallet and using blockchain to guarantee its veracity. As with any important and disruptive technological innovation, there is a large and timely opportunity for governments and private sector companies to take their first steps forward.

References

[Alamillo, 2019] Alamillo, N. (2019). *Identificación, firma y otras pruebas electrónicas: la regulación jurídico-administrativa de la acreditación de las transacciones electrónicas.* Cizur Menor, Navarra: Aranzadi. Retrieved from https://almena.uva.es/discovery/fulldisplay/alma991008080150205774/34BUC_UVA:VU1.

[Alamillo, 2020] Alamillo, N. (2020). *SSI eIDAS Legal Report.* European Comission. Retrieved from https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

[CAF, 2012] Corporacion Andina de Fomento. (2012). *Fundamentos de la firma digital y su estadodel arte en América Latina y el Caribe.* Retrieved from http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/503ADEE40C4F859505257D1C00708FE4/$FILE/Di-7-12_Fundamentos_Firma_Digital_y_su_Estado_Arte_en_ALC-Final.pdf

[California, 2018] California State Legislature. (2018). *Bill AB/375 - California Consumer Privacy Act*. Retrieved from https://oag.ca.gov/privacy/ccpa

[Consensys et al., 2019] Consensys et al. (2019). Retrieved from https://drive.google.com/file/d/1gQrI02QjEiYHh6V-iFHbXxPKA6HWHgfMt/view

[EU, 2018] The European Union Blockchain Observatory and Forum. (2018). *Blockchain for government and public services.* Retrieved from https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf

[EU, 2019] European Union. (2019). *EIDAS supported self-sovereing identity*. Retrieved from https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

[EU-BDID, 2019] The European Union Blockchain Observatory and Forum. (2019). *Blockchain and digital identity.* Retrieved from https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

[EU-GDPR, 2016] European Union. (2016). *Regulation No 2016/679 on general data protection. Directive 95/46/EC*. Retrieved from https://gdpr-info.eu/

[EU-eIDAS, 2014] European Union. (2014). *Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. Retrieved from https://www.eid.as/Regulation

[ETSI, 2015] European Telecommunications Standards Institute. *Quantum safe cryptography and security (White Paper No. 8. ISBN No. 979-10-92620-03-0). (2015)*. Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[EWF, 2018] Energy Web Foundation. (2018). *The energy web chai*n. Retrieved from https://energyweb.org/wp-content/uploads/2019/05/EWF-Paper-TheEnergyWebChain-v1-201810-FINAL-1.pdf

[FATF, 2020] Financial Action Task Force. (2020). *Guidance on Digital ID.* Retrieve from https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

[FOMIN-I, 2014] Fondo Multilateral de Inversiones. (2014). *Las remesas a América Latina y el Caribe en 2013: aún sin alcanzar niveles de pre-crisis*. Retrieved from https://www.findevgateway.org/es/paper/2014/06/las-remesas-america-latina-y-el-caribe-en-2013-aun-sin-alcanzar-niveles-de-pre-crisis

[FOMIN-II, 2014] Fondo Multilateral de Inversiones. (2014). *Situación económica y envío de remesas.* Retrieved from https://www.microfinancegateway.org/sites/default/files/mfg-es-documento-situacion-economica-y-envio-de-remesas-de-migrantes-de-america-latina-y-el-caribe-en-el-periodo-post-recesion-4-2014.pdf

[FDIC, 2017] Federal Deposite Insurace Corporation. (2017). *FDIC National survey of unbanked and underbanked households*. Retrieved from https://www.fdic.gov/householdsurvey/

[FEMA, 2019] Federal Emergency Management Agency. (2019). *National Advisory Council DRAFT Report to the FEMA Administrator November 2019*. Retrieve from https://www.fema.gov/media-library-data/1572880188002-31454e3c26dff6922fde9d34cbe19e26/November_2019_NAC_Report_Draft_v5.pdf

[ForgeRock, 2019] ForgeRock. US Consumer Data Breach Report. (2019). *Personally Identifiable Information Targeted in Breaches that Impact Billions of Records.* Retrieved from https://www.forgerock.com/resources/view/92170441/industry-brief/us-consumer-data-breach-report.pdf.

