

Whitepaper Tango¹

Identidad Auto-Soberana: Fundamentos de un Nuevo Ecosistema
Digital Descentralizado

Buenos Aires, Argentina

V. 0.1
10/3/2022

¹ Nombre sujeto a discusión con la comunidad.

| | |
|--|-----------|
| Resumen | 4 |
| Introducción | 5 |
| ¿Por qué? La motivación | 5 |
| ¿Para qué? El propósito / Los beneficios esperados | 7 |
| ¿Cómo? El enfoque propuesto | 7 |
| ¿Qué? Lo que proponemos hacer | 8 |
| ¿Para quién? Audiencia | 9 |
| Trabajos preexistentes | 9 |
| W3C & Decentralized Identity Foundation | 9 |
| Sovrin Foundation | 9 |
| Hyperledger Aries & Ursa & Indy | 9 |
| Trust Over IP (ToIP) | 9 |
| Ethereum community (ENS / EIPs) | 9 |
| Proof Of Humanity | 9 |
| Estado de Colorado | 9 |
| Unión Europea | 9 |
| IDunion | 9 |
| LACChain ID | 9 |
| Conceptos de Identidad Auto-Soberana | 9 |
| Terminología | 10 |
| Identificador descentralizado o DID (por sus siglas en inglés) | 10 |
| Sujeto de un DID (DID Subject) | 10 |
| Métodos DID (DID Methods) | 10 |
| Documentos DID | 11 |
| Registros de datos verificables | 11 |
| DID resolvers y resolución de un DID | 11 |
| Arquitectura de la Solución | 11 |
| Nivel 1: Identificadores Descentralizados (DIDs) | 12 |
| Identificadores descentralizados, distintas implementaciones | 12 |
| DID Methods | 13 |
| DID Manager | 14 |
| Universal DID Resolver | 14 |
| Peer DID (did:peer) | 14 |
| TANGO DID (did:tdb) | 15 |
| Temas a profundizar en la fase de co-creación del whitepaper: | 17 |
| Nivel 2: billeteras y agentes digitales | 17 |
| Tipos de billeteras en la Web 3.0 | 17 |
| Billeteras y Agentes - terminología relacionada | 18 |
| Billeteras de Identidad - Arquitectura conceptual | 18 |

| | |
|--|-----------|
| Key Management Service (KMS) | 19 |
| Confidential Storage | 19 |
| DIDComm Messaging | 20 |
| Nodo web descentralizado (DWN) | 20 |
| Custodial vs Non-custodial | 21 |
| Recuperación de identidad | 21 |
| Buenas prácticas de seguridad | 21 |
| Nivel 3: intercambio y verificación de credenciales | 21 |
| Credenciales Verificables - Modelo de Datos | 22 |
| A continuación se enumeran los actores y las principales entidades dentro del modelo de Credenciales Verificables, tal como las define la especificación “Verifiable Credentials Data Model v1.1” del W3C. | 22 |
| Tipos de Credenciales Verificables | 24 |
| JSON-LD | 24 |
| JWT | 25 |
| ZKP-CL | 25 |
| Intercambio de Credenciales | 25 |
| Intercambio de Presentaciones | 26 |
| Wallet and Credential Interactions (WACI) | 27 |
| Tango VC | 27 |
| Nivel 4: aplicaciones | 28 |
| Tango en Nivel 4 | 30 |
| Biometría | 30 |
| Gestión y recupero de identidad | 30 |
| DIDs vs SCIDs | 30 |
| DID Document | 31 |
| Controller | 31 |
| Delegate | 32 |
| Administración de claves | 32 |
| Rotación de Claves | 32 |
| Pérdida y Recuperación del control sobre la Identidad | 33 |
| Custodial vs Non-Custodial | 33 |
| Guardianship | 34 |
| Estrategia de Adopción | 35 |
| Anexo I | 36 |
| Anexo II | 39 |
| Anexo III | 40 |
| Billeteras Cripto vs Billeteras de Identidad | 40 |
| Aspectos generales | 40 |

| | |
|---------------------------------|-----------|
| Claves Privadas y Firma Digital | 40 |
| Almacenamiento | 41 |
| Glosario | 43 |

Whitepaper Tango

Identidad Auto-Soberana: Fundamentos de un Nuevo Ecosistema Digital Descentralizado

1. Resumen

En el mundo digital es frecuente escuchar que la tenencia de datos otorga poder a quien los controla. La información identitaria, en especial, es quizás el registro de datos más trascendental relativo a un individuo u organización que existe. Sin embargo, hoy el acceso y uso de estos registros está fuera del control de los individuos a los que identifican. El poder y control está del lado de los entes que guardan la información, no sobre quienes refieren. El verdadero portador de la identidad queda relegado, sin noción de dónde se encuentra su información, quiénes tienen acceso a ella ni para qué es utilizada. Es por esto que, desde el GCBA, invitamos a la comunidad a co-crear un nuevo protocolo de identidad digital y auto-soberana con el usuario en el centro y al mando de su información.

El objetivo es construir un ecosistema de interacciones digitales sobre la base del protocolo de identidad digital auto-soberana consensuado con la comunidad. Buscamos facilitar la utilización del protocolo por parte de una masa crítica de usuarios para que luego el ecosistema tome vida propia de manera descentralizada. Nos imaginamos un nuevo paradigma que permita transacciones ágiles, simplificando procesos burocráticos, tanto entre actores privados como con actores gubernamentales. Hacerlo empoderará a los individuos, les dará control sobre su información y quién accede a ella. Los beneficios esperados incluyen una mayor soberanía de las personas sobre su información, una devolución del tiempo hoy gastado en trámites y burocracias a las personas y una reducción de costos transaccionales a las organizaciones.

2. Introducción

Las siguientes secciones describirán la motivación y el objetivo del proyecto. Utilizando lenguaje llano (no-técnico) se buscará captar la mayor audiencia posible, dando un panorama claro de la dirección y alcance del mismo.

2.1. ¿Por qué? La motivación

Nota: esta sección explicará en términos motivacionales el impulso del proyecto, poniendo foco en responder por qué es necesaria esta iniciativa, por qué orientarla al dominio de las identidades digitales, por qué es oportuno hacerla en este momento y por qué debe ser impulsada desde GCBA.

- Motivación: dar lugar a un nuevo paradigma en el cual las transacciones seguras sean ágiles; donde la verificación de documentación necesaria se realice de manera rápida, confiable y privada. Este paradigma se monta sobre el principio de que las personas son quienes controlan su identidad, y son ellas quienes deciden dónde está alojada su información y quién puede acceder a ella.
- Hoy en día, la información identitaria se gestiona según el paradigma de datos centralizados. Los registros y documentos son manejados por grandes organizaciones, gubernamentales y privadas, y son éstas quienes poseen la potestad absoluta para emitir, leer, modificar o eliminar información. Las personas no tienen control sobre su propia identidad ni pueden elegir quién tiene acceso a su información, y dependen directamente de un tercero que, como todos, siempre puede fallar. La situación actual lleva a que individuos incluso acepten condiciones sin conocer sus detalles o incluso mejores alternativas. La dependencia excesiva de unos pocos entes centralizados junto a la ampliamente conocida relevancia y poder de los datos en el siglo XXI vuelven al paradigma actual uno anticuado y riesgoso.
- En una interacción entre dos partes, conocer y verificar las identidades de las partes involucradas es condición necesaria para la construcción de un vínculo de confianza. Este vínculo es un aspecto fundamental de las relaciones sociales, comerciales y público-privadas. El primer paso de toda interacción es siempre verificar la identidad de las partes involucradas. Ya sea para registrar una nueva compañía, abrir una cuenta bancaria, anotarse en un club o contratar un servicio. Cuanto menos confianza tengan las partes, más riesgosa y menos deseable será la interacción.
- Estas transacciones también suelen requerir la presentación de documentación adicional, proceso que suele ser ineficiente y hoy ocupa mucho tiempo de las personas. ¿Qué si pudiéramos cambiar esta realidad? Hoy existe la tecnología

para hacerlo. Proponemos cambiar el proceso actual de presentar documentación por otro dónde los individuos únicamente autorizan a un interesado a verificar automáticamente el cumplimiento de condiciones a través de un canal seguro. Este cambio llevaría a una enorme reducción de tiempo en las transacciones, a la vez que elevaría su confiabilidad y seguridad. En un mundo hiperconectado donde lo digital ocupa cada vez más espacio en nuestras vidas, es fundamental que se generen mecanismos confiables, seguros, abiertos y ágiles para interactuar digitalmente con lo que nos rodea sin correr riesgos.

- La existencia de una identidad digital gobernada por las personas y respaldada por un estado posibilitará nuevos escenarios de uso y, entre otras cosas, elevará la confiabilidad y la sustentabilidad en el tiempo. Los mayores beneficios se darán cuando el ecosistema se expanda por la creación de identidades digitales por parte de organizaciones privadas, gane volumen por el incremento de interacciones entre privados y se nutra de la creación de nuevas aplicaciones para canalizar transacciones entre privados. Con este protocolo se abren infinitas puertas a terceros para que desarrollen nuevas tecnologías sostenidas en la identidad, ahora de forma segura, ágil y abierta.
- Si bien existen numerosos intentos de implementar sistemas de identidad digital y auto-soberana, el componente intrínsecamente comunitario de este concepto implica la necesidad de una masa crítica de usuarios para su real y efectivo funcionamiento. Es por esto que un estado, dada sus facultades institucionales, es probablemente el mejor organismo para dar un puntapié inicial a este nuevo paradigma, garantizando una adopción masiva a través de la implementación oficial del sistema. Una vez logrado esto, la sociedad en su conjunto se beneficiará, ya que será considerablemente más simple construir nuevos protocolos sobre o en paralelo a este.
- Por primera vez en la historia de la humanidad es posible crear marcos de confianza por medios puramente tecnológicos, gracias a los avances en el campo de la criptografía que aportan tecnologías como blockchain y zero-knowledge proofs, que permiten evolucionar hacia un paradigma dónde son los mismos individuos y la sociedad los garantes sociales y no unos pocos entes centralizados.
- Existe una comunidad de emprendedores y programadores argentinos que son reconocidos mundialmente por encontrarse a la vanguardia en el desarrollo de estas nuevas tecnologías, que si se complementará con un marco institucional y un accionar coordinado con los organismos del Estado, permitiría crear riqueza, empleos de alta calidad y un posicionamiento de liderazgo para nuestro país en un tema estratégico a nivel mundial.

2.2. ¿Para qué? El propósito / Los beneficios esperados

Nota: esta sección explicará cuál es el propósito del proyecto, poniendo foco en explicar sus impactos y los beneficios que generará en distintas dimensiones.

- Empoderar a los individuos y evolucionar hacia un paradigma dónde los individuos y la sociedad son los garantes sociales y no unos pocos entes centralizados. Un ecosistema abierto, confiable, seguro y transparente, montado sobre una arquitectura descentralizada, donde la confianza está respaldada por la red y no por entes centralizados.
- Potenciar las relaciones entre individuos y las instituciones (públicas y privadas) basadas en la confianza, con un resguardo tecnológico respaldado por los mismos usuarios. Al hacerlo se reemplaza un paradigma regido por fronteras y estructuras de control, por uno descentralizado y fluido.
- Agilizar los tiempos de transacción al simplificar el proceso de verificación de identidad y cumplimiento de requerimientos, devolviendo así tiempo a las personas y reduciendo costos para las empresas. Eliminar la necesidad de presentar documentación, reemplazandola por una sencilla autorización a un interesado de verificar automáticamente la tenencia de una credencial que acredite el cumplimiento de una condición o acceder a información.
- Habilitar nuevas formas de hacer negocios, compartir información y brindar acceso a servicios y recursos gubernamentales. Quién quiera podrá desarrollar y construir sobre la base ofrecida por este protocolo, abriendo innumerables puertas a nuevos proyectos y metodologías que involucren a la identidad como un factor fundamental.

2.3. ¿Cómo? El enfoque propuesto

Nota: esta sección explicará cómo se desarrollará y ejecutará el proyecto. El foco no estará puesto en las herramientas específicas a utilizar sino en las metodologías, protocolos y estándares a implementar.

