Quark ID Whitepaper

Self-Sovereign Identity: Basis of a New Decentralized Digital Ecosystem

Buenos Aires, Argentina

V. 0.1
10/3/2022

Quark Whitepaper

Self-Sovereign Identity: Basis of a New Decentralized Digital Ecosystem

1. Summary

It is pretty frequent to listen, in the digital world, that owning data grants power to those who control them. Identity information, particularly, is maybe the most transcendental data registry related to an individual or organization ever to exist. However, nowadays the access and usage of said records is beyond the control of the individuals these identify. Power and control are on the hands of entities that store the information, not on those these data refer to. The true identity holder is then relegated, not knowing where their data is, who has access to it or what is it used for. This is the reason why the GCBA (Gobierno de la Ciudad de Buenos Aires, Government of the City of Buenos Aires) invited the community to co-create a new protocol of digital, self-sovereign identity focused on the user being in charge of their own data.

The goal is building an ecosystem of digital interactions over the basis of the digital, self-sovereign identity protocol the community agreed on. We seek to ease the usage of the protocol to a critical mass of users, so that the ecosystem can become alive in a decentralized manner. We imagine a new paradigm that allows quick transactions, simplifying bureaucratic processes whether they be private or public parties. Doing so will empower individuals, give them control over their data and who has access to it. The expected benefits include a higher sovereignty for the people over their data, a return in the time spent nowadays on paperwork and bureaucracy to the people, and a reduction on the transactional costs to the organizations.

2. Introduction

The upcoming sections will describe the motivation and the goal of the project. By using plain language (non-technical) we will aim to obtain the largest possible audience, providing a clear outlook of the direction and reach of it.

2.1. Why? The motivation

Note: this section will explain, in motivational terms, the drive of the project, by focusing in answering why this initiative is necessary, why it should be oriented to the realm of the digital identities, why this is the right time and why it should be driven by the GCBA.

- Motivation: instating a new paradigm in which secure transactions are agile; where the required documentation verification can be done in a timely, reliable and private manner. This paradigm is based on the principle that people should be controlling their identity, and it is them who decide where their information is stored and who can access it.

- Nowadays, identity information is managed according to the centralized data paradigm. Registries and documents are managed by large organization, both governmental and private, and these organizations own the rights to issue, read, modify or delete information. People have no control over their own identity nor can they choose who has access to their data, relying entirely on a third-party that can, as everybody else, miss. The current situation leads to individuals even accepting terms and conditions without knowing their details or better options. The excessive dependency on a few centralized entities, together with the widely known importance and power of data in the 21st Century make the current paradigm both outdated and dangerous.

- In any interaction between parties, knowing and verifying the identities of the parties is a condition required for building trusty bonds. This bond is a fundamental aspect of social, commercial and Public-Private relationships. The first step in every interaction is always verifying the identity of the parties involved. Either to register a new company, opening a bank account, signing up for a club or a service. The least trust the parties have, more dangerous and less desirable the interaction will be.

- These transactions can also require the presentation of additional documents, a process that tends to be inefficient and currently takes a lot of the people’s time. What if we could change this reality? Today we have the technology to do it. We propose to change the current document presentation process for another where the individuals only authorize an interested party to verify automatically how conditions are fulfilled by means of a secure channel. This change would lead to a huge time reduction in transactions, as well as it would increase its reliability and security. In a hyper-connected world where digital takes more and more space in our lives, it is crucial that reliable, secure, open and agile methods are developed to digitally interact with our surroundings without taking risks.

- The existence of a people-governed digital identity and backed-up by a Government will allow new use cases and, among others, increase the reliability and sustainability in time. Larger benefits will take place when the ecosystem expands by the creation of digital identities of private organizations, gain volume due to the increase in the interaction between private parties and nourishes from the creation of new apps to channel transactions between private parties. This protocol opens infinite doors to third-parties to develop new technologies based on identities, now in a secure, agile and open manner.

- Even though there are several attempts of implementing digital, self-sovereign identity systems, the intrinsically community component of this concept implies the need of a critical mass of users for its real and effective functioning. This is why a Government, given its institutional faculties, is probably the best organization to kickstart this new paradigm, achieving a massive adoption by officially implementing the system. Once this is achieved, society as a whole will benefit from it, as it will be considerably simpler to build new protocols over or parallel to this one.

- For the first time in the history of mankind it is possible to create reliable frameworks by using purely technological means thanks to the breakthroughs in the field of cryptography, that provide technologies like blockchain and zero-knowledge proofs, which allow us to evolve into a paradigm where individuals and society are the social grantors; and not a few centralized organizations.

- There is a community of Argentine entrepreneurs and developers that is worldwide renowned for being at the forefront of the development of these new technologies that, were it complemented by an institutional framework and a coordinated action plan with the Government, it would increase wealth, generate highly rated jobs and a leadership positioning for our Country in a strategic topic worldwide.

2.2. What for? The purpose/The expected benefits

Note: this section will explain which is the purpose of the project, focusing on explaining its impact and the benefit that it can bring.

- Empowering individuals and evolving into a paradigm where individuals and the society are the social grantors; instead of a few centralized organizations. An open, reliable, secure and transparent ecosystem built over a decentralized architecture, where the reliability is backed-up by the network and not by centralized organizations.

- Building relationships between individuals and organizations (both Public and Private) based on trust, with a technology safeguard backed-up by the same users. By doing so we replace a paradigm governed by frontiers and control structures by one smooth and decentralized.

- Speeding up the transactional times by simplifying the identity verification and requirement fulfillment processes, giving back time to people and reducing costs for the companies. Eliminating the necessity of presenting documentation, replacing it by a simple authorization to an interested party to automatically verify the ownership of a credential that corroborates the fulfillment of a condition or access to a data.

- Creating new ways of doing business, sharing information and granting access to governmental services and resources. Those that so desire can develop and build over the provided bases of this protocol, opening countless doors to new projects and methods that involve identity as a key factor.

2.3. How? The proposed focus

Note: this section will explain how this project will be developed and executed. It will not be centered on specific tools to be used, but on methods, protocols and standards to be implemented.

- A co-creation focus open to everyone who wants to collaborate.

- Following the paradigms of Self-Sovereign Identity.

- Taking advantage of the possibilities created by breakthroughs in the field of cryptography (e.g. blockchain, ZKP, etc.).

- Taking advantage of the capacities of the entrepreneurs and developers ecosystem in Argentina, both in the field of self-sovereign identity as well as in the field of technologies involved in public, decentralized and non-permissioned networks.

- Taking advantage of the GCBA capacity to drive forward the mass adoption and quickly obtaining a critical mass of users.

2.4. What? What we propose to do

Note: this section will focus in describing the object, the elements that shall be built or developed as part of this initiative.

It must clarify that the goal is not to develop digital identities to be exclusively used in the City of Buenos Aires nor for any other specific context, but to set the grounds of a protocol that can be user or copied by whoever, whenever.

The document will not emphasize the tech stacks to be used, but outline a solution independent, as much as possible, from the tools used for its implementation.

For starters, we have to identify the key elements required to achieve the goal of the initiative:

- A digital identity protocol that can make paperwork and any actions related to identities easier and more efficient, as well as creating new ways of sharing information and granting access to services provided by all kinds of institutions, both public and private. It should be decentralized, public, non-permissioned, open, expandable and able to interoperate with similar protocols.

- A critical mass of digital identities that serves to bootstrap the digital ecosystem and gives it enough relevance so as to allure new users, institutions and companies, achieving a dynamic that allows it to self-sustain and grow.

- A first App, sponsored by the GCBA, that allows access and interoperability among all services the government provides through common standards, so that users can see concrete benefits from an early stage.

- A thriving ecosystem that expands on the services originally provided by the government, to create new experiences and more benefits to the users and organizations that reside, transit or operate in the City of Buenos Aires, and could be then copied in other jurisdictions or environments locally, regionally or globally.

2.5. For whom? Audience

This document is aimed to serve as a framework for governmental agents, software providers, commercial agents, future issuers of private credentials, lawmakers, regulators and the general audience.

3. Pre-existing works

Note: this section will reference pre-existing works that were analyzed and will be used as material in any way while designing the proposed platform.