[Garner, 2000] Gartner. (2020). *Guidance for decentralized identity and verifiable claims.* Retrieved from https://www.

gartner.com/en/documents/3979940/guidance-for-decentralized-identity-and-verifiable-claim

[IDB, 2013] Brito, S., Corbacho, A., Osorio, R., & Harbitz, E. Inter-American Development Bank. (2013). *El registro de nacimientos: La llave para la inclusión social en América Latina y el Caribe*. Retrieved from https://publications.iadb.org/publications/spanish/document/El-registro-de-nacimientos-La-llave-para-la-inclusi%C3%B3n-social-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

[IDB, 2015] Inter-American Development Bank. (2015). *Inclusión financiera en América Latina y el Caribe.* Retrieved from https://publications.iadb.org/es/publicacion/13894/inclusion-financiera-en-america-latina-y-el-caribe-coyuntura-actual-y-desafios

[IDB, 2016] Inter-American Development Bank. (2016). *Programas de transferencias monetarias condicionadas e incusión financiera.* Retrieved from https://publications.iadb.org/publications/spanish/document/Programas-de-transferencias-monetarias-condicionadas-e-inclusi%C3%B3n-financiera.pdf

[IDB, 2017] Inter-American Development Bank. (2017). *Así funcionan las transferencias condicionadas*. Retrieved from https://publications.iadb.org/es/publicacion/17226/asi-funcionan-las-transferencias-condicionadas

[IDB-REM, 2017] Inter-American Development Bank. (2017). *Un mayor dinamismo en 2017 del envío de remesas.* Retrieved from https://publications.iadb.org/publications/spanish/document Un-mayor-dinamismo-en-2017-del-ingreso-por-remesas-de-Am%C3%A9rica-Latina-y-el-Caribe.pdf

[IETF, 2012] Internet Engineering Task Force. (2012). *The OAuth 2.0 Authorization Framework.* https://tools.ietf.org/html/rfc6749

[ISO, 2013] International Organization for Standardization. (2018). *Information technology - Security techniques - Entity authentication assurance framework (ISO/IEC 29115:2013).* Retrieved from https://www.iso.org/standard/45138.html

[ISO, 2018] International Organization for Standardization. (2018). *Governance of blockchain and distributed ledger technology systems (ISO/TC 307/SG/ 6)*. Retrieved from https://www.iso.org/committee/6266604.html

[ISO, 2019] International Organization for Standardization. (2019). *IT Security and Privacy — A framework for identity management - Part 1: Terminology and concepts*. (ISO/IEC Standard No. 24760-1) Retrieved from https://www.iso.org/standard/77582.html

[ISO, 2020] International Organization for Standardization. (2020). *Guidelines for governance (ISO TS WD5 23635)*. Retrieved from https://www.iso.org/standard/76480.html

[ITU, 2018] International Telecommunications Union. (2018). *Digital identity roadmap guide.* Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). ISBN: 978-92-61-27821

[ITU, 2019] International Telecommunications Union. (2019). *Distributed ledger technology reference architecture.* Retrieved from https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

[Josan & Pope, 2005] Josang, A., & Pope, S. (2005). *User Centric Identity Management.* Retrieved from http://folk.uio.no/josang/papers/JP2005-AusCERT.pdf

[Lum et al., 1988] Lum, M., Feldman, P., & Micali, S. (1988). Non-Interactive Zero-Knowledge and Its Applications. *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. pp. 103–112. doi:10.1145/62212.62222. ISBN 978-0897912648.

[McKenzie, 2018] McKenzie. (2018). *Global Privacy and Information Management Handbook*. Retrieved from https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/global_privacy_handbook-_2018.pdf?la=en

[NIST-DSS, 2019] National Institute of Standards and Technology. (2019). *Digital Signature Standard (DSS)*. (Natl. Inst. Stand. Technol. Spec. Publ. 186-5 (Draft)). Retrieve from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5-draft.pdf

[NIST-ECDM, 2019] National Institute of Standards and Technology. (2019). *Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters*. (Natl. Inst. Stand. Technol. Spec. Publ. 800-186 (Draft)). Retrieve from https://csrc.nist.gov/publications/detail/sp/800-186/draft

[NIST-IDG, 2017] National Institute of Standards and Technology. (2017). *Digital identity guidelines*. (Natl. Inst. Stand. Technol. Spec. Publ. 800-63-3). DOI: https://doi.org/10.6028/NIST.SP.800-63-3

[NIST-IDGa, 2017] National Institute of Standards and Technology. (2017). *Digital identity guidelines.* (Natl. Inst. Stand. Technol. Spec. Publ. 800-63-3a). DOI: https://doi.org/10.6028/NIST.SP.800-63-3

[NIST-Q, 2016] National Institute of Standards and Technology. (2016). *Report on post-quantum cryptography*

(Internal Report NISTIR 8105). Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[NIST-TA, 2020] National Institute for Standards in Technology. (2020). *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*. Retrieved from https://csrc.nist.gov/publications/detail/white-paper/2020/01/14/a-taxonomic-approach-to-understanding-emerging-blockchain-idms/final