- Un enfoque de co-creación abierta a todo aquel que quiera colaborar.
- Siguiendo los paradigmas de la identidad auto-soberana.
- Aprovechando las posibilidades que abren nuevos avances en el campo de la criptografía (Ej.: blockchain, ZKP, etc.).

- Aprovechando las capacidades del ecosistema de emprendedores y desarrolladores que existe en Argentina, tanto en el campo de la identidad auto-soberana, como en el campo de las tecnologías utilizadas en redes públicas, descentralizadas y no permissionadas.
- Aprovechando la capacidad de GCBA para impulsar la adopción masiva y lograr rápidamente una masa crítica de usuarios.

2.4. ¿Qué? Lo que proponemos hacer

Nota: esta sección se enfocará en describir el objeto, los elementos que serán contruidos o desarrollados como parte del alcance de esta iniciativa.

Debe dejar en claro que el objetivo no es desarrollar identidades digitales exclusivamente para su uso en la Ciudad de Buenos Aires ni para ningún otro contexto específico, sino sentar las bases de un protocolo que pueda ser utilizado o incluso replicado por quién sea, dónde sea.

El documento no hará énfasis en los stacks tecnológicos a utilizar, sino que planteará una solución, en la mayor medida posible, agnóstica a las herramientas empleadas para su implementación.

A priori, se identifican los elementos claves que son necesarios para cumplir con el propósito de la iniciativa:

- Un protocolo de identidad digital que permita facilitar y eficientizar la realización de trámites y todo tipo de acciones asociadas a la identidad, y a la vez de habilitar nuevas formas de compartir información y brindar acceso a servicios provistos por todo tipo de instituciones, públicas y privadas. Que sea descentralizado, público, no permissionado, abierto, extensible y capaz de interoperar con otros protocolos similares.
- Una masa crítica de identidades digitales que sirva como “bootstrapping” del ecosistema digital y le de suficiente relevancia como para atraer tanto a nuevos usuarios, como a nuevas instituciones y empresas, logrando de esta forma una dinámica que le permita sostenerse y crecer de manera autónoma.
- Una primera aplicación, patrocinada por el GCBA, que permita el acceso y la interoperabilidad entre todos los servicios que provee el gobierno a través de estándares comunes, de forma que los usuarios perciban beneficios concretos desde una etapa muy temprana.
- Un ecosistema pujante que extienda los servicios inicialmente brindados por el gobierno, para crear nuevas experiencias y mayores beneficios para las

personas y organizaciones que residan, transiten u operen en la Ciudad de Buenos Aires, que luego puedan replicarse en otras jurisdicciones o entornos a nivel local, regional y global.

2.5. ¿Para quién? Audiencia

Este documento apunta a servir como marco de referencia para agentes gubernamentales, proveedores de software, agentes comerciales, futuros emisores de credenciales privadas, legisladores, reguladores y público en general.

3. Trabajos preexistentes

Nota: esta sección hará referencia a trabajos preexistentes que se analizaron y de alguna manera se tomarán en cuenta en el diseño específico de la plataforma propuesta.

- 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. [Estado de Colorado](#)
- 3.8. [Unión Europea](#)
- 3.9. [IDunion](#)
- 3.10. [LACChain ID](#)

4. Conceptos de Identidad Auto-Soberana

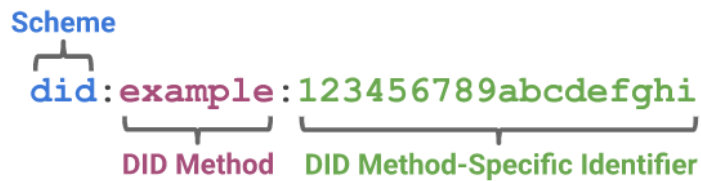
Nota: esta sección detallará todas las definiciones de términos relevantes que serán utilizados a lo largo del documento.

Según Sovrin, “identidad auto-soberana (Self-sovereign identity o SSI por sus siglas en inglés) es un término utilizado para describir el movimiento digital que reconoce que un individuo debe poseer y controlar su identidad sin la intervención de autoridades administrativas. La SSI permite a las personas interactuar en el mundo digital con la misma libertad y capacidad de confianza que en el mundo físico”². En 2016, Christopher Allen estableció los 10 principios para la identidad auto-gestionada que se han convertido en una referencia en el campo (ver [Anexo I](#)).

4.1. Terminología

Identificador descentralizado o DID (por sus siglas en inglés)

Un identificador persistente y globalmente único que no requiere una autoridad de registro centralizada porque se genera y/o registra utilizando plataformas descentralizadas (Ej.: blockchain). Mientras el formato genérico de un DID se define en la especificación [DID-CORE](#) del W3C, cada DID Method en particular define sus esquemas DID específicos.



Sujeto de un DID (DID Subject)

Según la especificación [DID-CORE](#) del W3C, el “sujeto de un DID” es, por definición, la entidad identificada por el DID. Tanto las personas, como las organizaciones, pero también las cosas, o incluso los conceptos, podrían ser el sujeto de un DID.

Métodos DID (DID Methods)

Los métodos DID son el mecanismo mediante el cual se crea, resuelve, actualiza y desactiva un tipo particular de DID y su documento DID asociado. Si bien cada método DID tiene libertad para definir los detalles de su implementación – por ejemplo: cada método DID puede definir e implementar su propio “Registro de Datos Verificables” – los implementadores de un método DID deben respetar las especificaciones que se definen en la sección “[Methods](#)” de la especificación [DID-CORE](#) del W3C.

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

Documentos DID

Los “documentos DID” contienen información asociada con un DID. Por lo general, expresan métodos de verificación, como claves públicas de criptografía asimétrica y “end-points” a servicios relevantes para las interacciones con el sujeto DID. Las propiedades genéricas admitidas en un documento DID se especifican en la sección “[Core Properties](#)” de la especificación [DID-CORE](#) del W3C.

Registros de datos verificables

Un sistema que permite registrar los DIDs y la información necesaria para producir sus “documentos DID” asociados. Estos registros típicamente utilizan algún tipo de almacenamiento descentralizado que permita la verificación de los datos sin necesidad de tener una autoridad de registro (Ej.: blockchain).

DID resolvers y resolución de un DID

Un “DID resolver” es un componente con una interfaz web estándar y provisto por cada método DID que toma un DID como entrada y produce un documento DID conforme al estándar [DID-CORE](#) como salida. Este proceso se denomina resolución del DID. Los pasos para resolver un tipo específico de DID están definidos por la especificación de cada método DID en particular.

5. Arquitectura de la Solución

Nota: en esta sección se describe la arquitectura de la solución, incluyendo la dimensión de tecnología, pero también la dimensión del governance. Esta descripción busca ser agnóstica respecto de implementaciones tecnológicas particulares, apoyarse en estándares de la industria y enfocarse en describir los requerimientos para cada componente de la arquitectura.

La arquitectura propuesta toma como base el modelo desarrollado por la fundación “[Trust Over IP](#)”³, pero con algunas extensiones y modificaciones que se consideran necesarias, por un lado para adaptar dicho modelo a las necesidades específicas de esta iniciativa, pero a la vez para incluir conceptos originados en otros trabajos preexistentes dentro del campo de la identidad digital que enriquecerán la arquitectura propuesta y permitirán ampliar su alcance a un público más grande y a una mayor diversidad de escenarios de uso.

³ [Trust Over IP model](#)

El modelo de [ToIP](#) consolida mucho del conocimiento y los componentes tecnológicos generados en [trabajos preexistentes](#) dentro del campo de la identidad digital auto-soberana, dado que la Fundación ToIP trabaja en estrecha colaboración con otras organizaciones de desarrollo de estándares, fundaciones y consorcios de la industria, para combinar sus estándares abiertos, arquitecturas y protocolos en un stack completo y coherente que permita crear una “infraestructura de confianza digital” a escala de Internet.

El modelo de [ToIP](#) está organizado en cuatro niveles, cada uno de los cuales tiene una dimensión de governance y una dimensión tecnológica, y se enfoca en resolver una problemática específica:

- Nivel 1: [identificadores descentralizados \(DIDs\)](#)
- Nivel 2: **billeteiras y agentes digitales**
- Nivel 3: **intercambio y verificación de credenciales verificables**
- Nivel 4: **ecosistemas de confianza digital**

En cada uno de los 4 niveles del modelo “ToIP” existen especificaciones y tecnologías que permiten su implementación y surgen definiciones de solución que deben ser abordadas. A continuación se presentan brevemente tanto las tecnologías a utilizar en cada nivel, como las definiciones críticas que es necesario abordar para lograr un diseño que responda a las necesidades específicas de esta iniciativa.

5.1. Nivel 1: Identificadores Descentralizados (DIDs)

En este nivel se aborda toda la problemática relacionada con un nuevo tipo de identificadores descentralizados, persistentes, globalmente únicos e interoperables, que se generan y verifican criptográficamente y por lo tanto no requieren ni autoridades de registro centralizadas, ni proveedores de servicios centralizados.

En este nivel se implementa un conjunto de servicios públicos y abiertos, necesarios para crear, administrar, resolver y verificar los identificadores descentralizados, que constituyen las raíces criptográficas sobre las que luego se apoya toda la construcción de la “identidad digital auto-soberana”.

Identificadores descentralizados, distintas implementaciones

En los últimos años se han desarrollado distintas aproximaciones a la problemática de identificadores únicos y descentralizados. Solo para citar alguno de ellos, podemos nombrar los siguientes:

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

- Ethereum Name Service ([ENS](#))

Si bien todas estas aproximaciones cubren, en alguna medida, los requerimientos de nuestra iniciativa, nuestra propuesta es implementar inicialmente el nivel 1 del modelo siguiendo la especificación [DID-CORE](#) del W3C, dado que:

- Por un lado brinda mejor cobertura a los requerimientos específicos de esta iniciativa y, por otro lado, porque es la que se encuentra más avanzada y la que está siendo más ampliamente adoptada por distintos gobiernos, organismos multilaterales y ecosistemas digitales alrededor del mundo.
- Adicionalmente, muchas de las otras aproximaciones están confluyendo hacia la especificación [DID-CORE](#) del W3C, lo cual facilitará la interoperabilidad en un futuro cercano. Por ejemplo: por el lado de KERI, este ya fue incorporado como un grupo de trabajo en la [Decentralized Identity Foundation](#) y se está creando un nuevo método DID bajo el nombre de [did:keri](#), y por el lado de ENS, [Veramo](#) ([ExuPort](#)) está implementando otro método DID ([did:ens](#)) que permite generar dinámicamente un DID y su correspondiente DID Document para cada nombre publicado en ENS utilizando los datos almacenados en dicho registro y lo ha registrado como did:ens en el [W3C DID registry](#)

DID Methods

Los [métodos DIDs](#) representan el componente central en la implementación de este nivel del modelo, y una de las decisiones más críticas en este sentido es la definición de qué métodos DID serán soportados por la plataforma para cada escenario en particular, concretamente: qué métodos DIDs serán soportados para administrar DIDs generados en esta plataforma y qué métodos DID serán soportados sólo en modalidad resolución (sólo lectura) para efectos de compatibilidad e interoperabilidad con otras plataformas similares.

Es importante destacar que no hay una única implementación de un método DID, sino múltiples implementaciones que cumplen con la especificación [DID-CORE](#) y que están optimizadas y personalizadas para distintos requerimientos. A la fecha, hay más de 70 métodos DID registrados en el [W3C DID registry](#), y seguramente ese número seguirá creciendo aceleradamente en el futuro próximo.

Si bien, en teoría, las plataformas de identidad digital descentralizada deberían poder manejar todas las implementaciones de métodos DID sin un esfuerzo adicional, en la práctica, dado que [DID-CORE](#) es un estándar que permite ciertas extensiones, cada método DID presenta particularidades y su integración a la plataforma requiere un esfuerzo considerable.

DID Manager

En este componente, es donde serán registrados los métodos DID soportados por la plataforma en “modalidad de gestión”, es decir aquellos métodos DID que estarán habilitados para crear, actualizar y desactivar los DIDs en esta plataforma.