3.1. W3C & Decentralized Identity Foundation
3.2. Sovrin Foundation
3.3. Hyperledger Aries & Ursa & Indy
3.4. Trust Over IP (ToIP)
3.5. Ethereum community (ENS / EIPs)
3.6. Proof Of Humanity
3.7. State of Colorado
3.8. European Union
3.9. IDunion
3.10. LACChain ID

4. Concepts of the Self-Sovereign Identity

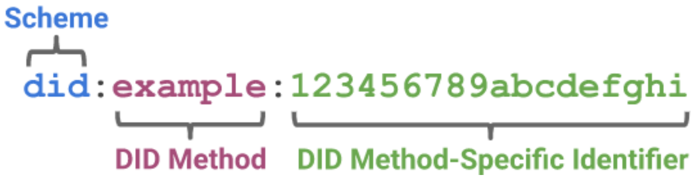
Note: this section will detail all definitions of key terms that will be used through the extent of this document.

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 intervening 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”[2]. In 2016, Christopher Allen established the 10 principles for Self-Sovereign Identity that have become a reference in the field (see Appendix I).

4.1. Terminology

Decentralized Identifier (DID)

A globally unique and persistent identifier that does not require a centralized registration authority because it is generated and/or registered using decentralized platforms (e.g. blockchain). While the generic format of a DID is defined in the DID-CORE Specification from WC3, each DID Method particularly defines their specific DID scheme.


Scheme
did:example:123456789abcdefghi
DID Method
DID Method-Specific Identifier

DID Subject

According to the DID-CORE Specification from W3C, the “DID Subject” is, by definition, the entity identified by the DID. People and organizations, but also things or even concepts could be a DID subject.

DID Methods

The DID methods are the mechanisms by which a particular type of DID and the associated DID document are created, resolved, updated and deactivated. Even though each DID method has freedom to define its implementation details - e.g.: each DID method can define and implement its own “Verifiable Data Registry” - the implementers of a DID method have to respect the specifications established in the “Methods” section of the DID-CORE Specification from W3C.

[2] Sovrin - Self-sovereign identity (SSI)

DID Documents

The “DID documents” contain the associated data to a DID. In general, these express verification methods, as public asymmetric cryptography keys and endpoints to relevant services for the DID subject interactions. The generic properties admitted in a DID Document are specified in the “Core Properties” section of the DID-CORE Specification from W3C.

Verifiable data registry

A system that allows to register DIDs and the required information to produce the associated “DID Documents”. These registries usually use some form of decentralized storage that allows data verification without the need for a registration authority (e.g. blockchain).

DID resolvers and DID resolution

A “DID resolver” is a component with a standard web interface and provided by each DID method that takes a DID as input and produced a DID document compliant to the DID-CORE standard as output. This process is called DID resolution. The steps to resolve a specific type of DID are defined in the specification for each particular DID method.

5. Solution Architecture

Note: this section will describe the solution architecture, including dimensions of technology but also governance. This description seeks to be independent from any particular technological implementation, basing it in industry standards and focusing on describing the requirements for each component in the architecture.

The proposed architecture is based on the model developed by the “Trust Over IP”[3] foundation, but with some extensions and modifications that are deemed necessary to adapt said model to the specific needs of this initiative on one hand; but also to include concepts originated in other pre-existing works within the digital identity field that will enrich the proposed architecture and expand its reach to a broader audience and a larger diversity of use cases.

[3] Trust Over IP model

The ToIP model consolidates a lot of the know-how and the technological components generated in pre-existing works within the field of self-sovereign digital identity, considering that the ToIP Foundation works in close collaboration with other organizations in the development of standards, foundations and industry consortia to combine their open standards, architectures and protocols in a cohesive, complete stack that allows to create a “digital trust infrastructure” on an Internet scale.

The ToIP model is organized in four layers, each of which has a governance dimension and a technological dimension, and they focus in solving specific problems:

- Layer 1: **decentralized identifiers (DIDs)**
- Layer 2: **digital wallets and agents**
- Layer 3: **verifiable credential exchange and verification**
- Layer 4: **digital trust ecosystems**

In each of the 4 layers of the “ToIP” model there are specifications and technologies that allow their implementation and there are solution definitions that should be reviewed. Both the technologies to be used in each layer, as well as the crucial definitions that need to be reviewed to achieve a design that complies with the specific requirements of this initiative are listed in the following paragraphs.

5.1. Layer 1: Decentralized Identifiers (DIDs)

This layer covers the problems related to a new type of decentralized, persistent, globally unique and interoperable identifiers, which are cryptographically generated and verified and, thus, do not require centralized registration authorities nor centralized service providers.

This layer implements a series of open, public services, required to create, manage, resolve and verify the decentralized identifiers, which constitute the cryptographic roots over which the construction of the “self-sovereign digital identity” is based on.

Decentralized identifiers, different implementations

Different takes on the problem of unique, decentralized identifiers have been developed over the course of the past years. Just to quote some of them, we can enumerate:

- W3C Decentralized Identifiers (DIDs)
- Key Event Receipt Infrastructure (KERI)

- Ethereum Name Service (ENS)

Even if all these approaches cover, in any way, shape or form, the requirements of our initiative, our proposal is to initially implement the layer 1 of the model by following the DID-CORE Specification from W3C, considering that:

- On one hand it provides a better coverage of the specific requirements of this initiative and; on the other hand, because it is the most advanced and the one being widely adopted by different governments, multilateral organizations and digital ecosystems worldwide.

- Additionally, many of the other approaches are converging to the DID-CORE Specification from W3C, which will make interoperability easier in a near future. For example: KERI has been incorporated as a taskforce in the Decentralized Identity Foundation and a new DID method is being created under the name did:keri; and for ENS, Veramo (Ex uPort) is implementing another DID method (did:ens) that allows to dynamically generate a DID and its corresponding DID Document for each name published under ENS by using the data stored in said registry, and has been registered as did:ens under the W3C DID registry.

DID Methods

The DID methods represent the main component in the implementation of this layer of the model, and one of the most crucial decisions in this sense is the definition of which DID methods will the platform support for each particular scenario. That is to say, which DID methods will be supported to manage DIDs generated in this platform and which DID methods will be supported only in resolution mode (read only) in terms of compatibility and interoperability with other similar platforms.

It is important to note that there is not a unique implementation of a DID method, but several implementations that comply with the DID-CORE and that optimized and customized for different requirements. To this date, there are over 70 DID methods registered in the W3C DID registry, and most likely this number will exponentially grow in the near future.

Even if, in theory, the decentralized digital identity platforms should be able to handle all the DID method implementations without any additional efforts; in practice, and considering that DID-CORE is a standard that allows certain extensions, each DID method presents particularities and their integration to the platform requires considerable efforts.

DID Manager

All the DID methods supported by the platform in “management mode”, i.e. all DID methods that will be enabled to create, update, and deactivate the DIDs in this platform, will be registered in this component.

As a starting point, the DID Manager will implement the Peer DID method (did:peer), to handle private interactions between two parties and a proprietary DID method from the platform, which will be public and based on a Verifiable Data Registry, to be used in cases where an unknown number of parties exist (for example, the global audience or a subset of this group).

Details of the two DID methods that will be supported from the beginning in our platform are provided later in this section.

Universal DID Resolver

Even if the Decentralized Identity Foundation maintains a public and open service, known as Universal Resolver (dev.uniresolver.io), which purpose is to provide a unique access point to the DID Resolvers provided by each of the DID methods self-registered with said service, a common practice considering the particularities that each different DID method presents; the idea is that each platform implements its own Universal Resolver to provide not only a unique access point to resolvers but also to standardize the interaction with the DID methods supported by the Universal Resolver, hiding the complexity arising from the particularities of each DID method from the users.

The DID methods supported by the platform in “resolution only mode” will be registered in this component. As a starting point, support will only be implemented for the DID method that will be created specifically for this platform; then, gradually, additional DID methods can be registered to broaden the interoperability and compatibility with DIDs generated in other decentralized digital identity platforms. The Peer DID method is not included in the Universal Resolver due to its resolution is private to the parties and only the involver parties have access to the DID Documents generated through this method.

Peer DID (did:peer)

The particularity in this method is that it does not require a Verifiable Data Registry, as it is optimized for scenarios where only two parties that know each other and have a direct relationship interact, reason which it is destined to be economical, fast, escalatable, secure and very private.

It can be said that Peer DIDs are to public DIDs in a Verifiable Data Registry what constructions like Ethereum Plasma, State-Channels or

Lighting Network are to on-chain transactions, which is to say, they handle the largest portion of the off-chain interactions to increase escalability and privacy, but offer options to reconnect on-chain if necessary.

For more information on the Peer DID method, you can check the specification in the following link: https://identity.foundation/peer-did-method-spec/

QUARK DID (did:tbd)

A proprietary DID method will be created to handle situations that require creating and managing DIDs within our platform and in scenarios that involve three or more parties (e.g. verifiable credentials), which will be formally registered in the W3C DID registry so that it is globally acknowledged.