[NSA, 2016] National Security Agency. (2016). *CNSA suite and quantum computing FAQ (MFQ-U-OO-815099-15).* Retrieved from https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm

[OASIS, 2008] OASIS. (2008). *Security Assertion Markup Language (SAML).* http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

[OIX, 2014] Open Identity Exchange. (2014). *The Vocabulary of Identity Systems Liability.* Retrieved from https://openidentityexchange.org/blog/2014/06/08/the-vocabulary-of-identity-systems-liability/

[OIX, 2017] Open Identity Exchange. (2017). *Trust frameworks for identity systems.* Retrieved from https://openidentityexchange.org/blog/2017/06/22/trust-frameworks-for-identity-systems/

[OIX-TF, 2010] Open Identity Exchange. (2010). *The open identity trust framework model*. Retrieved from https://www.openidentityexchange.org/wp-content/uploads/2017/03/open_identity_trust_framework_model_2010.pdf

[OIX-TOOLS, 2019] Open Identity Exchange. (2019). *Aligning the Rules and Tools of Digital Identity: Solving Today's Burning Business Problems*. Retrieved from https://openidentityexchange.org/blog/2019/11/12/aligning-the-rules-and-tools-of-digital-identity-solving-todays-burning-business-problems/

[OIX-UK, 2019] Open Identity Exchange. (2019). *Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK*. Retrieved from https://openidentityexchange.org/blog/2019/10/04/establishing-a-trusted-interoperable-digital-identity-ecosystem-in-the-uk/

[SDG, 2016] Inter-Agency and Expert Group on SDG Indicators. (2016). *Final list of proposed Sustainable Development Goal indicators.* Retrieved from https://sustainabledevelopment.un.org/content/documents/11803Official-List-of-Proposed-SDG-Indicators.pdf

[SOVRIN, 2019] Sovrin Governance Framework. (2019). *Sovrin Trust Assurance Framework*. Retrieved from https://sovrin.org/wp-content/uploads/Sovrin-Trust-Assurance-Framework-V1.pdf

[UN, 1498] United Nations. (1948). *Universal declaration of human rights.* Retrieve from https://www.un.org/en/universal-declaration-human-rights/.

[W3C-DID, 2019] World Wide Web Consortium. (2019). *Verifiable Credentials Data Model 1.0.* Retrieved from https://www.w3.org/TR/vc-data-model/

[W3C-JSONLD, 2019] World Wide Web Consortium. (2019). *A JSON-based serialization for linked data.* Retrieved from https://json-ld.org/spec/latest/json-ld/

[W3C-VC, 2019] World Wide Web Consortium. (2019). *Decentralized Identifiers (DIDs).* Retrieved from https://www.w3.org/TR/did-core/

[WB-ID4D, 2018] World Bank. (2018). *ID4D Global Dataset.* Retrieved from https://id4d.worldbank.org/global-dataset

[WB-TS, 2018] World Bank. (2018). *Technical standards for digital identification systems*. Retrieved from http://documents.worldbank.org/curated/en/707151536126464867/pdf/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf

[Wu & Hang, 2014] Wu, H. & Wang, F. (2014). *A Survey of Noninteractive Zero Knowledge Proof System and Its Applications.* The Scientific World Journal, 560484.

Electronic Signature Regulations

Antigua and Barbuda - http://legalaffairs.gov.ag/pdf/bills/Electronic_Transactions_Amendment_Act_2016.pdf

Argentina - https://www.argentina.gob.ar/firmadigital/normativa#:~:text=Ley%20N%C2%B0%2025.506%20de,Digital%20de%20la%20Rep%C3%BAblica%20Argentina.

Bahamas - http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0004/ElectronicCommunicationsandTransactionsAct_1.pdf

Barbados - https://www.barbadosparliament.com/uploads/bill_resolution/abebbcf80e26815632d4b130d9906644.pdf

Belize - https://www.global-regulation.com/law/belize/3268571/electronics-transaction-act.html

Bolivia - https://www.att.gob.bo/content/bolivia-ingresa-la-era-de-la-firma-digital#:~:text=BOLIVIA%20INGRESA%20A%20LA%20ERA%20DE%20LA%20FIRMA%20DIGITAL%20La,Telecomunicaciones%20y%20Transportes%2DATT%2C%20se

Brazil - http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

Cayman Islands - https://www.ofreg.ky/upimages/commonfiles/1506773099ElectronicsTransactionLaw2003Revision.pdf