En un principio el DID Manager implementará el método Peer DID (did:peer), para manejar interacciones privadas entre dos partes y un método DID propio de la plataforma, que será público y basado en un [Registro de Datos Verificables](#), para ser utilizado en situaciones donde existe un número desconocido de partes (por ejemplo, el público global o algún subconjunto del mismo).

Más abajo, en esta sección, se brindan detalles de los dos métodos DID que serán soportados desde el inicio por nuestra plataforma.

Universal DID Resolver

Si bien la Decentralized Identity Foundation mantiene un servicio público y abierto, conocido como Universal Resolver (dev.uniresolver.io), cuyo propósito es brindar un único punto de acceso a los [DID Resolvers](#) provistos por cada uno de los métodos DID auto-registrados con dicho servicio, una práctica común, debido a las particularidades que presentan los diferentes métodos DIDs, es que cada plataforma implemente su propio Universal Resolver, para brindar, no solo un único punto de acceso a los resolvers, sino además homogeneizar la interacción con los métodos DID soportados por el Universal Resolver, ocultando la complejidad a los usuarios que se derivan de las particularidades de cada método DID.

En este componente, es donde serán registrados los métodos DID soportados por la plataforma en “modalidad solo de resolución”. En un principio, sólo se implementará soporte para el método DID que será creado específicamente para esta plataforma, luego, en forma gradual, se podrán ir registrando métodos DID adicionales para ampliar la interoperabilidad y compatibilidad con DID generados en otras plataformas de identidad digital descentralizada. El método Peer DID no se incluye en el Universal Resolver, porque su resolución es privada entre las partes y solo las partes tienen acceso a los DID Documents generados por ese método.

Peer DID (did:peer)

Este método tiene la particularidad de que no requiere un [Registro de Datos Verificables](#), dado que está optimizado para situaciones donde solo intervienen dos partes que se conocen y tienen relación directa, por lo que está destinado a ser económico, rápido, escalable, seguro y muy privado.

Puede decirse que Peer DIDs son a los DID públicos basados en un [Registro de Datos Verificables](#), lo que construcciones como Ethereum Plasma, los State-Channels o

Lighting Network son para las transacciones on-chain, es decir, mueven la mayor parte de las interacciones off-chain, para aumentar la escalabilidad y la privacidad, pero ofrecen opciones para volver a conectarse on-chain según sea necesario.

Para más información sobre el método Peer DID, puede consultarse la especificación en el siguiente link: <https://identity.foundation/peer-did-method-spec/>

TANGO DID (did:tdb)

Para cubrir situaciones que requieran crear y administrar DIDs dentro de nuestra plataforma y en escenarios que involucren a tres o más partes (Ejemplo: credenciales verificables) se creará un método DID propio de nuestra plataforma, el cual será registrado formalmente en el [W3C DID registry](#) para que sea reconocido a nivel global.

La creación de un método DID propio permitirá ajustar sus características a los requerimientos específicos de esta iniciativa, en particular, se pondrá especial atención a crear un mecanismo de mitigación de spam y ataques de denegación de servicio que sea apropiado para una implementación de esta naturaleza, concretamente, un mecanismo que sea eficaz para mitigar este tipo de ataques, pero que a la vez no tenga costos por transacción elevados, particularmente en situaciones donde se deba incorporar un volumen alto de identidades genuinas en un período corto de tiempo, como podría ser en la carga inicial de las identidades cuando se incorpore, por ejemplo, una nueva jurisdicción.

La creación de este método DID no será realizada desde cero, sino tomando como base las definiciones y los componentes tecnológicos disponibles de algún otro método DID que haya sido probado en experiencias anteriores y se ajuste a las necesidades propias de esta iniciativa. Existen al menos tres iniciativas que tienen un track record sólido y que podrían servir como base para crear nuestro propio método DID:

- Sovrin: creado por la [Sovrin Foundation](#) quien a su vez es uno de los miembros fundadores de la Decentralized Identity Foundation y uno de los actores más influyentes en los desarrollos que se realizaron dentro del marco del DIF/W3C.
- ETHR: creado originalmente por uPort, una empresa del grupo Consensys, otro de los miembros fundadores de la Decentralized Identity Foundation y que también tuvo gran influencia que se realizaron dentro del marco del DIF/W3C.
- Sidetree: es una iniciativa que surgió ya dentro de la Decentralized Identity Foundation que, por tratarse de una iniciativa más moderna, no solo aprovecha los aprendizajes de experiencias previas en iniciativas como Sovrin y ETHR, sino también los avances que hubo en los últimos años en los protocolos blockchain, particularmente los referidos a protocolos de segundo nivel.

De estas tres iniciativas, consideramos que SOVRIN, aún cuando es una experiencia muy valiosa, no puede ser tomada como base porque requieren: o bien montarse sobre la red Sovrin, o desplegar una nueva red usando Hyperledger Indy, y en ambos casos serían redes permissionadas, lo cual colisiona con uno de los principios fundamentales de nuestra iniciativa de ser pública, abierta y no-permisionada.

En función de eso, las dos alternativas a evaluar serían:

- A. Desplegar el método DID utilizando ETHR sobre un protocolo de nivel 2 en alguna red que sea EVM compatible, para tener niveles de escalabilidad y costos compatibles con los requerimientos de esta iniciativa.
- B. Desplegar el método DID utilizando Sidetree como base en una red blockchain y una red IPFS que deberán ser definidas al momento de realizar la especificación detallada de la implementación.

Cada una de estas dos opciones tiene sus ventajas y desventajas, que deberán ser estudiadas en detalle antes de definir cuál es la opción más conveniente para esta iniciativa. De manera muy resumida, podemos decir que:

- **ETHR**, por el simple hecho de ser una implementación más antigua, tiene muchas más implementaciones, tiene abundante documentación y cuenta con un ecosistema más amplio de desarrolladores con experiencia. Por otra parte, por la misma razón de haber sido pionera, presenta algunos problemas estructurales en su diseño, lo cual limita su funcionalidad y su desarrollo a futuro. Un aspecto favorable de ETHR es que no requiere el despliegue de nodos de ningún tipo, solo desplegar los smart contracts asociados al método en alguna red compatible con EVM.
- **Sidetree**, al ser una implementación más moderna, que recoge experiencias anteriores y avances en la tecnología de base, tiene un diseño mucho más eficiente y con mayor potencial de desarrollo a futuro, está siendo apadrinada directamente por la Decentralized Identity Foundation y siendo adoptada por actores muy influyentes (Ej.: Microsoft). A la vez, por las mismas razones, no cuenta con tantas implementaciones, la documentación es incompleta y el ecosistema de desarrolladores con experiencia es limitado. Una consideración importante a tener en cuenta con Sidetree es que, aunque es un protocolo que se ancla en una red blockchain subyacente y aprovecha el mecanismo de consenso de la misma, requiere el despliegue de nodos tanto para el protocolo Sidetree, como para la red IPFS que se utilice para almacenar la información, esta característica puede ser una ventaja en algunos casos, pero requiere un mayor esfuerzo para crear el ecosistema de nodos que darán soporte a la red.

Temas a profundizar en la fase de co-creación del whitepaper:

- Mecanismos de recuperación de identidad
- Rotación de claves y resolución de DIDs
- Proof of Existence
- Buenas prácticas de seguridad

5.2. Nivel 2: billeteras y agentes digitales

Este nivel aborda la problemática de las billeteras y agentes digitales necesarios para aceptar, almacenar e intercambiar credenciales digitales sobre protocolos estándares de comunicación entre pares (P2P). El objetivo de este nivel es crear un espacio seguro y privado para todas las interacciones digitales que puedan ocurrir ya sea entre individuos, empresas, gobiernos o cualquier tipo de "cosa" con la que podamos interactuar digitalmente a través de una billetera/agente digital.

Tipos de billeteras en la Web 3.0

Las billeteras físicas tradicionalmente se utilizan para almacenar una variedad de activos personales, como efectivo, tarjetas de crédito, licencia de conducir, seguro médico y tarjetas de presentación. En la actualidad, también contamos con una amplia variedad de billeteras digitales para almacenar y acceder a versiones digitales de estos mismos activos, y cada día surgen más opciones en el mercado. Sin embargo, cada billetera representa los datos e implementa sus capacidades de manera diferente, lo cual restringe significativamente la interoperabilidad y en muchos casos genera una dependencia con el proveedor de la wallet.

En el contexto de la Web 3.0 existen dos tipos de billeteras que resultan relevantes:

- Billeteras utilizadas para manejar **activos digitales** (Ej.: Criptomonedas, NFTs)
- Billeteras utilizadas para manejar **credenciales verificables** (Ej.: licencias de conducir, títulos universitarios).

Si bien ambos tipos de billeteras se utilizan para implementar aplicaciones que hacen uso de arquitecturas descentralizadas (Ej.: redes blockchain), sus características son significativamente diferentes dado el hecho de que han sido diseñadas para satisfacer los requerimientos propios de cada uno de los escenarios de uso en que se enfocan (activos digitales vs identidad digital).

Dado que Tango se enfoca a la problemática de Identidad Auto Soberana, el término “billetera” se utilizará para referirnos al tipo de billeteras que se utiliza para manejar la problemática de identidad, pero, dado que existe cierta superposición entre las audiencias de Activos Criptográficos e Identidad Auto Soberana, y además porque es posible que en el futuro aparezcan billeteras que sean capaces de manejar ambos escenarios de uso, en el “Anexo III” de este documento incluimos un breve análisis

comparativo de las características fundamentales de cada uno de estos tipos de billeteras.

Billeteras y Agentes - terminología relacionada

Dado que no existe total uniformidad respecto de la terminología que es utilizada en las distintas comunidades y proyectos que abordan la problemática de la identidad Auto Soberana, en particular respecto del significado de los términos Billetera y Agente, definiremos en esta sección lo que entendemos por cada uno de esos términos dentro del proyecto Tango.

Billetera: es un módulo de software y, opcionalmente, un módulo de hardware asociado, para almacenar y acceder de forma segura a claves privadas, credenciales y otros secretos o materiales confidenciales pertenecientes a un sujeto. Una billetera a menudo es facilitada o controlada por un agente.

Agente: un agente es un módulo de software que actúa como representante de un sujeto (generalmente una persona), que controla el acceso a una billetera y otros almacenamientos privados de dicho sujeto y que puede facilitar las interacciones con otros sujetos mediante el intercambio de mensajes. Un agente puede estar hospedado en diferentes ubicaciones en una red (nube versus local).

Billetera de Identidad: dentro del contexto de Tango utilizaremos este término para referirnos a la entidad lógica que combina todas las capacidades que tienen las billeteras y los agentes según las definiciones dadas en los dos párrafos anteriores. Esta entidad es en definitiva la que utilizan los distintos sujetos – individuos, organizaciones o cosas – para ejecutar las distintas operaciones relacionadas con su identidad Auto Soberana.

Billeteras de Identidad - Arquitectura conceptual

En esta sección se describen los principales componentes que a nuestro criterio deben incorporarse a la arquitectura de una Wallet de Identidad, el cual trata de sintetizar y homogeneizar las descripciones y la terminología que utilizan distintos grupos y proyectos que abordan este tema como parte de la problemática de Identidad Auto Soberana. Para esto, dado que no existe total acuerdo ni en los componentes, ni en la terminología utilizada para describir la arquitectura de una Billetera de Identidad en dichos grupos y proyectos, hemos tomado como base las especificaciones que se están siendo desarrolladas por el W3C y la Decentralized Identity Foundation y las complementamos con elementos que provienen de los otros grupos o proyectos y que consideramos valiosos y complementarios.

Key Management Service (KMS)

Esta es la capacidad más básica y fundamental en una Billetera de Identidad, dado que es la que permite generar y almacenar pares de claves públicas y privadas, proteger las claves privadas y firmar digitalmente utilizando diversidad de algoritmos criptográficos. En algunos casos además puede soportar esquemas de múltiples firmas, normalmente conocidos como “multisig”.

Esta capacidad se implementa de manera muy similar en las Billeteras de Identidad y en las billeteras utilizadas para las aplicaciones de manejo de activos digitales (Ej.: criptomonedas), al punto tal que muchas implementaciones se realizan utilizando las mismas primitivas y librerías criptográficas, e incluso ciertas “Billeteras Cripto” pueden utilizarse para cubrir estas necesidades dentro de una Billetera de Identidad. Por ejemplo: las llamadas billeteras de hardware o billeteras como Metamask podrían ser utilizadas para implementar esta capacidad dentro de una Billetera de Identidad.