The creation of a proprietary DID method will allow us to adjust its characteristics to the specific requirements of this initiative. Particularly, we will focus in developing a mechanism for spam and denial of service attacks mitigations adequate for an implementation of this nature; that is to say, a mechanism that can effectively mitigate this attacks but is cost-efficient in terms of transactions, taking into account scenarios in which a large volume of genuine identities in a short period of time has to be added to the system, such as the initial upload of identities when a new jurisdiction is incorporated to the platform.

The creation of this DID method will not be done from scratch, but taking as a basis the available definitions and technological components from other DID methods that have been tested in previous experiences and that can be adjusted to the requirements of this initiative. There are at least three initiatives with a solid track record and that could work as a basis for our own DID method:

- Sovrin: created by the Sovrin Foundation , one of the founding members of the Decentralized Identity Foundation and one of the key participants in the developments on the DIF/W3C framework.
- ETHR: originally created by uPort, a company from the Consensys group, another of the founding members of the Decentralized Identity Foundation and a great influencer of the developments on the DIF/W3C framework.
- Sidetree: a more modern initiative created after the Decentralized Identity Foundation that not only takes advantage of prior experiences like Sovrin and ETHR, but also of the breakthroughs from the past years on blockchain protocols, particularly those of Layer 2.

Of these three initiatives, we consider that SOVRIN, even it being a very valuable experience, cannot be taken as basis as it requires either to be created under the Sovrin Network, or deploy a new network by using Hyperledger Indy; and both cases would be permissioned networks which conflicts with one of the fundamental principles of our initiative: being public, open and non-permissioned.

Based on that, the two alternatives to assess would be:

A. Deploying a DID method by using ETHR over a Layer 2 protocol in an EVM-compatible network so as to obtain escalability layers and costs that match the requirements of this initiative.
B. Deploying a DID method by using Sidetree as a basis in a blockchain network and an IPFS network that have to be defined at the time of creating the detailed specification for the implementation.

Each of these come with advantages and disadvantages that have to be considered in full before defining which is the most convenient. To summarize, we can say that:

- **ETHR,** due to the simple fact of it being an older implementation, has a lot more implementations, extensive documentation and a broader ecosystem of experienced developers. On the other hand, and for the reason of it being a pioneer, it presents some structural problems on its design, which limits its functionality and future development. A favorable aspect of ETHR is that it does not require deploying any nodes, only deploying the smart contracts associated to the method in an EVM-compatible network.

- **Sidetree**, being a more modern implementation that takes advantage of previous experiences and breakthroughs in the base technology, is a lot more efficient and has a higher potential of future developments, is being directly sponsored by the Decentralized Identity Foundation and is being adopted by influential participants like Microsoft. At the same time and for the same reasons, it does not have as many implementations, documentation is not complete and there is a limited ecosystem of experienced developers. An important consideration to take into account with Sidetree is that, even though it is a protocol anchored in an underlying blockchain network that takes advantage of the consensus mechanism in it, it requires the deployment of nodes not only for the Sidetree protocol, but also for the IPFS network used to store the information. This characteristic can be an advantage in some cases, but requires a larger effort to create the node ecosystem that will support the network.

Topics to delve in during the whitepaper co-creation:

- Identity recovery mechanisms
- Key rotation and DID resolution
- Proof of Existence
- Good Safety Practices

5.2. Layer 2: digital wallets and agents

This layer covers the problems on digital wallets and agents required to accept, store and exchange digital credentials over standard communication protocols among peers (P2P). The goal of this layer is to create a secure, private space for all digital interactions that may take place either between individuals, companies, governments or any other "thing" with which we can digitally interact through a digital wallet/agent.

Types of wallets on the Web 3.0

Traditionally, physical wallets are used to store a variety of personal assets, like cash, credit cards, driver licenses, medical insurance cards and presentation cards. Nowadays, we also have a wide variety of digital wallets to store and access digital versions of said assets, with newer options arising every day in the market. However, each wallet represents data and implements their capabilities in a different manner, which significantly restricts interoperability and, in many cases, generates a dependency to the wallet supplier.

In the context of Web 3.0 there are two types of relevant wallets:

- Wallets used to handle **digital assets** (e.g. cryptocurrencies, NFTs)
- Wallets used to store **verifiable credentials** (e.g. driver license, university titles)

Even if both wallets are used to implement applications that base on decentralized architectures (e.g. blockchain networks), their characteristics are significantly different due to the fact that they have been designed to comply with the specific requirements of each of the use cases these were created for (digital assets vs digital identity).

Considering that Quark will focus on Self-Sovereign Identity, the term "wallet" will be used to refer to the type of wallets that is used to handle identity problems but, given that there is certain overlap between audiences on Cryptographic Assets and Self-Sovereign Identity, and also because it is possible that in the future wallets arise that are capable of handle both use cases, we include a brief analysis on the "Appendix III" of this document that compares the fundamental characteristics of each of these wallets.

Wallets and Agents - related terminology

Given there is no complete uniformity on the terminology used by different communities and projects that tackle Self-Sovereign Identity, particularly respecting the terms Wallet and Agent, we shall define what we understand for each of these within the Quark project in this section.

Wallet: a software module, and optionally an associated hardware module, to store and access private keys, credentials and other secrets or confidential resources pertaining a subject in a secure manner. A wallet is usually provided or controlled by an agent.

Agent: a software module that acts as representative of a subject (usually a person), that controls access to a wallet and other private storages of said subject, and that can facilitate interactions with other subjects by message exchange. An agent can be hosted in different locations in a network (cloud vs local).

Identity Wallet: within the context of Quark we will use this term to refer to the logical entity that combines all the capabilities that wallets and agents have according to the definitions above. This entity is, ultimately, the one the different subjects will use (individuals, organizations, things) to perform the different operations relating their Self-Sovereign Identity.

Identity Wallets - Conceptual Architecture

This section describes the main components we believe should be incorporated in the architecture of an Identity Wallet, which tries to synthesize and standardize the descriptions and terminology used by different groups and projects that tackle this topic as part of the Self-Sovereign Identity. For this, and given there is not a total agreement in components nor in terminology used to describe the architecture of an Identity Wallet in said groups or projects, we have based ourselves in the specifications developed by the W3C and the Decentralized Identity Foundation, and supplement it with elements coming from other groups or projects that we deemed valuable.

Key Management Service (KMS)

This is the most basic and fundamental capability in an Identity Wallet, considering it is the one that allows to generate and store pairs of public and private keys, protecting the private keys and digitally sign using diverse cryptographic algorithms. In some cases, it can also support multiple signature schemes, known as “multisig”.

This capability is implemented similarly in the Identity Wallets and in the wallets used for handling digital assets (e.g. cryptocurrency), to such extent that many implementations are done using the same primitive cryptographic libraries; and even certain “Crypto Wallets” can be used to fulfill these needs within an Identity Wallet. For example, the so-called hardware wallets, or wallets like Metamask could be used to implement this capability in an Identity Wallet.

Confidential Storage

A Confidential Storage, as defined in the draft confidential storage specification that is being developed by the Decentralized Identity Foundation, is a mechanism designed with emphasis in data privacy and that allows to store, index and recover encrypted data in a storage provider in such a way that said provider cannot access, analyze, aggregate or resell the data. It additionally guarantees that data can be mobile and are protected against data breaches the storage provider may suffer.

This specification is limited to detailing the requirements for this component in an independent way from the implementation details, to allow diversity of implementations in different types of devices and network locations. In this way, a confidential storage implemented in a mobile device or in a cloud provider will have similar capabilities and the same operation interface, even if the underlying infrastructure is completely different. This allows, on one hand, the data portability amongst different implementations, and on the other hand that a subject (individual, organization, thing) can have their information replicated in different sites to prevent data access loss if there is a problem with any of the copies.

Typically, access to a confidential storage” is done through one or several “Decentralized Web Nodes” (a.k.a.: Identity Hubs), another key component in the architecture of an Identity Wallet, which shall be described later in the document.

DIDComm Messaging

Even though currently there are robust mechanisms for secure communications, all of them depend in centralized constructions mainly tied to a specific means and were designed to comply with requirements in Web 2.0, where it is assumed that interactions between parties are facilitated through highly available web servers operated by experts who, at the same time, impose terms and conditions non-compatible with the privacy, interoperability and independence requirements Web 3.0 demands.

In this context, DIDComm proposes a new alternative that not only reuses a lot of the existing technology in terms of secure communications, but also solves the limitations of current mechanisms in this matter.