Chile - http://www.oas.org/juridico/pdfs/mesicic4_chl_ley19799.pdf

Colombia - https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

Costa Rica - http://www.firmadigital.go.cr/Documentos/ley%208454.pdf

Dominican Republic - https://www.wipo.int/edocs/lexdocs/laws/es/do/do030es.pdf

Ecuador - https://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf, https://www.firmadigital.gob.ec/wp-content/uploads/2018/01/reglamento_ley_de_comercio_electronico.pdf

El Salvador - https://www.asamblea.gob.sv/decretos/details/166

Granada - https://www.yumpu.com/en/document/view/26268942/electronic-transactions-act-2008-government-of-grenada

Guatemala - https://www.minfin.gob.gt/images/archivos/leyes/tesoreria/Decretos/DECRETO%2047-2008.pdf

Haití - https://www.haitilibre.com/en/news-19982-haiti-politics-the-law-on-electronic-signature-finally-voted-in-the-senate.html

Jamaica - https://moj.gov.jm/sites/default/files/laws/Electronic%20Transactions%20pgs.%201-34.pdf

Mexico - https://eservicios.impi.gob.mx/seimpi/ayudaSEIMPI/LFEA.pdf

Nicaragua - http://legislacion.asamblea.gob.ni/Normaweb.nsf/9e314815a08d4a6206257265005d21f9/1ceea41dc1bdc53d06257951005bbc04?OpenDocument

Panama - https://www.firmaelectronica.gob.pa/documentos/Ley_82-Que_modifica_la_Ley_51_de_2008.pdf

Paraguay - https://www.bacn.gov.py/archivos/3550/20150709092101.pdf

Peru - https://www.minjus.gob.pe/wp-content/uploads/2014/03/Ley27269.pdf

Puerto Rico - http://www.bvirtual.ogp.pr.gov/ogp/Bvirtual/leyesreferencia/PDF/Tecnolog%C3%ADas/148-2006/148-2006.pdf

Saint Christopher and Nevis - https://skncustoms.com/pdfs/GoSKN-ElectronicTransactionsAct2011.pdf

Saint Lucía - https://www.investstlucia.com/files/downloads/date_201102161647/Electronic%20transactions%20ACT.pdf

Suriname - https://www.loc.gov/law/foreign-news/jurisdiction/suriname/

Trinidad and Tobago - http://www.ttparliament.org/legislations/a2011-06.pdf

Uruguay - https://legislativo.parlamento.gub.uy/temporales/leytemp1979099.htm

Venezuela - http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-sobre-Mensajes-de-Datos-y-Firmas-Electr%C3%B3nicas.pdf

Data Protection Regulations

Antigua y Barbuda - http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/102704/124275/F-167635569/ATG102704.pdf

Argentina - http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf

Aruba - https://www.doingbusinessdutchcaribbean.com/aruba/intellectual-property/data-protection-privacy/#:~:text=There%20are%20no%20specific%20laws,data%20in%20general%20in%20Aruba.&text=Any%20such%20personal%20information%20may,concerned%20collection%20of%20personal%20data.

Bahamas - http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf

Barbados - https://www.barbadosparliament.com/bills/details/396

Belize - https://www.right2info.org/laws/BelizeFreedomofInformationAct20002.pdf

Brazil - https://www.lgpdbrasil.com.br/wp-content/uploads/2019/06/LGPD-english-version.pdf

Chile - https://dfsobservatory.com/sites/default/files/LEY-20575_17-FEB-2012.pdf

Colombia - http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Costa Rica - http://www.oas.org/es/sla/ddi/docs/CR4%20Ley%20de%20Protecci%C3%B3n%20de%20la%20Persona%20frente%20al%20Tratamiento%20de%20sus%20Datos%20Personales.pdf

Dominican Republic - http://dominicanlaw.com/dominican-data-protection-law/

Ecuador - https://corporate.dataguidance.com/ecuador-bill-addresses-lack-of-data-protection-culture/#:~:text=The%20National%20Assembly%20announced%2C%20on,('the%20Bill').&text=Specifically%2C%20the%20Bill%20requires%20organisations,before%20collecting%20and%20using%20data.

Jamaica - https://www.japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202017----.pdf

Mexico - http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Nicaragua - http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/7bf684022fc4a2b406257ab70059d10f?OpenDocument

Panama - https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf

Paraguay - https://www.pj.gov.py/ebook/monografias/nacional/informatico/Adriana-Marecos-Proteccion-de-datos-Py.pdf

Peru - http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Uruguay - https://www.impo.com.uy/bases/leyes/18331-2008



IDB IDB | LAB LACCHAIN