Confidential Storage

Un Almacenamiento Confidencial, tal como lo define el borrador de la [especificación de confidential storage](#) que está siendo elaborada por la Decentralized Identity Foundation, es un mecanismo diseñado poniendo especial énfasis en la privacidad de la información y que permite almacenar, indexar y recuperar datos cifrados en un proveedor de almacenamiento de forma tal que dicho proveedor de almacenamiento no pueda ver, analizar, agregar o revender esos datos. Adicionalmente garantiza que los datos sean portátiles y estén protegidos contra violaciones de datos (data breaches) que pueda sufrir el proveedor de almacenamiento.

Dicha especificación se limita a detallar los requerimientos para este componente de manera agnóstica respecto de los detalles de implementación, para permitir que diversidad de implementaciones en diferentes tipos de dispositivos y ubicaciones en una red. De esta forma, un “confidential storage” implementado en un dispositivo móvil o en un cloud provider tendrán capacidades similares y las mismas interfaces de operación, aunque la infraestructura subyacente sea totalmente diferente. Esto permite, por un lado la portabilidad de los datos entre distintas implementaciones, pero a la vez que un sujeto – individuo, organización o cosa – pueda tener su información replicada en distintos sitios para prevenir la pérdida de acceso a sus datos si existe un problema con alguna de las réplicas.

Típicamente, el acceso a un “confidential storage” se realiza a través de uno o varios “Nodos Web Descentralizados” (aka: Identity Hubs), otro componente clave en la arquitectura de una Billetera de Identidad y que será descrito más adelante en este documento.

DIDComm Messaging

Si bien en la actualidad ya existen mecanismos robustos para realizar comunicaciones seguras, todos ellos dependen de construcciones centralizadas, en su mayoría están ligados a un transporte específico y fueron diseñados para cubrir los requerimientos de la web 2.0, donde se asume que las interacciones entre partes son facilitadas a través de servidores web altamente disponibles y operados por expertos, que a la vez imponen términos y condiciones que no son compatibles con los requerimientos de privacidad, interoperabilidad e independencia que plantea la web 3.0.

En ese contexto, DIDComm propone una nueva alternativa, que por un lado reutiliza mucha de la tecnología existente en materia de comunicaciones seguras, pero que a la vez resuelve las limitaciones de los actuales mecanismos en esa materia.

El propósito de DIDComm es proveer un nuevo mecanismo de comunicaciones seguras y privadas, que se apalanca sobre el diseño descentralizado de los DIDs para crear una infraestructura de comunicaciones realmente peer-to-peer, que no sea dependiente de ningún servicio centralizado, que pueda funcionar a través de una variedad de transportes de comunicación y en escenarios donde la disponibilidad de las comunicaciones puede ser intermitente, como ocurre, por ejemplo, con usuarios individuales que operan a través de dispositivos móviles. Todas características necesarias para cumplir con los requerimientos de la web 3.0.

Actualmente ya está disponible la [versión 2 de la especificación del protocolo DIDComm](#), existe una buena diversidad de librerías que la implementan y un muy alto nivel de adopción en proyectos de Identidad Auto Soberana alrededor del mundo, lo cual lo ha convertido en un estándar de facto para cubrir los requerimientos de comunicaciones entre pares propios de la WEB 3.0.

Nodo web descentralizado (DWN)

Un “[Nodo Web Descentralizado](#)” (aka: “Identity Hub”), también conocido como DWN, por sus siglas en inglés, es un mecanismo que facilita la transmisión de mensajes en modalidad peer-to-peer entre sujetos – ya sean individuos, organizaciones y cosas – así como también la gestión del almacenamiento de datos públicos o privados relacionados con un identificador descentralizado (DID) dado.

Los nodos web descentralizados son una construcción de almacenamiento de datos con una arquitectura de malla (mesh) que permite que un sujeto tenga múltiples nodos que se sincronizan entre sí para mantener un mismo estado de información, lo que permite al sujeto proteger y administrar sus datos, así como también realizar transacciones con otros sujetos sin depender de la ubicación o de infraestructuras, interfaces o mecanismos de enrutamiento dependientes de un proveedor específico.

Es importante destacar que el DWN no realiza la transmisión de los mensajes, ni administra el almacenamiento, sino que actúa como un facilitador, como una interfaz pública accesible desde la web para darle presencia on-line a todos los actores involucrados en flujos relacionados con el intercambio de credenciales. La gestión en sí misma del almacenamiento de información es realizado por la capacidad de Confidential Storage, descrita anteriormente en esta sección del documento y la transmisión de los mensajes se realiza utilizando el protocolo DIDComm también descrito anteriormente en este documento.

El DWN es particularmente importante en el caso de individuos o cosas, dado que típicamente no cuentan con una presencia on-line permanente en la web que les permita recibir interacciones iniciadas desde otros DWN, propios o de terceros. Por ejemplo: un individuo que sólo utiliza una Billetera de Identidad en un dispositivo móvil no podría ser contactado en forma directa desde otro sujeto que requiera iniciar un flujo peer-to-peer para intercambiar credenciales con él. Para mayores detalles sobre este tipo de interacciones, puede consultarse la sección “[topology](#)” en el [borrador de la especificación de DWN](#) que está siendo desarrollada por el Decentralized Identity Foundation.

Billeteras individuales vs organizacionales

Custodial vs Non-custodial

Recuperación de identidad

Buenas prácticas de seguridad

5.3. Nivel 3: intercambio y verificación de credenciales

El nivel tres del modelo de ToIP habilita un marco de “**confianza humana**” – en forma de afirmaciones verificables acerca de entidades, atributos y relaciones – el cual complementa al marco de “**confianza criptográfica**” habilitado por los niveles uno y dos. El nivel cuatro, como veremos más adelante, extiende y complementa este marco de “**confianza humana**” con los modelos y políticas de confianza propias y específicas de cada ecosistema de confianza digital.

Para lograr su propósito, este nivel facilita el intercambio de credenciales verificables y pruebas criptográficas entre emisores, titulares y verificadores, apoyándose en los formatos de intercambio de datos, protocolos de credenciales verificables y el modelo del [triángulo de confianza de las credenciales verificables](#), lo cual permite establecer relaciones de confianza transitivas para las interacciones por canales digitales, de forma interoperable y a escala global entre cualquiera de los tres actores que define dicho modelo: emisores, titulares y verificadores.

El “modelo de confianza” descrito en la especificación “[Verifiable Credentials Data Model v1.1](#)” enumera los supuestos acerca de las relaciones de confianza que se asumen como válidas entre los distintos actores y que dan sustento al modelo como tal. Por ejemplo: “el verificador confía en el emisor de una credencial”.

Credenciales Verificables - Modelo de Datos

El [modelo de datos de VC](#), definido por el W3C, es un formato de datos universal que permite que cualquier entidad realice “afirmaciones verificables” (Verifiable Claims) sobre otra entidad, para describir una cualidad o cualidades, propiedad o propiedades que establecen la existencia y unicidad de la entidad sobre la cual se realizan dichas afirmaciones.

El objetivo fundamental del estándar de Credenciales Verificables es habilitar el equivalente digital de las credenciales físicas que almacenamos en nuestras billeteras físicas y que utilizamos en el día a día para proporcionar prueba de nuestra identidad y/o de nuestros atributos.

El modelo de datos de VC, proporciona un mecanismo común para la implementación interoperable de credenciales digitales que son criptográficamente seguras, a prueba de manipulaciones, respetuosas de la privacidad y verificables por mecanismos digitales. Este modelo permite empaquetar credenciales, firmarlas criptográficamente y generar pruebas criptográficas asociadas de forma estandarizada. Esto habilita la creación de ecosistemas que comparten juegos de credenciales interoperables que pueden ser procesadas y comprendidas por sistemas dispares dentro del ecosistema.

A continuación se enumeran los actores y las principales entidades dentro del modelo de Credenciales Verificables, tal como las define la especificación “[Verifiable Credentials Data Model v1.1](#)” del W3C.

Sujeto: es una entidad sobre la cual se hacen afirmaciones (claims). Los sujetos pueden ser personas u organizaciones, pero también animales, cosas e incluso conceptos. Un individuo, una empresa, un auto o un animal son ejemplos de sujetos. El titular (holder) de una credencial verificable puede o no ser el sujeto de dicha credencial. Por ejemplo: un padre (el titular o holder) puede tener las credenciales verificables de su hijo (el sujeto), o el dueño de una mascota (el titular o holder) puede tener las credenciales verificables de su mascota (el sujeto).

Titular (holder): un rol que un sujeto desempeña cuando posee una o más credenciales verificables y generar presentaciones verificables a partir de ellas.

Emisor (issuer): un rol que desempeña una entidad que realiza afirmaciones (claims) sobre uno o más sujetos, que crea credenciales verificables a partir de estas afirmaciones y que transmite dichas credenciales a sus titulares. Los emisores, por ejemplo, pueden ser: empresas, organizaciones sin fines de lucro, asociaciones comerciales, gobiernos e incluso individuos.

Verificador: un rol que realiza una entidad al recibir una o más credenciales verificables, opcionalmente dentro de una presentación verificable, para su procesamiento. Los verificadores pueden ser, por ejemplo: empleadores, personal de seguridad, sitios web o individuos.

Afirmación (Claim): representa una calificación, logro, cualidad o información sobre los antecedentes de un sujeto, como ser, por ejemplo, un nombre, una identificación gubernamental, una dirección particular o un título universitario. Un sujeto puede ser un individuo, una organización o una cosa.

Credenciales: es un conjunto de una o más afirmaciones (claims) realizadas por la misma entidad respecto del mismo sujeto. También pueden incluir un identificador y metadatos para describir las propiedades de la credencial en sí misma, como el emisor, la fecha y hora de vencimiento, una imagen representativa, una clave pública para usar con fines de verificación, el mecanismo de revocación, etc.

Credenciales Verificables: es una credencial, tal como se definió en el párrafo anterior, pero que incluye material criptográfico que permite detectar la manipulación de sus datos y probar fehacientemente quién la emitió.

Presentaciones Verificables: contienen datos de una o más credenciales verificables empaquetados de tal manera que la autoría y la integridad de los datos es verificable. También pueden estar conformados por datos que son derivados de credenciales verificables cuya validez y autoría pueden ser verificadas criptográficamente, generalmente utilizando algoritmos de Zero Knowledge Proofs. Los datos de una presentación a menudo tratan sobre el mismo sujeto, pero pueden haber sido emitidos por varios emisores. Las presentaciones verificables deben incluir una prueba criptográfica, típicamente una firma digital, que permita verificar que quien está realizando la presentación es el titular de la credencial (holder).

Registro de datos verificables: un sistema que media en la creación y verificación de identificadores, claves y otros datos relevantes – como esquemas de credenciales verificables, registros de revocación, claves públicas de emisores, etc – que podrían ser necesarios para usar credenciales verificables. Estos registros pueden ser implementados utilizando tecnologías de registros descentralizados (Ej.: blockchain), pero esto no es mandatorio, también podrían ser implementados utilizando tecnologías centralizadas.

Tipos de Credenciales Verificables

Esta sección presenta las diferentes variantes de Verificables Credentials (VC) que describe la especificación “[Verifiable Credentials Data Model v1.1](#)” del W3C. También explica brevemente sus diferencias y presenta el trilema de interoperabilidad que surge debido a la existencia de tres opciones diferentes de VCs. Finalmente, recomienda la adopción del formato de VC más nuevo dado que este apunta a satisfacer los requerimientos de un mayor número de partes interesadas.

¿Por qué importa esto? Sin la convergencia a un formato de VC estandarizado, no habrá interoperabilidad funcional en todo el ecosistema. Si los creadores de aplicaciones implementan la criptografía relacionada con las VC utilizando bibliotecas y métodos incompatibles, y los datos subyacentes tienen distintas propiedades de legibilidad, no se logrará la interoperabilidad.