The purpose of DIDComm is providing a new secure, private communication mechanism based on the decentralized design of DIDs to create a truly peer-to-peer communication infrastructure, independent of any centralized service, able to function in a variety of communication means and in scenarios where communication availability could be intermittent, like in the case of users operating through mobile devices. All of these are characteristics needed to comply with the Web 3.0 requirements.

DIDComm protocol specification v2 is already available. There is a decent diversity of libraries that implement it and a high adoption level in Self-Sovereign Identity projects worldwide, which has made it into a *de facto* standard to comply with the communication between peers corresponding to Web 3.0.

Decentralized web node (DWN)

A Decentralized Web Node (a.k.a.: Identity Hub, or DWN) is a mechanism that facilitates the message transmission in peer-to-peer mode between subjects (individuals, organizations and things), as well as manages the storage of public or private data with a given decentralized identifier (DID).

The Decentralized Web Nodes are a data storage construction with a mesh architecture that allows a subject to have multiple synchronized nodes to maintain an equal status of information, allowing the subject to protect and manage their data, as well as perform transactions with other subjects without depending on location or infrastructures, interfaces or routing mechanisms dependent from a specific provider.

It is important to note that DWNs do not perform the message transmission nor it manages storage, but it acts as facilitator, a public interface that can be accessed from the web to provide online presence to all involved parties in flows related to the credential exchange. Management of the data storage itself is performed by the capacity of Confidential Storage described above, and message transmission is performed by the DIDComm protocol also described above.

DWNs are particularly important in the cases of individuals or things, as they typically do not have a permanent online presence that allows them to receive interactions started on others DWN, either from themselves or from third parties. For example, an individual that only uses an Identity Wallet in a mobile device could not be directly contacted by other subject that requires to start a peer-to-peer flow to exchange credentials. For more details on these type of interactions you can check the Topology section in the DWN Specification draft developed by the Decentralized Identity Foundation.

Individual vs Organizational Wallets

Custodial vs Non-custodial

Identity Recovery

Good Safety Practices

5.3. Layer 3: credential exchange and verification

Layer 3 of the ToIP model enables a "**human trust**" framework (in verifiable claims about entities, attributes and relationships) that supplements the "**cryptographic trust**" enabled by layers one and two. Layer four, as we will see later, expands and supplements this framework of "**human trust**" with models and trust policies belonging and specific to each digital trust ecosystem.

To achieve its purpose, this layer facilitates the exchange of verifiable credentials and cryptographic proofs between issuers, holders and verifiers; by leaning in the formats of data exchange, verifiable credential protocols and the verifiable credentials' trust triangle model, which allows it to establish transitive trust relationships for the interactions in digital channels in an interoperable way on a global scale among any of the three participant that define said model: issuers, holders and verifiers.

The “trust model” described in the Verifiable Credentials Data Model v1.1 specification lists the principles over which trust relations are deemed valid among the different participants and that support the model as such. For example, “the verifier trusts the issuer of a credential”.

Verifiable credentials - Data model

The VC data model, defined by W3C, is a universal data format that allows any entity to perform verifiable claims over another entity to describe a quality or qualities, property or properties that determine the existence and uniqueness of the entity over which said claims are made of.

The fundamental goal of the Verifiable Credentials standard is to enable the digital equivalent of the physical credentials that we store in our physical wallets and that we use daily to prove our identity and/or our attributes.

The VC data model provides a common mechanism for the digital credentials interoperable implementation that are cryptographically secure, tamper-free, privacy-respectful and verifiable through digital mechanisms. This model allows to pack credentials, sign them cryptographically and generate associated cryptographic proofs in a standardized manner. This enables the creation of ecosystems that share sets of interoperable credentials that can be processed and understood by different systems within the ecosystem.

Here are listed the participants and main entities within the Verifiable Credentials model, as defined by the “Verifiable Credentials Data Model v1.1” specification from W3C.

Subject: an entity over which claims are made. Subjects could be people or organizations, but also animals, things and even concepts. An individual, a company, a car or an animal are examples of subjects. The holder of a verifiable credential may or may not be the subject of said identity. For example: a parent (holder) could have the verifiable credential of their child (subject), or the owner of a pet (holder) may have the verifiable credentials of their pet (subject).

Holder: a role a subject performs when they possess one or more verifiable credentials and generate verifiable presentations from them.

Issuer: a role an entity performs that carries out claims over one or more subjects, that creates verifiable credentials from these claims and that transmits said credentials to their holders. Issuers, for example, can be companies, non-profit organizations, commercial associations, governments and even individuals.

Verifier: a role an entity performs when receiving one or more verifiable credentials, optionally within a verifiable presentation, for its processing. Verifiers can be, for example, employers, security personnel, websites or individuals.

Claim: represents a qualification, achievement, quality or information on the antecedents of a subject such as a name, a governmental identification, a particular address or a university degree. A subject can be an individual, an organization or a thing.

Credentials: a set of one or more claims performed by the same identity over the same subject. They can also include an identifier and metadata to describe the properties of a credential, such as the issuer, date and time of expiration, a representative image, a public key to be used for verification, a revoking mechanism, etc.

Verifiable Credentials: it is a credential, as defined in the previous paragraph, which includes cryptographic material that allows the detection of data tampering and to irrefutably prove who issued it.

Verifiable Presentations: they contain data of one or more verifiable credentials packeted in such a way that it is possible to verify the data issuing and integrity. They can also be conformed by data derived from verifiable credentials which validity and issuing can be cryptographically verified, usually by using Zero Knowledge Proofs algorithms. Presentation data often deal over the same subject, but could have been issued by different issuers. Verifiable presentations must include a cryptographic proof, typically a digital sign, which allows to verify that whoever is doing the presentation is the holder of the credential.

Verifiable Data Registry: a system that intervenes in the creation and verification of identifiers, keys and other relevant data, like verifiable credential schemes, revoking registries, issuers public keys, etc., that could be needed to use verifiable credentials. These registries can be implemented by using decentralized registry technologies (e.g. blockchain); but this is not a must as they can also be implemented using centralized technologies.

Types of Verifiable Credentials

This section will present the different variants of Verifiable Credentials (VC) that are described in the Verifiable Credentials Data Model v1.1 specification from W3C. It also briefly explains their differences and presents the interoperability trilemma that arises from the existence of three different VC options. Finally, it recommends the adoption of the newest VC format considering this is aimed to satisfy the requirements of a larger part of interested parties.

Why does this matter? Without converging to a standardized VC format, there would not be a functional interoperability in the entire ecosystem. If the app developers implement cryptography related to the VC using incompatible libraries and methods, and the underlying data have different read properties, interoperability cannot be achieved.

What is common between the different methods is that issuers use them to packet claims over a subject. The issuing entity then uses cryptography to seal the credential, and this seal provides a mechanism for other entities (verifiers) verify the cryptographic signatures to verify if the credential has integrity in terms of the issuer public keys.

The difference is in the formats that use claims within verifiable credentials and presentations, as well as the proofs they use to seal the verifiable credentials and/or presentations.

Next, you will find the three variants of VC that are described in the Verifiable Credentials Data Model v1.1 specification from W3C. All of them have more than one critical implementation in several production steps.

JSON-LD

This variant uses a format based on JSON-LD secured with Linked Data Signatures or BBS+ signatures to enable Zero Knowledge Proofs (ZKP) and is mainly driven by the ecosystem driving the Linked Data and Semantic Web paradigm.

The variant that combines JSON-LD ZKP and BBS+ is gaining traction, considering it enables a way to use JSON-LD with ZKP capabilities, something that was not possible before the appearance of BBS+. The benefit of using this approach is that, first and foremost, it totally complies with the VC specification as it currently is. Besides, since its signatures and proofs are self-descriptive and self-contained, they do not require any additional configuration nor external dependencies. This approach allows the simple standardized use of JSON-LD to take advantage of open data vocabulary, and at the same time it keeps the characteristics of privacy preservation such as Selective Disclosure or ZKP, which traditionally came with their own set of limitations and concessions. With this variant it is no longer needed to choose between interoperability based on standards or privacy-preserving cryptography; we can have both.

JWT

This variant uses a JSON format secured with JSON Web Signatures, specifically in the form of JSON Web Tokens (JWT) and is mainly driven from the Identity and Access Management (IAM) solutions suppliers' ecosystem.

This ecosystem tends to visualize Login as the base of the VC exchange protocol and aims to perform an implementation by reusing the technology stack they currently use: JSON Object Signing and Encryption (JOSE) and OpenID Connect.