Lo que tienen en común los diferentes métodos es que los emisores los usan para empaquetar “claims” sobre un sujeto. La entidad emisora luego usa criptografía para sellar la credencial y este sello proporciona un mecanismo para que otras entidades (los verificadores) verifiquen las firmas criptográficas para ver si la credencial tiene integridad en función de las claves públicas del emisor.

En lo que se diferencian es en los formatos que utilizan para los “claims” dentro de las credenciales y las presentaciones verificables, así como también en tipo de pruebas (proofs) que utilizan para sellar las credenciales y/o las presentaciones verificables.

A continuación se presentan las tres variantes de VC que se describen en la especificación “[Verifiable Credentials Data Model v1.1](#)” del W3C. Todas tienen más de una implementación crítica en varias etapas de producción.

JSON-LD

Esta variante utiliza un formato basado en JSON-LD asegurado con “Linked Data Signatures” o firmas BBS+ para habilitar Zero Knowledge Proofs (ZKP) y es impulsada mayormente por el ecosistema que impulsa el paradigma de Linked Data y Semantic Web.

La variante que combina JSON-LD ZKP con BBS+ está ganando mucha popularidad, dado que habilita una forma de usar JSON-LD con capacidades de ZKP, cosa que no era posible antes de la aparición de BBS+. El beneficio de usar este enfoque es, ante todo, que cumple totalmente con la especificación de VC tal como existe en la actualidad. Además, debido a que sus firmas y pruebas son autodescriptivas y autocontenidas, no requieren ninguna configuración adicional ni dependencias externas. Este enfoque permite el uso simple y estandarizado de JSON-LD, para aprovechar los vocabularios de datos abiertos, y al mismo tiempo conserva las características de preservación de la privacidad, como Selective Disclosure o ZKP, los que tradicionalmente venían con su propio conjunto de limitaciones y concesiones. Con esta variante ya no es necesario elegir entre la interoperabilidad basada en estándares o la criptografía que preserva la privacidad: se pueden tener ambas.

JWT

Esta variante utiliza un formato JSON asegurado con JSON Web Signatures, específicamente en forma de JSON Web Tokens (JWT) y es impulsada mayormente desde el ecosistema de proveedores de soluciones para Identity and Access Management (IAM).

Este ecosistema tiende a visualizar al “login” como la base del protocolo de intercambio de VC y apunta a realizar una implementación reutilizando el stack de tecnología que usan actualmente: JSON Object Signing and Encryption (JOSE) y OpenID Connect.

Claramente es una opción muy robusta para implementar el caso de uso de Login a sitios web utilizando Self-Sovereign-Identity como proveedor de identidad, pero no es la opción más apropiada para otros escenarios de uso más propios de la Web 3.0.

ZKP-CL

Esta variante utiliza ZKP con firmas del tipo Camenisch-Lysyanskaya (ZKP-CL).

Dado que es un formato que está íntimamente relacionado con Hyper Ledger Indy, no será considerado dentro del proyecto Tango porque este busca ser agnóstico respecto de la red Blockchain que utilice como anclaje.

Intercambio de Credenciales

La forma en que los “agentes” de los emisores, los titulares y los verificadores deben realizar el intercambio de credenciales entre sí es otra de las características que define el modelo ToIP en el nivel tres con el objetivo de habilitar la interoperabilidad funcional a través de todo el ecosistema.

Dado que existen múltiples especificaciones que abordan los distintos aspectos de la problemática del intercambio de credenciales verificables y, en algunos casos, existe más de una aproximación para resolver un mismo aspecto, en esta sección se describen brevemente los distintos aspectos que abordan dichas especificaciones y se propone una alternativa para aquellos casos donde existan divergencias en la comunidad sobre cómo implementar un aspecto en particular.

Intercambio de Presentaciones

El problema más básico para lograr la interoperabilidad en el intercambio de credenciales es definir un mecanismo estándar para facilitar los dos pasos principales en un intercambio de este estilo: una forma para que los “verificadores” describan los requisitos de prueba y para que los “titulares” (holders) describan las presentaciones de prueba alineadas con dichos requisitos.

Para abordar estas necesidades, la especificación “[Presentation Exchange v1.0.0](#)” define un protocolo de intercambio de datos que consta de dos formatos de datos: “Definición de Presentación” o “Presentation Definition” y “Envío de Presentación” o “Presentation Submission”.

La “Definición de Presentación” es el formato de datos que utilizan los “verificadores” para articular los requisitos de prueba que deben ser cumplidos por los “titulares” (holders). Entre otras cosas, este formato define el tipo de credenciales que son requeridas y las opciones que son aceptadas para cada tipo (Ej.: se requiere presentar un documento de identidad y las opciones válidas son, un pasaporte, un DNI y una licencia de conducir). Adicionalmente, este formato de datos define las características de encoding y el tipo de algoritmos criptográficos que soporta el verificador.

El “Envío de Presentación” es el formato de datos que utilizan los “titulares” (holders) para describir las pruebas que están enviando, las cuales obviamente deben estar alineadas y deben cumplir con los requisitos especificados por los verificadores en la “Definición de la presentación”.

La especificación “[Presentation Exchange v1.0.0](#)” está diseñada para ser agnóstica respecto de los distintos tipos de credenciales verificables y también de los sobres de transporte (transport envelope) que típicamente se asocian con cada tipo de credencial verificable. Esto implica que un implementador puede usar JSON Web Tokens (JWTs), Verifiable Credentials (VCs), JWT-VCs o cualquier otro formato claims, y transmitirlos a través de Open ID Connect, DIDComm, Credential Handler API o cualquier otro sobre de transporte.

Adicionalmente, esta especificación no define protocolos de transporte, end-points específicos u otros medios para transmitir los objetos formateados que define, para que otras especificaciones y proyectos que definen dichos mecanismos puedan utilizar dentro de sus flujos los formatos de datos definidos en esta especificación.

Wallet and Credential Interactions (WACI)

A diferencia de la especificación “[Presentation Exchange v1.0.0](#)”, descrita en la sección anterior, el borrador de la especificación “[Wallet And Credential Interactions](#)” proporciona una definición completa de un protocolo para cubrir los distintos aspectos necesarios para implementar las dos interacciones principales (emisión y presentación) que son requeridas en el ciclo de vida de las credenciales verificables.

Dicha especificación incorpora los formatos de datos definidos por la especificación “[Presentation Exchange v1.0.0](#)” y los complementa con elementos que incorpora de una serie de otras especificaciones y protocolos existentes, sin asumir ni requerir que un implementador los entienda todos y de esta forma lo abstrae toda esa complejidad. Hereda su estructura general del borrador inicial de [WACI](#), pero utiliza elementos del protocolo de mensajería [DIDComm v2.0](#) junto con formatos de mensaje de “[Aries Present Proof](#)” y los objetos de datos de DIF “[Presentation Exchange v1.0.0](#)”. Esta versión de la especificación también se restringe al tipo de credenciales verificables que utilizan BBS+ y LD-Signatures.

Tango VC

En función de lo expresado en las secciones anteriores de este capítulo y los requerimientos, la implementación del nivel tres del modelo de ToIP en el proyecto Tango se realizará utilizando inicialmente el esquema de credenciales JSON-LD asegurado con firmas BBS+ y un esquema de intercambio de credenciales basado en la especificación WACI, dado que es el modelo que más se adapta a las necesidades presentes y futuras del proyecto, a los distintos escenarios de uso y flujos de proceso requeridos y al paradigma de la Web 3.0, pero además porque es el que logra el mayor apalancamiento con las capacidades implementadas en los niveles uno y dos del modelo.

Esta aproximación permitirá, entre otras cosas, implementar funcionalidades muy sofisticadas, como Selective Disclosure y ZKP con un mínimo esfuerzo, sin tener que realizar concesiones en cuanto a experiencia de usuario o introducir requerimientos que podrían elevar la barrera de entrada a los usuarios y otros actores del ecosistema.

Eventualmente, para tener compatibilidad hacia atrás con aplicaciones de la Web 2.0 que utilicen mecanismos de Identidad Federada, específicamente para escenarios de Login con SSI, se podría evaluar la implementación adicional de un esquema de credenciales basado en JWT y un esquema de intercambio de credenciales basado en el stack tecnológico de Open ID Connect y JOSE.

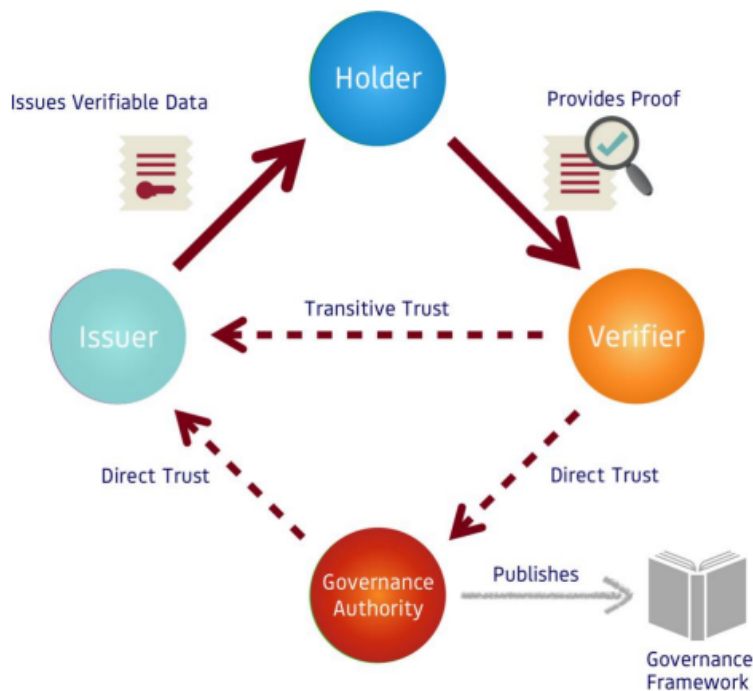
Otros Temas a abordar en esta sección

- Credenciales vs NFTs
- Selective disclosure
- Recuperación de identidad

5.4. Nivel 4: aplicaciones

El nivel cuatro del modelo de ToIP es el que facilita el desarrollo de “**ecosistemas de confianza digital**”, familias completas de aplicaciones y credenciales que no solo están diseñadas para interoperar técnicamente, sino que además comparten un “**marco común de gobernanza del ecosistema**”, el cual especifica el propósito, los principios y las políticas que se aplican a todas las autoridades de gobierno y marcos de gobierno que operen en cada uno de los cuatro niveles del stack de ToIP para cada ecosistema. Entre otras cosas, esto permite definir modelos de información estandarizados para el conjunto de credenciales propio de cada ecosistema lo que a su vez habilita la interoperabilidad funcional de extremo-a-extremo dentro de los mismos.

De esta manera, el “triángulo de confianza”, definido e implementado en el nivel 3, evoluciona al “diamante de confianza”, tal como puede verse en la siguiente figura, en la cual: mientras la mitad superior muestra la arquitectura básica del triángulo de confianza utilizada por las credenciales verificables, la mitad inferior muestra un segundo triángulo de confianza, el “**triángulo de confianza de gobierno**”, que puede resolver una serie de problemas relacionados con la adopción y la escalabilidad en el mundo real de las credenciales verificables y el stack de ToIP.



El diamante de confianza y la gobernanza digital
Fuente: trustoverip.org⁴

⁴ [Introduction to Trust Over IP](https://trustoverip.org)

El **triángulo de confianza de gobierno** representa el mismo modelo de gobierno que existe para muchas de las credenciales físicas más exitosas que usamos todos los días: pasaportes, licencias de conducir, tarjetas de crédito, tarjetas de seguro médico, etc. Estas credenciales están "respaldadas" por reglas y políticas que en muchos casos han tardado décadas en evolucionar. Estas reglas y políticas han sido desarrolladas, publicadas y aplicadas por muchos tipos diferentes de "**autoridades de gobernanza**" existentes: empresas privadas, consorcios industriales, redes financieras y, por supuesto, gobiernos.