It is clearly a robust option to implement the use case of logins to websites using Self-Sovereign-Identity as an identity supplier, but it is not the best options of other use cases belonging to Web 3.0.

ZKP-CL

This variant uses ZKP with Camenisch-Lysyanskaya signatures (ZKP-CL).

Given it is a format that is intimately related to Hyper Ledger Indy, it will not be considered for the Quark project since it seeks to be independent from the blockchain network it uses as anchor.

Credential Exchange

The way the issuer agents, the holders and the verifiers must perform the credential exchange among themselves is another characteristic that defines the ToIP model on Layer three with the goal of enabling functional interoperability through the entire ecosystem.

Considering there are several specifications that cover the different aspects of the verifiable credentials exchange, this section will briefly describe the different aspects of said implementations and will propose an alternative for those cases where there is no common decision from the community on how to implement a particular aspect.

Presentations Exchange

The basic problem to achieve credential exchange interoperability is defining a standard mechanism to facilitate the two main steps in an exchange of this kind: a way for verifiers to describe their proof requirements and one for holders to describe the proof presentations aligned to those requirements.

To tackle these requirements, the Presentation Exchange v1.0.0 specification defines a data exchange protocol composed of two data formats: Presentation Definition and Presentation Submission.

Presentation Definition is the data format used by verifiers to articulate the proof requirements that must be fulfilled by the holders. This format defines, amongst others, the type of required credentials and the accepted options for each type (e.g. it is required to present an identity document and the valid options are a password, a national ID and a driver’s license). Additionally, this data format defines the encoding characteristics and the type of cryptographic algorithms supported by the verifier.

Presentation Submission is the data format used by holders to describe the proofs they are submitting, which must be obviously aligned and must fulfill the requirements specified by the verifiers in the Presentation Definition.

The Presentation Exchange V1.0.0 specification is designed to be independent from any type of verifiable credentials and also from the transport envelops that are typically associated with each type of verifiable credential. This means that an implementer can use JSON Web Tokens (JWTs), Verifiable Credentials (VCs), JWT-VCs or any other claim format, and transmit them through Open ID Connect, DIDComm, Credential Handler API or any other transport envelope.

Additionally, this specification does not define transport protocols, specific endpoints or other means to transmit the formatted objects it defines, so that any other specification and projects that define said mechanisms can use within their workflows the data formats define in this specification.

Wallet and Credential Interactions (WACI)

Unlike the Presentation Exchange v1.0.0 specification described above, the draft of Wallet And Credential Interactions specification provides a complete definition of a protocol to cover the different required aspects to implement the two main interactions (issuing and presentation) needed in the life cycle of verifiable credentials.

Said specification incorporates the data formats defined in the Presentation Exchange v1.0.0 specification and supplements them with elements arising from a series of other existing specifications and protocols, without assuming nor requiring an implementer understand all of them, hence removing the complexity of it. It inherits the general structure from the WACI original draft, but uses elements coming from the DIDComm v2.0 messaging protocol together with "Aries Present Proof" message formats and "Presentation Exchange v1.0.0" DIF data objects. This specification version is also restricted to the verifiable credentials that use BBS+ and LD-Signatures.

Quark VC

Based on what was stated in the previous sections in this chapter and the requirements, the layer three implementation of the ToIP model in the Quark project will be done initially by using a JSON-LD credential scheme secured with BBS+ signatures, and a credential exchange scheme based on the WACI specification, considering it is the model that adapts best to the present and future needs of the project, the different use cases and workflows required and the Web 3.0 paradigm; but also because it is the one that has the best leverage with the capacities implemented in both layer one and two of the model.

This approach will allow us, among other things, to implement very sophisticated functionalities, like Selective Disclosure and ZKP, with minimum effort without doing concessions in terms of user experience or introducing requirements that might raise an entry barrier for users and another ecosystem actors.

Eventually, to obtain backwards compatibility with Web 2.0 that use Federated Identity mechanisms, specifically for SSI login cases, an additional implementation of a credentials scheme based on JWT and a credential exchange based on the technological stack of OpenID Connect and JOSE could be assessed.

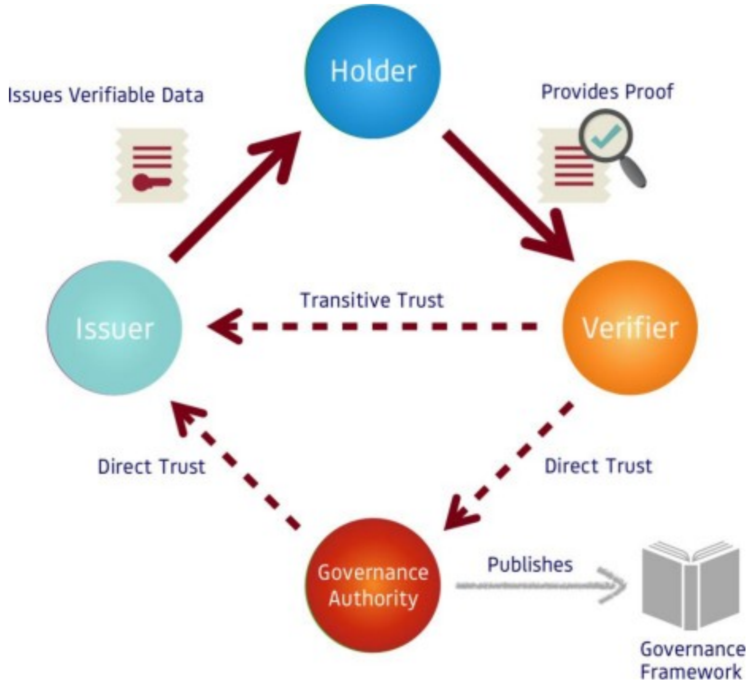
Other topics to analyze in this section

- Credentials vs NFTs
- Selective Disclosure
- Identity recovery

5.4. Layer 4: Apps

Layer four of the ToIP model facilitates the development of "**digital trust ecosystems**", complete families of apps and credentials not only designed to technically interoperate, but also share a "**common framework of ecosystem governance**", which specifies the purpose, principles and policies applied to all the government authorities and government frameworks that operate in each of the four ToIP stack layers for each ecosystem. Among others, this allows to define standardized information models for the set of credentials from each ecosystem, which also enables end-to-end functional interoperability between them.

This way, the trust triangle defined and implemented in layer 3 evolves to the trust diamond, as can be seen in the following figure, in which while the top half shows a basic trust triangle architecture used by verifiable credentials, the lower half shows a second trust triangle, the **governance trust triangle**, that can solve a series of problems related with the adoption and escalability in the real world of the verifiable credentials and the ToIP stack.



Trust diamond and digital governance. Source: trustoverip.org4

[4] Introduction to Trust Over IP

The **governance trust triangle** represents the same model of governance that exists for many successful physical credentials that we use daily: passports, driver licenses, credit cards, medical insurance cards, etc. These credentials are backed up by rules and policies that, in many cases, have taken decades to evolve. These rules and policies have been developed, published and applied by many different types of existing **governance authorities:** private companies, industrial unions, financial networks and, of course, governments.

The same model can be applied to verifiable credentials by simply making this same government authorities, or new ones explicitly formed for the ToIP government, publish **digital governance frameworks.** Any group of issuers that wishes to standardize, strengthen and escalate the credentials they offer, they can join under the auspice of a sponsoring authority to create a governance framework. Whichever the organization form (government, union, association, cooperative), the purpose remains the same: defining the commercial, legal and technical rules under which the members of an ecosystem agree to operate to achieve trust through said ecosystem.

With the ToIP stack, this governance architecture can be applied to any set of roles and/or credentials, to any digital trust ecosystem, of any size and in any jurisdiction.

Nowadays Internet is a network of networks, where interconnections between each net is done through the TCP/IP stack. ToIP enables the evolution to **an ecosystem of digital trust ecosystems**, where interconnections between each of these ecosystems is done through the ToIP stack and the limits of each digital trust ecosystem is determined by the governance frameworks under which their members operate.

This allows Internet to maintain the same diversity and richness that it has nowadays, but with a new capacity that allows to form and maintain trust relationships of any type at any distance: personal, commercial, social, academical, political. This trust relationships can flow from one trust ecosystem to another in the same way IP packets can flow from one net to another in the actual Internet.

Quark at Layer 4

The first step in the Quark roadmap aims to deploy a first ecosystem and its corresponding governance framework surrounding credentials and use cases related to the Government of the City of Buenos Aires but, as previously mentioned, this will create an open, decentralized and non-permissioned infrastructure that can be freely reused by other digital trust ecosystems to end up constituting an ecosystem of digital trust ecosystems over the ToIP stack. Additionally, the critical mass that Quark will provide in this first stage will act as a gravitational force that will stimulate the creation of said ecosystems, creating the required feedback for the system to obtain long-term sustainability and complete autonomy from the Government of the City of Buenos Aires.

6. Biometry

7. Identity Management and Recovery

The expression "not your keys, not your coins" is very popular and important in the world of crypto currency and crypto assets. This means that, if somebody does not have the exclusive control over their private keys, they cannot really have control and decision-making power over said assets.

Given that Self-Sovereign Digital Identity can be understood as a type of digital asset which implementation also shares a lot of the technological stack and the decentralization paradigms used in the crypto assets world, this section explores the concept mentioned earlier but specifically applied to the "control of the self-sovereign digital identity".

DIDs vs SCIDs

A **Self-Certifying IDentifier,** or SCID, cryptographically links an identifier to a pair of private and public keys, in such a way that: 1) the relationship between the identifier and the public key can be proved in a deterministic manner, 2) the corresponding private key can be used to prove control over the identifier, and 3) it is not required to have any additional elements to certify this relationships.

Crypto assets typically use some form of SCIDs to identify who holds control over them. The **addresses** are the most common form of SCIDs in blockchain networks that handle crypto assets. Correspondence between a blockchain address and a public key can be proved in a deterministic manner and, therefore, the corresponding private key can be used to prove control over the blockchain address, without needing any other additional element to certify these relationships.

DIDs are identifiers that share with SCIDs the characteristic that control over the identifier can be verified cryptographically but, unlike SCIDs, DIDs usually require additional elements to perform this check (DID Documents and DID Registries). There are some DID methods that generate DIDs that also are SCIDs, but it is not that frequent.

Even though SCIDs are easy to implement and highly efficient due to their self-certifying characteristic, they generally do not comply with all the requirements imposed by the Self-Sovereign Identity. DIDs, however, pose certain complexity due to their requirements of a complex infrastructure, but allow the implementation of advanced functions such as key rotation, multiple-signature schemes or role management associated with a DID, all needed functions to fulfill the requirements of Self-Sovereign Identity.

DID Document

To enable the advanced functions mentioned in the previous paragraph, the DIDs model introduced the DID Document resource, which allows to specify the information associated with a DID that said functions require. Among other things, these documents can include several verification methods (e.g. public keys) associated to the DID and the roles in which said verification methods can be used.

There are two main roles that can be included in a DID Document: Controllers and Delegates

Controller

This role allows to modify the information of the DID Document. A DID Document can define one or more controllers by specifying the public keys of each of them.

The controller holds control of the DID Document and ultimately, of the DID, as they can modify the DID Document and have the faculty of eliminating or adding other controllers. In other words: **whoever holds control over the private key corresponding to a DID Document controller holds control over said document and, ultimately, over the DID.**

When it comes individuals, usually the DID subject is also the DID Document controller; but there are cases where the controller may not be the DID subject. For example: parents of an underage child can be the controllers of the DID Document of their child.

When a DID identifies an organization, animal or thing, the controllers are always the individuals authorized to fulfill that role. Example: the owner of a pet will usually appear as DID Document controller of the pet.

Delegate

This role allows to delegate a specific set of functions to a delegate so they can act on behalf of the DID subject for those functions. For example: a DID Subject, through their controller, delegates to a third-party the faculty of signing verifiable credentials on their behalf.

Delegates can only perform the faculties they were authorized for and have no permission to update the DID Document, so they don’t control the document and, therefore, do not control the DID.

Key Management

Some situations related to the public and private key management associated to the DIDs needed to be considered when implementing a Self-Sovereign Identity platform are described next.

Key Rotation

Key Rotation allows to modify the pairs of private and public keys associated to the different roles defined in a DID Document.

Periodic key rotation is a good safety practice and is aimed at minimizing the possibility of the private keys associated to any of the defined roles be compromised and used by non-authorized people.

Loss and Recovery of control over Identity

As mentioned in previous paragraphs, in the context of Self-Sovereign Identity, holding control over the identity is synonym of holding control over the private keys of the controllers specified in a DID Document associated with a DID.

Even if there are several identity recovery schemes, all of them ultimately lead to one thing: recovering control and exclusive access to the private keys of the controllers that are specified in the DID Document, usually by executing a key rotation in these roles, by some mechanism predefined in the DID Method. Different DID Methods could define different approaches to enforce key rotation as part of the identity recovery mechanism.

An aspect to highlight is that, given that key rotation does no change the DID value, the association between DID and verifiable credentials issued from that DID is not affected when a key rotation is performed. This means that it is not needed to issue new verifiable credentials for a subject if they recover their identity by means of a key rotation.

Custodial vs Non-Custodial

As previously mentioned, and in the context of crypto assets, having or not exclusive control over private keys normally determines having or not control of the crypto assets associated with the corresponding addresses.

There are two wallets aligned with this concept: Custodial and Non-Custodial; and there is also a large debate on the crypto world over the advantages and disadvantages of each of these wallets.

In the context of Self-Sovereign Identity, having control over an identity means having control over the private keys of all the controllers defined in the DID Document, considering that if a private key of one of them is compromised, a malicious party could use it to change or eliminate the controllers and all the data in the DID Document, gaining then control over said identity.

Additionally, it is important to remember that a DID can also have delegates that can represent them in specific situations, which implies that if any of these private keys are compromised, the control over some aspects of the identity can also be compromised.

Given this, and in the context of Self-Sovereign Identity, the terms “custodial” and “non-custodial” are not directly related with having or not control over the Identity, since holding control over the identity means controlling all the private keys that control one of the aspects, which could be controlled by different people that, at the same time, could be using different types of wallets to handle their private keys.

Even with these considerations, it is important to seriously take into account this aspect in any implementation of a Self-Sovereign Identity platform, especially thinking that an implementation of this kind aims at being massive, goes through different user segments with diverse capacities and preferences that have to be included so as not to generate any exclusions.

Even if a custodial wallet can be considered as less secure than a non-custodial wallet because it involves trusting a third-party, in reality this depends on the ability each person has to comply with all the security rules in a non-custodial wallet. In many cases, a custodial wallet can be a valid option for users that prefer not to be burdened with such responsibility and that prefer other aspects like ease of use.

Having a variety of custodial and non-custodial wallets seems ideal, and having each user choose the one that better adjusts to their needs.

Guardianship

As humanity constantly progresses to a more digital world, there is the risk that digital exclusion increases to those that cannot act for themselves in this new context. This risk is particularly important in a Digital Identities implementation, since depriving access to identities has a severe impact in terms of exclusion, and also because there are many cases in which individuals cannot act for themselves to access this fundamental right.

Self-Sovereign Identity systems in which control of a digital identity is proven by using digital credentials stored in a digital wallet pose an additional challenge. How can we allow everyone to control their digital identity when, by definition, we experience different stages in life (like childhood) and conditions (like dementia) in which the Law and social rules determine we cannot be self-sufficient? This challenge cannot be resolved by a simple delegation because a child, a person suffering dementia or a refugee without internet connection cannot delegate something they do not have. It is not also a simple controller relationship to a thing (like a drone) because, unlike a drone, a child acquires rights progressively and eventually becomes more self-sufficient. Similarly, a person suffering dementia will experience a change in capacity over time.

Given this, identity systems need a means to represent those that cannot act for themselves in the digital world. This is the Guardianship capacity that has to be carefully developed and implemented in any Self-Sovereign Identity platform.

For more information on this issue, please read the document “On Guardianship in Self-Sovereign Identity” published by the Sovrin Foundation.