El mismo modelo se puede aplicar a las credenciales verificables simplemente haciendo que estas mismas autoridades de gobierno, u otras nuevas formadas explícitamente para el gobierno de ToIP, publiquen "**marcos de gobierno digital**". Cualquier grupo de emisores que desee estandarizar, fortalecer y escalar las credenciales que ofrecen pueden unirse bajo los auspicios de una autoridad patrocinadora para elaborar un marco de gobernanza. Cualquiera que sea la forma de la organización — gobierno, consorcio, asociación, cooperativa — el propósito es el mismo: definir las reglas comerciales, legales y técnicas bajo las cuales los miembros de un ecosistema acuerdan operar para lograr la confianza a través de dicho ecosistema.

Con el stack de ToIP, esta arquitectura de gobierno se puede aplicar a cualquier conjunto de roles y/o credenciales, para cualquier ecosistema de confianza digital, de cualquier tamaño y en cualquier jurisdicción.

Hoy Internet es una red de redes, donde las interconexiones entre cada red se facilitan a través del stack de TCP/IP. ToIP habilita la evolución hacia **un ecosistema de ecosistemas de confianza digital**, donde las interconexiones entre cada uno de estos ecosistemas se facilita a través del stack de ToIP y los límites de cada ecosistema de confianza digital están determinados por los marcos de gobernanza bajo los cuales operan sus miembros.

Esto permite que Internet conserve la misma diversidad y riqueza que tiene hoy en día, pero con una nueva capacidad que permite formar y mantener relaciones de confianza de cualquier tipo – personal, comercial, social, académica, política – y a cualquier distancia. Estas relaciones de confianza pueden traspasar fluir de un ecosistema de confianza a otro de la misma manera como los paquetes IP pueden fluir de una red a otra en la actual Internet.

Tango en Nivel 4

El primer paso en el hoja de ruta de Tango apunta a desplegar un primer ecosistema y su correspondiente marco de gobernanza alrededor de las credenciales y los casos de uso relacionados con el Gobierno de la Ciudad de Buenos Aires, pero, como se mencionó anteriormente en este documento, esto dejará instalada una infraestructura abierta, descentralizada y no permissionada, que luego podrá ser re-utilizada libremente por otros ecosistemas de confianza digital, para terminar constituyendo un ecosistema de ecosistemas de confianza digital sobre el stack de ToIP. Adicionalmente, la masa crítica que aportará Tango en esta primera etapa, actuará como una fuerza gravitatoria que estimulará la creación de dichos ecosistemas, creando la retroalimentación necesaria para que el sistema logre la sustentabilidad a largo plazo y total autonomía respecto del Gobierno de la Ciudad de Buenos Aires.

6. Biometría

7. Gestión y recupero de identidad

La expresión “not your keys, not your coins” es muy popular y muy importante en el mundo de las criptomonedas y de los cripto activos. Lo que significa es que si alguien no tiene el control exclusivo sobre sus claves privadas no tiene realmente el control y el poder de decisión sobre dichos valores.

Dado que la Identidad Digital Auto Soberana puede ser entendida como un tipo de activo digital, cuya implementación además comparte mucho del stack tecnológico y los paradigmas de descentralización que se usan en el mundo de los cripto activos, esta sección explora el concepto antes mencionado, pero aplicado específicamente al “control de la identidad digital auto soberana”.

DIDs vs SCIDs

Un “**identificador auto-certificable**” – “Self-Certifying IDentifier” o SCID – vincula criptográficamente a un identificador con un par de claves pública y privada, de forma tal que: 1) la relación entre el identificador y la clave pública se puede probar de forma determinística, 2) la clave privada correspondiente se puede usar para demostrar el control sobre él identificador y 3) no es necesario contar con ningún elemento adicional para certificar estas relaciones.

Los cripto activos típicamente utilizan alguna forma de SCIDs para identificar a quien tiene el control de los mismos. Las “**direcciones**” son la forma más común de SCIDs en redes blockchain que manejan cripto activos. La correspondencia entre una “dirección blockchain” y una “clave pública” se puede probar de forma determinística y, por lo tanto, la clave privada correspondiente se puede usar para demostrar el control sobre la “dirección de blockchain”, todo sin necesidad de contar con ningún elemento adicional para certificar estas relaciones.

Los DIDs por su parte, son identificadores que comparten con los SCIDs la característica de que el control sobre el identificador puede ser verificado mediante criptografía pero, a diferencia de los SCIDs, los DIDs por lo general requieren de elementos adicionales para realizar esta comprobación (DID Documents y DID Registries). Existen algunos métodos DID que generan DIDs que son SCIDs, pero no es lo más común.

Si bien los SCIDs, por su característica de “auto-certificación”, son simples de implementar y muy eficientes, por lo general no cumplen con todos los requisitos que impone la problemática de Identidad Auto Soberana. Los DIDs por su parte, imponen cierta complejidad, debido a que requieren de una infraestructura más compleja, pero permiten la implementación de funciones más avanzadas, tales como rotación de claves, esquemas de múltiples firmas o manejo de roles asociados a un DID, todas funcionalidades necesarias para cubrir los requerimientos de Identidad Auto Soberana.

DID Document

Para habilitar las funciones avanzadas que se mencionaron en el párrafo anterior, el modelo de DIDs introduce el recurso del “Documento DID” el cual permite especificar la información asociada con un DID que dichas funciones requieren. Entre otras cosas, en estos documentos se pueden incluir múltiples métodos de verificación (Ej.: claves públicas) asociados al DID y los roles en que pueden usarse dichos métodos de verificación.

Existen dos roles principales principales que se pueden incluir en un DID Document: Controllers y Delegates

Controller

Este rol permite modificar la información del DID Document en sí mismo. En un DID Document se pueden definir uno o múltiples controllers especificando las claves públicas de cada uno de ellos.

El controller, dado que puede modificar el DID Document y esto incluye la facultad de eliminar o incorporar otros controllers, es quien tiene el control del DID Document y en definitiva del DID. Dicho de otra forma: **quien tenga el control sobre la clave privada correspondiente a un controller de un DID Document tiene el control sobre dicho documento y en definitiva sobre el DID.**

Cuando se trata de individuos, típicamente el sujeto del DID es a su vez el controller del DID Document, pero hay situaciones donde el controller puede no ser el sujeto del DID. Por ejemplo: los padres de un menor de edad pueden ser los que tienen asignada la facultad de controllers en el DID Document de su hijo.

Cuando un DID identifica a una organización, un animal o una cosa, el o los controllers siempre son individuos autorizados para cumplir este rol. Ejemplo: el dueño de una mascota típicamente aparecerá como controller en el DID Document de la mascota.

Delegate

Este rol permite delegar un conjunto específico de funciones a un delegado para que este pueda actuar en representación del sujeto del DID para dichas funciones. Por ejemplo: el sujeto de un DID, a través de su controller, delega en un tercero la facultad de firmar credenciales verificables en su nombre.

Los delegados sólo pueden ejercer las facultades para las cuales han sido autorizados y no tienen autorización para actualizar el DID Document, por lo que no tienen el control del mismo y por lo tanto no controlan el DID.

Administración de claves

A continuación se detallan algunas situaciones relacionadas con la administración de claves públicas y privadas asociadas a los DIDs que es necesario considerar en la implementación de una plataforma de Identidad Auto Soberana.

Rotación de Claves

La rotación de claves permite modificar los pares de claves públicas y privadas asociadas a los distintos roles definidos en un DID Document.

La rotación periódica de claves es una buena práctica de seguridad y está orientada a minimizar la posibilidad de que las claves privadas asociadas a alguno de los roles definidos en un DID document se vean comprometidas y puedan ser utilizadas por personas no autorizadas.

Pérdida y Recuperación del control sobre la Identidad

Tal como se mencionó en párrafos anteriores, en el contexto de Identidad Auto Soberana, tener el control sobre la identidad es sinónimo de tener el control sobre las claves privadas de los controllers que están especificados en el DID document asociado a un DID.

Si bien existen muy variados esquemas de recuperación de identidad, todos en definitiva se resumen a una cosa: recuperar el control y acceso exclusivo a las claves privadas de los controllers que están especificados en el DID Document, típicamente ejecutando una rotación de claves en estos roles, por algún mecanismo predefinido en el DID Method. Distintos DID Methods podrían definir distintas aproximaciones para forzar la rotación de claves como parte del mecanismo de recuperación de identidad.

Un aspecto a destacar es que, dado que la rotación de claves no cambia el valor del DID, la asociación entre el DID y las credenciales verificables que hayan sido emitidas para ese DID no se afecta cuando se ejecuta una rotación de claves. Esto implica que no es necesario emitir nuevamente las credenciales verificables de un sujeto si éste recupera su identidad mediante una rotación de claves.

Custodial vs Non-Custodial

Tal como se mencionó anteriormente, en el contexto de los crypto activos, el tener o no el control exclusivo de las claves privadas normalmente determina si se tiene o no el control de los crypto activos asociados a las direcciones correspondientes.

Alineado con este concepto aparecen dos tipos diferentes de billeteras “custodial” y “non-custodial” y a la vez un gran debate en el mundo crypto respecto de las ventajas y desventajas de cada uno de estos tipos de billeteras.

En el contexto de Identidad Auto Soberana, tener el control de una identidad implica tener el control de las claves privadas de todos los controllers que están definidos en el DID Document, dado que si se compromete la clave privada de alguno de ellos un actor malicioso podría utilizarla para cambiar o eliminar los controllers y todos los datos del DID Document, ganando de esta forma el control sobre dicha identidad.

Adicionalmente, es importante recordar que un DID también puede tener “delegados” que pueden representarlo en situaciones específicas, lo que implica que si se compromete alguna de estas claves privadas, en alguna medida también se compromete el control sobre algún aspecto de la identidad.

Debido a esto, en el contexto de Identidad Auto Soberana los términos “custodial” y “non-custodial” no se relacionan directamente con tener o no tener el control de la Identidad, dado que mantener el control de la identidad implica controlar todas las claves privadas que controlan alguno de sus aspectos, las cuales podrían estar

controladas por distintas personas que a su vez podrían estar usando distintos tipos de billeteras para manejar sus claves privadas.

Aun con estas consideraciones, es importante considerar detenidamente este aspecto en toda implementación de una plataforma de Identidad Auto Soberana, y considerarlo teniendo en cuenta que una implementación de este estilo apunta a ser muy masiva, atraviesa distintos segmentos de usuarios con capacidades y preferencias muy diversas, que deben ser tenidas en cuenta para no generar exclusiones.

Si bien una billetera “custodial” puede considerarse menos segura que una billetera “non-custodial”, entre otras cosas porque involucra confiar en un tercero, la realidad es que esto depende de la habilidad que tenga cada persona para cumplir con todas las normas de seguridad en una wallet non-custodial. En muchos casos una billetera “custodial” puede representar una opción válida para usuarios que prefieran no cargar con tanta responsabilidad y que privilegien aspectos como la facilidad de uso.

Lo ideal es contar con una variedad de billeteras custodial y non-custodial y que cada usuario pueda optar por la que más se ajuste a sus necesidades.

Guardianship

En la medida que la humanidad avanza hacia un mundo cada vez más digital, existe el riesgo de que se aumente la “exclusión digital” de aquellos que no pueden actuar por sí mismos (o totalmente solos) en este nuevo contexto. Este riesgo es particularmente importante en una implementación de Identidades Digitales, dado que privar de acceso a la identidad tiene un impacto muy severo en términos de exclusión y además porque existen muchos casos donde los individuos no pueden valerse por sí solos para acceder a este derecho fundamental.

Los sistemas de Identidad Auto Soberana, en los que el control de una identidad digital se demuestra utilizando credenciales digitales almacenadas en una billetera digital, presentan un desafío adicional. Cómo podemos permitir que todos controlen su identidad digital cuando, por definición, experimentamos etapas de la vida (p. ej., la infancia) y condiciones (p. ej., demencia) en las que la ley y las normas sociales dictan que no podemos ser autosuficientes. Este desafío no se puede resolver con una simple delegación, porque un niño, una persona que vive con demencia o un refugiado sin conexión a Internet no puede delegar algo que no tiene. Tampoco es una simple relación de “controller” con una cosa (por ejemplo, un dron) porque, a diferencia de un dron, un niño adquiere derechos progresivamente y eventualmente se vuelve más autosuficiente. De manera similar, la persona que vive con demencia experimentará un cambio de capacidad con el tiempo.