8. Government

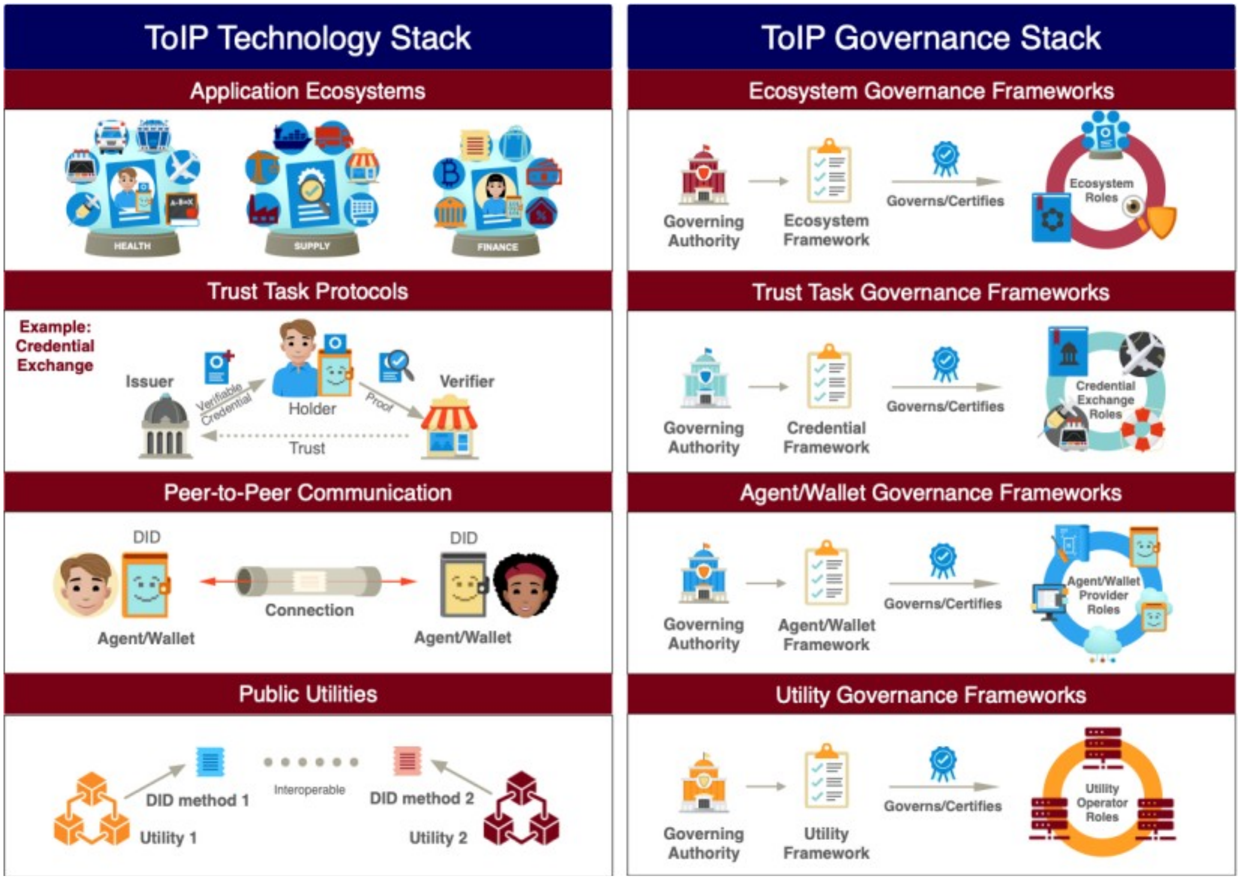
8.1. Introduction

Trust over IP (ToIP) defines a complete architecture to create **digital trust** on an Internet scale and enable the creation of interoperable **digital trust ecosystems** of all kinds and sizes.

A distinctive trait of this architecture is that it combines a series of protocols and tools in different technology layers with a set of rules formally known as Governance Frameworks (GF).

According to the ToIP Foundation, this fusion of governance and technology is crucial to enabling the path to a universal, reliable and interoperable decentralized identity system, and it constitutes the fundament of a new **digital trust framework** that satisfies the legal, commercial and social requirements deriving from the interaction between people, organizations and things in a completely globalized, digital context such as the one we are experiencing in the 21st Century.

The following figure shows the design in two dimensions (technology and governance) in the ToIP stack. The emphasis this model puts on governance has to do with, at least for the time being, technology on its own is not enough to generate digital trust in the context of global scale and diversity of situations, simply because trust is a psychological belief of the human beings. Therefore, technology must adapt to human behavior to generate end-to-end trust in said context.



The following sections will describe the most important characteristics of the governance model proposed by ToIP and their application to the specific context of Quark ID and the GCBA ecosystem.

For a detailed description of the architecture and the governance metamodel proposed by the Trust over IP Foundation, please refer to the following documents published on https://trustoverip.org/our-work/deliverables/:

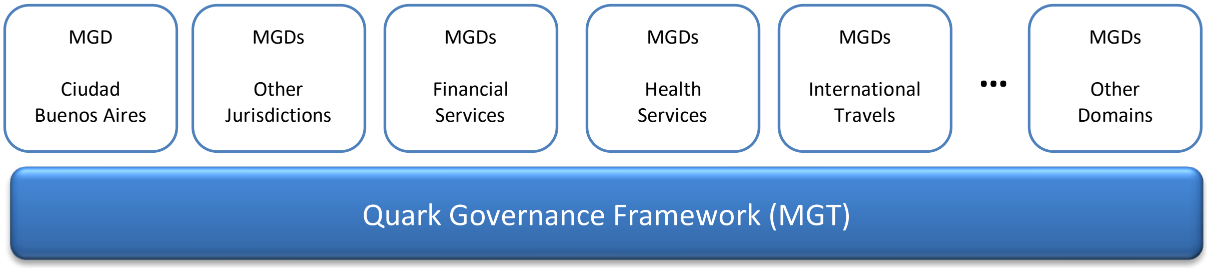
- Governance Architecture Specification V1.0
- Governance Metamodel Specification V1.0
- Governance Metamodel Specification Companion Guide

8.2. Digital Trust Ecosystems

As previously mentioned, ToIP enables the evolution of Internet from a **network of networks to an ecosystem of digital trust ecosystems**, where interconnections between each of these ecosystems is done through the ToIP stack and the limits of each digital trust ecosystem is determined by the governance frameworks under which their members operate.

The stated in the previous paragraph implies that withing Quark there is not just one but multiple governance frameworks operating simultaneously. As can be seen in the next figure, there is a Quark Governance Framework (MGT) that provides a base over which the rest of the Governance Frameworks are built for each of the Specific Domains (MGDs).

While the MGT provides the rules that apply to all ecosystems participating in the network, the Specific Domains Governance Models extend MGT with rules proprietary to each ecosystem.



The Quark Governance Framework (MGT) supplies the base of other Specific Domains Governance Frameworks

This structure allows to preserve the same diversity and richness that it has nowadays on Internet, but with a new capacity that allows to form and maintain trust relationships of any type at any distance: personal, commercial, social, academical, political. This trust relationships can flow from one trust ecosystem to another in the same way IP packets can flow from one net to another in the actual Internet.

8.3. Governance Frameworks per layer

Another important aspect to consider when defining a governance framework compatible with ToIP is that governance is applied in different ways to each of the four layers in the ToIP model and, therefore, governance authorities (of any kind) and governance frameworks (of any kind) are needed for each of these four layers.

These governance authorities and frameworks can be formally or informally implemented, either by computer coding or legal coding as needed, but its existence is fundamental to create digital trust and facilitate commercial, legal, social and political acceptance of these new paradigms.

DIDs Public Services

This layer implements the DID Public Services that are required to search and verify the public keys of the issuers of digital credentials, constituting the trust roots or trust anchors of the entire public/private key infrastructure; the starting points.

It is important to consider, when designing the governance framework for this layer, that these services are public, open and are commonly used by all the ecosystems that operate with the platform.

DID **public services** governance frameworks clearly establish the policies and procedures used to:

- Operate these public services in a secure, transparent and reliable way, maintaining their efficiency and escalability.
- Manage the life cycle of the public keys associated with the DIDs in a secure, efficient and friendly way, considering the specific needs of different types of users (e.g. identity creation and recovery, key rotation, etc.).
- Avoid abuse or misuse of these public services (e.g. spam) and ensure their economic sustainability in the long term.

Layer 2 - Wallets and Agents

This layer implements the wallets and agents people need, the organizations and digital “things” (or digital twins of non-digital things) to accept, store and exchange digital credentials using standard peer-to-peer communication protocols like DIDComm.

The governance framework for wallets/agents clearly establishes the standards, policies and procedures that must be observed by the wallet suppliers and agents to ensure the security, privacy, data protection, interoperability and data sovereignty.

Layer 3 - Credentials

This layer, in the technical aspect, implements the **trust triangle of verifiable credentials**, which allows establishing transitive trust relationships between three parties (issuers, holders and verifiers) using data exchange formats and protocols for verifiable credentials. The governance frameworks in this layer add a second trust triangle, called governance trust triangle, conformed by the issuers, the verifiers and the governance authority. The combination of both trust triangles creates what is known as a trust diamond, described earlier in this document.