Debido a eso, los sistemas de identidad necesitan un medio para representar a aquellos que no pueden actuar por sí mismos (o totalmente solos) en el mundo digital. Esta capacidad es la capacidad de Guardianship que debe ser cuidadosamente diseñada e implementada en toda plataforma de Identidad Auto Soberana.

Para más detalles sobre esta problemática, puede consultarse el documento “[On Guardianship in Self-Sovereign Identity](#)” publicado por la fundación Sovrin.

8. Gobierno

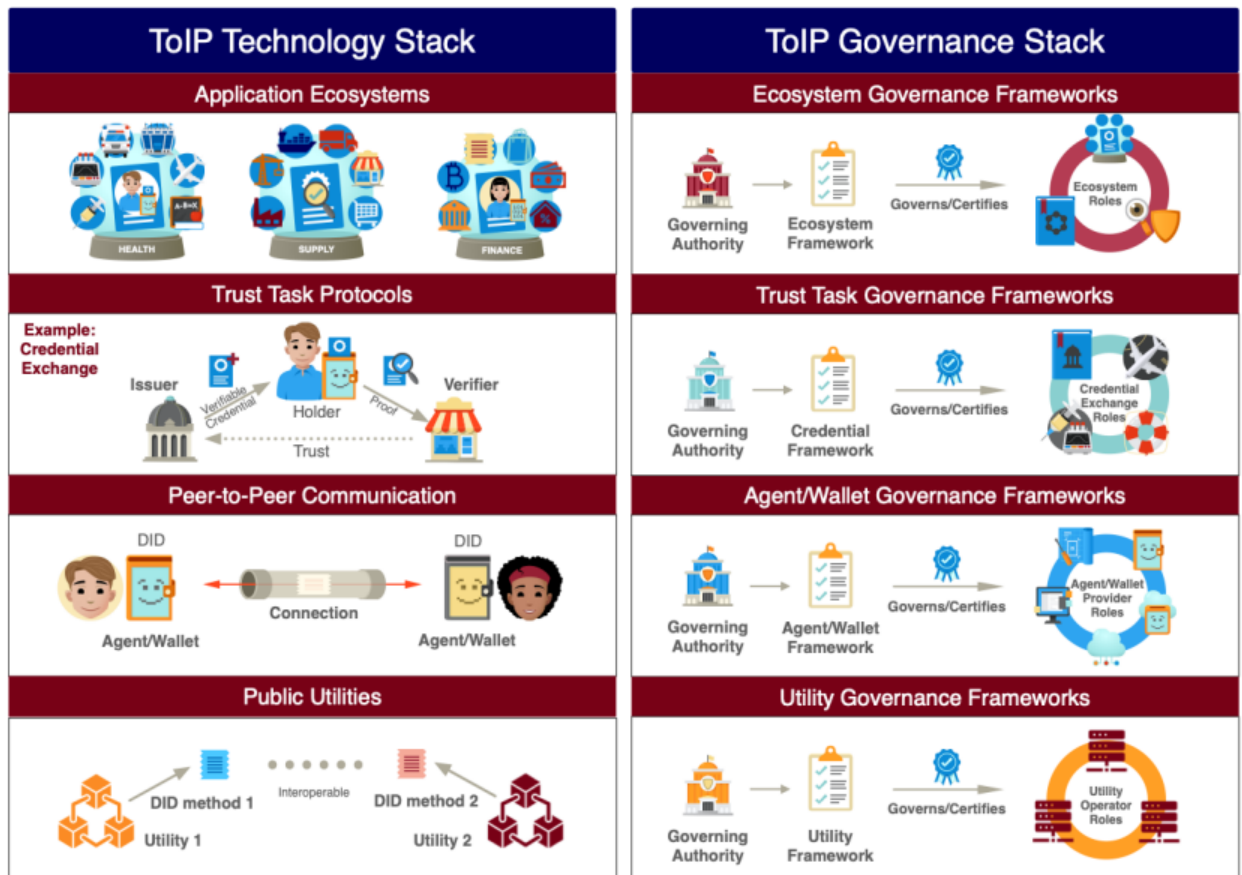
8.1. Introducción

Trust over IP (ToIP) define una arquitectura completa para crear “**confianza digital**” a escala de Internet y habilitar la formación de “**ecosistemas de confianza digital**” interoperables de todo tipo y tamaño.

Un sello distintivo de esta arquitectura es que combina una serie de protocolos y herramientas en diferentes capas de tecnología con un conjunto de "reglas" que se conocen formalmente como **Marcos de Gobernanza** (MG).

Según la Fundación ToIP, esta fusión de gobernanza y tecnología, es crucial para habilitar el camino hacia un sistema de identidad descentralizada que sea universal, confiable e interoperable, y que constituya el fundamento de un nuevo “**marco de confianza digital**” que satisfaga los requerimientos legales, comerciales y sociales derivados de las interacciones entre personas, organizaciones y cosas en un contexto totalmente globalizado y cada vez más digital como el que tenemos en el siglo XXI.

La siguiente figura muestra el diseño en dos dimensiones – tecnología y gobernanza – del stack de ToIP. El énfasis que pone este modelo en la gobernanza tiene que ver con que, al menos por el momento, la tecnología por sí sola no es suficiente para generar “confianza digital” en un contexto de escala global y gran diversidad de situaciones, simplemente porque la confianza es una creencia psicológica de los humanos (o grupos de humanos). Por lo tanto, la tecnología debe adaptarse al comportamiento humano para generar confianza de extremo a extremo en dicho contexto.



En las siguientes secciones describiremos las características más importantes del modelo de gobernanza propuesto por ToIP y también su aplicación al contexto específico de Tango ID y el ecosistema de GCBA.

Para tener una descripción detallada de la arquitectura y el metamodelo de gobernanza propuesto por la Fundación Trust over IP pueden consultarse los siguientes documentos publicados en <https://trustoverip.org/our-work/deliverables/>:

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

8.2. Ecosistemas de Confianza Digital

Tal como se mencionó anteriormente en este documento, ToIP habilita la evolución de Internet **desde una red de redes hacia un ecosistema de ecosistemas de confianza digital**, donde las interconexiones entre cada uno de estos ecosistemas se facilita a través del stack de ToIP y los límites de cada ecosistema de confianza digital están determinados por los marcos de gobernanza bajo los cuales operan sus miembros.

Lo expuesto en el párrafo anterior implica que en Tango no existe uno sino múltiples marcos de gobernanza operando simultáneamente. Como puede verse en la siguiente

figura, existe el Marco de Gobernanza de Tango (MGT), que provee la base sobre la cual luego se montan los Marcos de Gobernanza para cada uno de los Dominios Específicos (MGDs).

Mientras el Modelo de Gobernanza de Tango (MGT) provee las reglas que aplican a todos los ecosistemas que participen de la red, los Modelos de Gobernanza para Dominios Específicos “extienden” al MGT con reglas propias de cada ecosistema.



El marco de Gobernanza de Tango (MGT) provee la base para otros Marcos de Gobernanza en Dominios Específicos (MGDs)

Esta estructura permite preservar la diversidad y la riqueza que tenemos en Internet hoy en día, pero con una nueva capacidad que permite formar y mantener relaciones de confianza de cualquier tipo – personal, comercial, social, académica, política – y a cualquier distancia. Estas relaciones de confianza pueden traspasar o fluir de un ecosistema de confianza a otro de la misma manera que los paquetes IP pueden fluir de una red a otra en la actual Internet.

8.3. Marcos de Gobernanza por nivel

Otro aspecto importante a considerar al momento de definir un marco de gobernanza que sea compatible con ToIP, es que la gobernanza aplica de forma diferente a cada uno de los cuatro niveles del modelo ToIP y, por lo tanto, se necesitan autoridades de gobierno (de algún tipo) y marcos de gobernanza (de algún tipo) en cada uno de estos cuatro niveles.

Estas autoridades y marcos de gobernanza, según el caso, pueden ser implementados de manera formal o informal, mediante código informático o código legal, pero su existencia es crucial para crear “confianza digital” y facilitar la aceptación comercial, legal, social y política de estos nuevos paradigmas.

Servicios Públicos de DIDs

Este nivel implementa los servicios públicos de DID que se requieren, entre otras cosas, para buscar y verificar las claves públicas de los emisores de credenciales digitales, constituyendo las raíces de confianza o anclas de confianza de toda esta infraestructura de clave pública/privada, estos "puntos de partida".

Al diseñar un marco de gobernanza para este nivel es importante tener siempre presente que estos servicios son públicos, abiertos y de uso compartido para todos los ecosistemas que operen con la plataforma.

Los marcos de gobernanza de los **servicios públicos** de DID establecen claramente las políticas y los procedimientos utilizados para:

- Operar estos servicios públicos de manera segura, transparente y confiable, manteniendo su eficiencia y escalabilidad.
- Administrar el ciclo de vida de las claves públicas asociadas a los DIDs de manera segura, eficiente y amigable, considerando las necesidades específicas de diversos tipos de usuarios (Ej.: creación y recuperación de identidad, rotación de claves, etc).
- Evitar abusos o usos indebidos de estos servicios públicos (Ej.: spam) y garantizar su sustentabilidad económica a largo plazo.

Nivel 2 – Wallets y Agentes

Este nivel implementa las wallets y los agentes que necesitan las personas, las organizaciones y las "cosas" digitales (o los gemelos digitales de cosas no digitales) para aceptar, almacenar e intercambiar credenciales digitales utilizando protocolos estándares de comunicación peer-to-peer tales como DIDComm.

Los marcos de gobernanza para las wallets/agentes establecen claramente los estándares, las políticas y procedimientos que deben ser observados por los proveedores de wallets y agentes para garantizar la seguridad, privacidad, protección de datos, interoperabilidad y soberanía sobre la información.

Nivel 3 – Credenciales

Este nivel, en el plano técnico, implementa el **triángulo de confianza de credenciales verificables**, que permite el establecimiento de relaciones de confianza transitivas entre tres partes – emisores, titulares y verificadores – utilizando los formatos y protocolos de intercambio de datos para credenciales verificables. Los marcos de gobernanza en este nivel agregan un segundo triángulo de confianza, denominado “**triángulo de confianza de gobernanza**”, formado por los emisores, los verificadores y la autoridad de gobierno. La combinación de ambos triángulos de confianza genera lo que se conoce como el “**diamante de la confianza**” y que fue descrito anteriormente en este documento.

Los marcos de gobernanza de credenciales se enfocan en estandarizar las políticas comerciales, legales y técnicas para emitir, mantener y verificar un conjunto de credenciales. Entre otras cosas, estos marcos de gobernanza definen:

- Quienes están autorizados para emitir credenciales de cierto tipo, para que los verificadores tengan toda la información que necesitan para tomar decisiones de confianza basadas en las pruebas derivadas de credenciales verificables que se les presentan
- Qué información puede solicitar un verificador, para evitar que se solicite más información de la necesaria para un propósito dado

Nivel 4 – Ecosistemas

El nivel cuatro del modelo de ToIP es el que facilita el desarrollo de “**ecosistemas de confianza digital**”, familias completas de aplicaciones y credenciales que no solo están diseñadas para interoperar técnicamente, sino que además comparten un “**marco común de gobernanza del ecosistema**” el cual especifica el propósito, los principios y las políticas que se aplican a todas las autoridades de gobierno y marcos de gobierno que operen en cada uno de los cuatro niveles del stack de ToIP para cada ecosistema.

Por lo general, el marco de gobernanza de un ecosistema incluye el reconocimiento de autoridades y marcos de gobernanza independientes que estén autorizados y/o respaldados en los niveles inferiores. Estos marcos de gobernanza también pueden especificar marcas de confianza (trustmarks), registros de confianza, requisitos de usabilidad, programas de certificación y otros mecanismos necesarios para garantizar la integridad y la salud de todo el ecosistema.

9. Estrategia de Adopción

Nota: en esta sección se incluirán las definiciones y criterios relevantes para lograr una amplia adopción de la plataforma, contando con el respaldo e impulso que se puede dar desde el GCBA

Algunos pasos básicos del camino a seguir

1. Co-creación de las definiciones acerca del protocolo y los estándares a emplear.
2. Desarrollo de la infraestructura tecnológica requerida.
3. Desarrollo de la primera aplicación por parte de GCBA.
4. Adopción masiva de identidades digitales impulsada por la aplicación GCBA.
5. Impulsar la adopción del ecosistema por la sociedad y actores privados.
6. Impulsar la adopción de reputaciones vinculadas a la identidad digital entre privados.

Anexo I

A continuación se presentan los 10 principios para la identidad auto-gestionada definidos por Christopher Allen (2016)⁵:

- **Existencia.** *Los usuarios deben tener una existencia independiente.* Toda identidad auto soberana está, en definitiva, basada en el inefable “yo” presente en el corazón de la identidad. Nunca puede existir en forma enteramente digital. Este debe ser el núcleo del ser que se sostiene y apoya. Una identidad auto-soberana simplemente hace públicos y accesibles algunos limitados aspectos del “yo” ya existente.
- **Control.** *Los usuarios deben controlar su identidad.* Sujeto a algoritmos bien comprendidos y seguros que garanticen la validez continua de una identidad y sus atestaciones (*claims*), el usuario es la máxima autoridad sobre su identidad. Siempre deben ser capaces de referenciarla, actualizarla e incluso ocultarla. Deben poder elegir entre mantenerla privada o hacerla pública. Esto no significa que un usuario controle todas las atestaciones asociadas a su identidad: otros usuarios podrían hacer atestaciones asociadas a él/ella, pero no deben ser fundamentales para la identidad en sí.
- **Acceso.** *Los usuarios deben tener acceso a su propia información.* Un usuario debe siempre ser capaz de acceder fácilmente a todas las atestaciones e información extra asociada a su identidad. No debe haber datos ocultos ni guardianes. Esto no significa necesariamente que un usuario debe poder modificar todas las atestaciones asociadas a su identidad, pero sí que debe conocerlas. Tampoco significa que los usuarios tengan el mismo acceso a la información de los demás, sino sólo a la suya.
- **Transparencia.** *Los sistemas y algoritmos deben ser transparentes.* Los sistemas utilizados para administrar y operar una red de identidades deben ser abiertos, tanto en su funcionamiento como en su gestión y proceso de actualización. Los algoritmos deben ser libres, de código abierto bien comprendidos y lo más independientes posible de cualquier arquitectura en particular; cualquiera debe poder inspeccionar su funcionamiento.
- **Persistencia.** *Las identidades deben ser longevas.* Preferiblemente, las identidades deben durar para siempre, o al menos durante el tiempo que el usuario lo desee. Si bien se puede llegar a necesitar rotar las claves privadas y modificar cierta información, la identidad permanece. En el vertiginoso mundo de Internet, este objetivo puede no ser del todo razonable, por lo que las

⁵ La traducción es propia.

identidades deben durar como mínimo hasta que nuevos sistemas de identidad las vuelvan obsoletas. Esto no debe contradecir el "derecho a ser olvidado"; un usuario debe poder deshacerse de una identidad si lo desea, y las atestaciones deben modificarse o eliminarse con el paso del tiempo según convenga. Realizar esto requiere separar firmemente una identidad de sus atestaciones: no pueden estar vinculadas para siempre.

- **Portabilidad.** *La información y los servicios asociados a la identidad deben ser transportables.* Las identidades no deben estar en manos de un tercero, incluso aunque sea una entidad de confianza de la cual se espera que trabaje en el mejor interés del usuario. El problema es que las entidades pueden desaparecer - y en Internet, la mayoría acaba por hacerlo. Los regímenes pueden cambiar, los usuarios pueden trasladarse a otras jurisdicciones. Las identidades transportables garantizan que el usuario siga teniendo el control de su identidad pase lo que pase, y también pueden mejorar la persistencia de una identidad en el tiempo.
- **Interoperabilidad.** *Las identidades deben ser lo más ampliamente utilizables posible.* Las identidades tienen poco valor si sólo funcionan en nichos. El objetivo de un sistema de identidad digital del siglo XXI es hacer a la información identitaria ampliamente disponible, cruzando las fronteras internacionales para crear identidades globales, sin que el usuario pierda el control. Gracias a la persistencia y la autonomía, estas identidades ampliamente disponibles pueden volverse también continuamente disponibles.
- **Consentimiento.** *Los usuarios deben estar de acuerdo con el uso de su identidad.* Cualquier sistema de identidad se construye en torno a la puesta en común de aquella identidad y sus atestaciones, y un sistema interoperable aumenta el volumen de intercambio producido. Sin embargo, el intercambio de información sólo debe producirse con el consentimiento del usuario. Aunque otros usuarios tales como un empleador, una oficina de crédito o un amigo puedan presentar atestaciones, el usuario debe dar su consentimiento para que estas sean válidas. Tener en cuenta que este consentimiento puede no ser interactivo, pero sí debe ser deliberado y bien comprendido.
- **Minimización.** *La divulgación de las atestaciones debe ser mínima.* Cuando se revela información, esa revelación debe implicar la cantidad mínima de datos necesarios para cumplir la tarea en cuestión. Por ejemplo, si sólo se pide una edad mínima, no debe revelarse la edad exacta, y si sólo se pide una edad, no debe revelarse la fecha precisa de nacimiento. Este principio puede respaldarse en la divulgación selectiva, las pruebas de rango y otras técnicas de zero-knowledge, pero la no correlación sigue siendo una tarea muy difícil (quizás imposible); lo mejor que podemos hacer es emplear la minimalización para respaldar la privacidad lo mejor posible.

- **Protección.** *Los derechos de los usuarios deben ser protegidos.* Cuando existe un conflicto entre las necesidades de la red de identidad y los derechos de los usuarios individuales, la red debe pecar de preservar las libertades y los derechos de los individuos por encima de las necesidades de la red. Para garantizar la autenticación de la identidad debe realizarse mediante algoritmos independientes, resistentes a la censura y a la fuerza, y que se ejecuten de forma descentralizada.

Anexo II

Mapeo de principios de diseño contra los 10 principios para la identidad auto-gestionada.

| PRINCIPIOS PARA LA IDENTIDAD AUTO-GESTIONADA | PRINCIPIOS DE DISEÑO |
|--|-----------------------------|
| EXISTENCIA | <i>Proof of Existence</i> |
| | <i>Proof of Humanity</i> |
| CONTROL | Custodial vs Non-Custodial |
| | Recuperación de Identidad |
| ACCESO | Descentralizado |
| TRANSPARENCIA | Co-creación |
| | Código abierto |
| PERSISTENCIA | |
| PORTABILIDAD | |
| INTEROPERABILIDAD | Credenciales vs NFTs |
| CONSENTIMIENTO | <i>Selective Disclosure</i> |
| MINIMALIZACIÓN | |
| PROTECCIÓN | Estándares de seguridad |

Anexo III

Billeteras Cripto vs Billeteras de Identidad

Como se mencionó anteriormente en este documento, en el contexto de la Web 3.0 existen dos tipos de billeteras que resultan relevantes:

- Billeteras utilizadas para manejar **activos digitales** (Ej.: Criptomonedas, NFTs)
- Billeteras utilizadas para manejar **credenciales verificables** (Ej.: licencias de conducir, títulos universitarios).

A continuación se describen, comparativamente, las características fundamentales de cada uno de estos dos tipos de billeteras y, para facilitar la lectura, en este anexo nos referiremos a cada uno de ellos como “**billeteras cripto**” y “**billeteras de identidad**” respectivamente.

Aspectos generales

Tanto las billeteras cripto, como las billeteras de identidad pertenecen o están vinculadas a un “sujeto”, el cual puede ser un individuo, una organización o incluso a una cosa (Ej.: un vehículo eléctrico puede tener vinculada una billetera).

Desde el punto de vista de la utilidad, mientras las billeteras cripto se enfocan a manejar valores que el sujeto posee (Ej.: criptomonedas o NFTs), las billeteras de identidad se enfocan a manejar credenciales que describen alguna característica de la identidad del sujeto (Ej.: una licencia de conducir o un título universitario).

Claves Privadas y Firma Digital

La capacidad más básica y fundamental de ambos tipos de billeteras es la que permite administrar claves privadas y firmas digitales y en ambos casos se implementa de manera similar, de hecho, muchas implementaciones se realizan utilizando las mismas primitivas y librerías criptográficas.

En ambos casos se requiere implementar un “Key Management Service” (KMS) que permita generar y almacenar pares de claves públicas y privadas, proteger las claves privadas y firmar digitalmente utilizando diversidad de algoritmos criptográficos. En algunos casos esta capacidad puede además soportar esquemas de múltiples firmas normalmente conocidos como “multisig”.

Mientras que en las billeteras cripto, las claves privadas se utilizan para demostrar el control sobre activos digitales que están almacenados en una red blockchain, en las

billeteras de identidad las claves privadas se utilizan para demostrar el control sobre alguno de los aspectos descritos en un DID document.

Almacenamiento

Desde el punto de almacenamiento existen diferencias significativas entre las “billeteras cripto” y las “billeteras de identidad”, tanto en “la información que almacenan”, como en los mecanismos de replicación y sincronización que implementan.

Mientras que las “billeteras cripto” sólo almacenan la información relacionada con el KMS, es decir: claves privadas, claves públicas y direcciones blockchain – dado que el resto de la información se encuentra almacenada en las redes blockchain – las “billeteras de identidad”, son responsables de almacenar en forma privada y segura toda la información asociada a la identidad del sujeto, principalmente sus credenciales verificables. Por ejemplo: mientras el saldo de una criptomoneda asociado a una dirección de blockchain no se encuentra almacenado en la “billetera cripto”, sino en la red blockchain correspondiente, las credenciales verificables asociadas a un sujeto si se encuentran almacenadas en la “billetera de identidad” y no se recomienda almacenar esta información a nivel de una red blockchain por cuestiones de compliance y seguridad.

Por otro lado, mientras las “billeteras de identidad”, al menos las más sofisticadas, suelen implementar mecanismos que permitan mantener replicada y sincronizada la información relativa a la identidad del sujeto en los distintos dispositivos que este pueda utilizar, las “billeteras cripto” no requieren este tipo de mecanismos, porque las capacidades de replicación y sincronización de la información datos es provista a nivel de las redes blockchain (Ej.: el saldo de una dirección es almacenado en todos los nodos de una red blockchain).

En ambos casos, la información relacionada con el KMS suele sincronizarse en distintos dispositivos haciendo uso de “frases semilla” (seed phrases), a partir de las cuales se puede reconstruir toda la jerarquía de claves privadas, claves públicas y direcciones asociadas a la billetera.

Operaciones

Mientras que las billeteras cripto están orientadas a preparar y firmar transacciones que serán procesadas por una red blockchain, las billeteras de identidad están orientadas a preparar y firmar credenciales o pruebas que serán intercambiadas en forma peer-to-peer entre los actores involucrados.

Mientras las operaciones que se ejecutan desde billeteras cripto son típicamente públicas y, por lo tanto, conocidas por todos aquellos que tengan acceso a un nodo de la red, las operaciones que se ejecutan desde billeteras de identidad siempre son totalmente privadas y solo conocidas por las partes involucradas.

Comunicaciones

Las billeteras cripto típicamente no implementan un esquema de comunicaciones entre las partes involucradas en cada transacción dado que las transacciones se llevan a cabo con la intermediación de la red blockchain que utilicen en cada caso.

En el caso de las “billeteras de identidad”, las operaciones en sí mismas son realizadas de forma peer-to-peer pura, sin intermediación de ningún tipo, lo cual exige la implementación de protocolos de comunicación del tipo peer-to-peer y mecanismos de discovery y ruteo de mensajes entre las partes.

Es importante aclarar que, excepcionalmente, algunas billeteras cripto implementan esquemas de comunicación entre partes, pero estos no se utilizan para procesar la operación en sí misma, sino para intercambiar información que necesaria para preparar una operación que será procesada a través de una red blockchain (Ej.: intercambiar la dirección y el montos a transferir). Adicionalmente, dado que se implementan con mecanismos propietarios, estos mecanismos sólo son aplicables si ambas partes utilizan la misma billetera.

Glosario

A COMPLETAR