The credentials governance frameworks focus on standardizing the commercial, legal and technical policies to issue, maintain and verify a set of credentials. These governance frameworks define, among other things:

- Who is authorized to issue certain kind of credentials so that verifiers have all the information they need to make trust decisions based on the proofs deriving from the verifiable credentials presented to them.
- What information can a verifier request to avoid requesting additional information for a given purpose.

Layer 4 - Ecosystems

Layer four of the ToIP model facilitates the development of “**digital trust ecosystems**”, complete families of apps and credentials not only designed to technically interoperate, but also share a “**common framework of ecosystem governance**”, which specifies the purpose, principles and policies applied to all the government authorities and government frameworks that operate in each of the four ToIP stack layers for each ecosystem.

Generally, the governance framework of an ecosystem includes acknowledging independent authorities and governance frameworks authorized and/or backed-up on the lower layers. These governance frameworks can also specify trustmarks, trust registries, usability requirements, certification programs and other required mechanisms to ensure the integrity and health of the entire ecosystem.

9. Adoption Strategy

Note: this section will include the relevant definitions and criteria to achieve a large adoption of the platform, having the backup and drive given from the GCBA.

Some basic steps of the roadmap

1. Co-creation of the definitions on the protocol and standards to be implemented.
2. Development of the required technological infrastructure.
3. Development of the first app from the GCBA.
4. Mass adoption of digital identities driven by the GCBA app.
5. Drive the adoption of the ecosystem by society and private parties.
6. Drive the adoption of scores associated to the digital identities between private parties.

Appendix I

The 10 principles on Self-Sovereign Identity, as defined by Christopher Allen (2016)[5] are introduced next:

- **Existence.** *Users must have an independent existence.* Any self-sovereign identity is ultimately based on the ineffable "I" that is at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the "I" that already exists.

- **Control.** *Users must control their identities.* Subject to well-understood and secure algorithms that ensure the continued validity of an identity and its claims, the user is the ultimate authority on their identity. They should always be able to refer to it, update it, or even hide it. They must be able to choose celebrity or privacy as they prefer. This does not mean that a user controls all of the claims on their identity: other users may make claims about a user, but they should not be central to the identity itself.

- **Access.** *Users must have access to their own data.* A user must always be able to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers. This does not mean that a user can necessarily modify all the claims associated with his identity, but it does mean they should be aware of them. It also does not mean that users have equal access to others' data, only to their own.

- **Transparency.** *Systems and algorithms must be transparent.* The systems used to administer and operate a network of identities must be open, both in how they function and in how they are managed and updated. The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture; anyone should be able to examine how they work.

- **Persistence.** *Identities must be long-lived.* Preferably, identities should last forever, or at least for as long as the user wishes. Though private keys might need to be rotated and data might need to be changed, the identity remains. In the fast-moving world of the Internet, this goal may not be entirely reasonable, so at the least

[5] https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md

identities should last until they've been outdated by newer identity systems. This must not contradict a "right to be forgotten"; a user should be able to dispose of an identity if he wishes and claims should be modified or removed as appropriate over time. To do this requires a firm separation between an identity and its claims: they can't be tied forever.

- **Portability.** *Information and services about identity must be transportable.* Identities must not be held by a singular third-party entity, even if it is a trusted entity that is expected to work in the best interest of the user. The problem is that entities can disappear
— and on the Internet, most eventually do. Regimes may change, users may move to different jurisdictions. Transportable identities ensure that the user remains in control of his identity no matter what, and can also improve an identity's persistence over time.

- **Interoperability.** *Identities should be as widely usable as possible.* Identities are of little value if they only work in limited niches. The goal of a 21st-century digital identity system is to make identity information widely available, crossing international boundaries to create global identities, without losing user control. Thanks to persistence and autonomy these widely available identities can then become continually available.

- **Consent.** *Users must agree to the use of their identity.* Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user. Though other users such as an employer, a credit bureau, or a friend might present claims, the user must still offer consent for them to become valid. Note that this consent might not be interactive, but it must still be deliberate and well-understood.

- **Minimalization.** *Disclosure of claims must be minimized.* When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. For example, if only a minimum age is called for, then the exact age should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques, but non-correlatability is still a very hard (perhaps impossible) task; the best we can do is to use minimalization to support privacy as best as possible.

- **Protection.** *The rights of users must be protected.* When there is a conflict between the needs of the identity network and the rights of individual users, then the network should err on the side of preserving the freedoms and rights of the individuals over the needs of the network. To ensure this, identity authentication must occur through independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralized manner.

Appendix II

Mapping of design principles vs the 10 principles for Self-Sovereign Identity.

PRINCIPLES FOR SELF-SOVEREIGN IDENTITY	**DESIGN PRINCIPLES**
EXISTENCE	*Proof of Existence*
	Proof Of Humanity
CONTROL	Custodial vs Non-Custodial
	Identity Recovery
ACCESS	Decentralized
TRANSPARENCY	Co-creation
	Open code
PERSISTENCE	
PORTABILITY	
INTEROPERABILITY	Credentials vs NFTs
CONSENT	*Selective Disclosure*
MINIMALIZATION	
PROTECTION	Security standards

Appendix III

Crypto Wallets vs Identity Wallets

As previously mentioned in the document, in the context of Web 3.0 there are two types of relevant wallets:

- Wallets used to handle **digital assets** (e.g. cryptocurrencies, NFTs)
- Wallets used to store **verifiable credentials** (e.g. driver license, university titles)

The fundamental characteristics of each of these types of wallets are described next in a comparative manner. To make this reading easier, within this Appendix we will refer to them as “**crypto wallets**” and “**identity wallets**”, respectively.

General aspects

Both crypto and identity wallets belong or are linked to a subject, who can be an individual, organization or even a thing (e.g. an electric car could have an associated wallet).

From a utility point of view, while crypto wallets focus on handling assets from the subject (e.g. cryptocurrencies, NFTs), identity wallets focus on handling credentials that describe a characteristic of the subject’s identity (e.g. a driver license or a University degree).

Private Keys and Digital Signature

The most basic and fundamental capacity in both types of wallets is that they allow to manage private keys and digital signatures, and in both cases this is implemented in a similar manner; in fact, many implementations are performed using the same primitive cryptographic libraries.

In both cases it is required to implement a Key Management Service (KMS) that allows to generate and store pairs of private and public keys, protect private keys and digitally sign by using a diversity of cryptographic algorithms. In some cases, this capacity can also support multiple signature schemes, known as “multisig”.

While in crypto wallets private keys are used to prove control over digital assets stored in a blockchain network; in digital wallets, private keys are used to prove control over some of the aspects described in a DID document

Storage

There also are significant differences on storage between crypto wallets and identity wallets; not only on the information they store but also on the replication and synchronization mechanisms they implement.

While crypto wallets only store information related to KMS (private keys, public keys, blockchain addresses, as the rest of the data is stored in the blockchain networks), identity wallets are responsible for storing privately and securely all the information associated with the identity of a subject, mainly their verifiable credentials. For example: while the cryptocurrency balance associated to a blockchain address is not stored in the crypto wallet but on the corresponding blockchain network, the verifiable credentials associated with a subject are stored in the identity wallet. It is not recommended to store this data on a blockchain network due to compliance and security.

On the other hand, while identity wallets (at least the most sophisticated) tend to implement mechanisms that allow to keep the information relative to a subject replicated and synchronized in different devices the subject might use, crypto wallets do not require this mechanic as the replication and synchronization capacities is provided on a blockchain network level (e.g. the balance of an address is stored in all of the nodes of a blockchain network).

In both cases, information related to KMS can be synced in different devices by using seed phrases, from which the entire hierarchy of private keys, public keys and addresses associated with the wallet can be reconstructed.

Operations

While crypto wallets are aimed at preparing and signing transactions that will be processed in a blockchain network, identity wallets are aimed at preparing and signing credentials or proofs that will be exchanged in a peer-to-peer manner between the involved parties.

Operations performed from crypto wallets are typically public and therefore known to those that have access to a node in the network; however, operations done from identity wallets are fully private and only known by the involved parties.

Communications

Crypto wallets do not usually implement a communication scheme between the involved parties for each transaction considering that these are performed through the blockchain network they use for each case.

In the case of identity wallets, operations are performed purely in a peer-to-peer manner without any third parties, which demands implementing peer-to-peer communication protocols and discovery and message mapping mechanisms between the parties.

It is important to note that, exceptionally, some crypto wallets do implement communication schemes between parties, but these are not used to process the operation in an on itself, but to exchange information required to prepare an operation that will be processed through a blockchain network (like exchanging addresses and amounts to transfer). Additionally, and given these are done with proprietary mechanisms, these are only applicable if both parties use the same wallet.