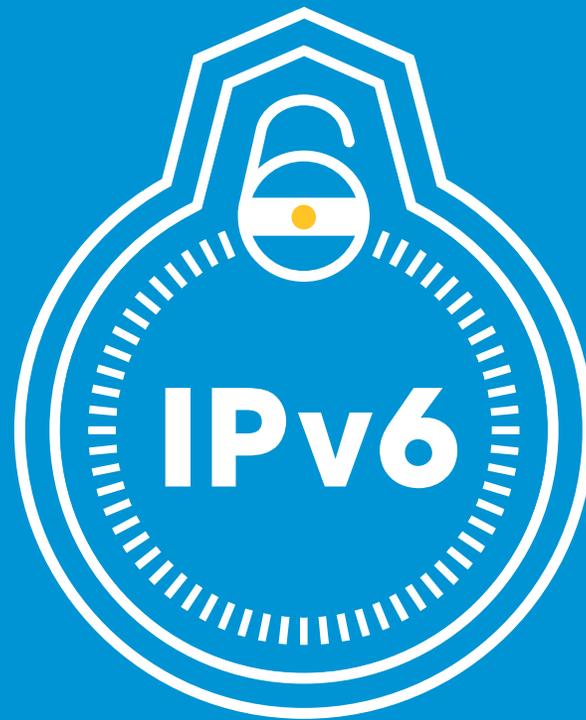


IPv6

Blockchain y BFA





¿Qué es una IP?

Las direcciones del Protocolo de Internet (IP) son identificadores numéricos únicos asignados a todo lo que está conectado a Internet, desde servidores web hasta smartphones, cámaras e impresoras.



IPv4

La versión más usada del Protocolo de Internet, IPv4, se desarrolló a principios de los años 80 y ha estado al servicio de la comunidad global de Internet por más de tres décadas.

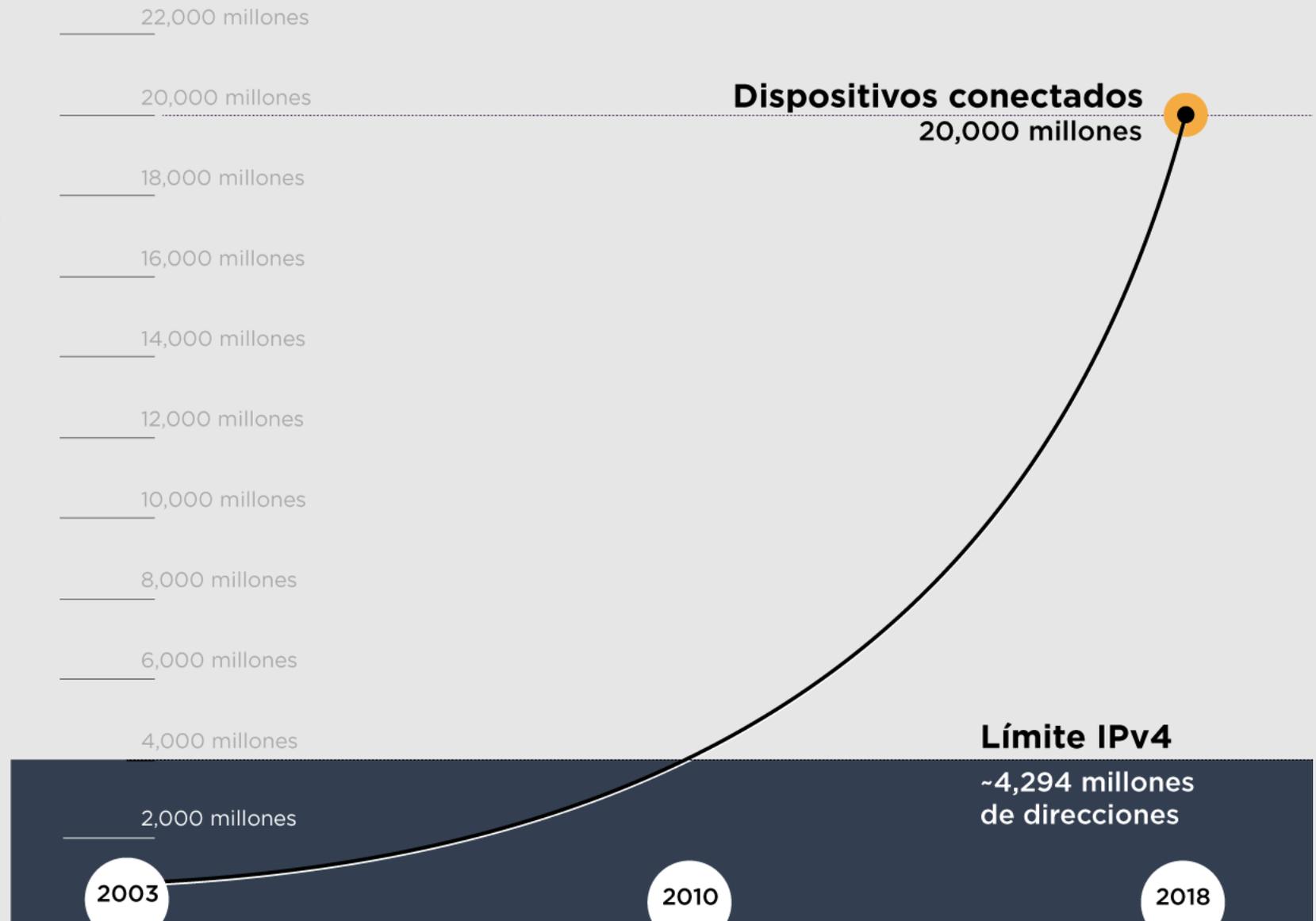
Debido a su formato de 32 bits, es posible lograr un poco más de 4000 millones de direcciones diferentes, lo que en un principio se consideraba más que suficiente para las necesidades de Internet.



IPv4 al límite

El enorme crecimiento que ha tenido Internet demostró que IPv4 ya no es suficiente.

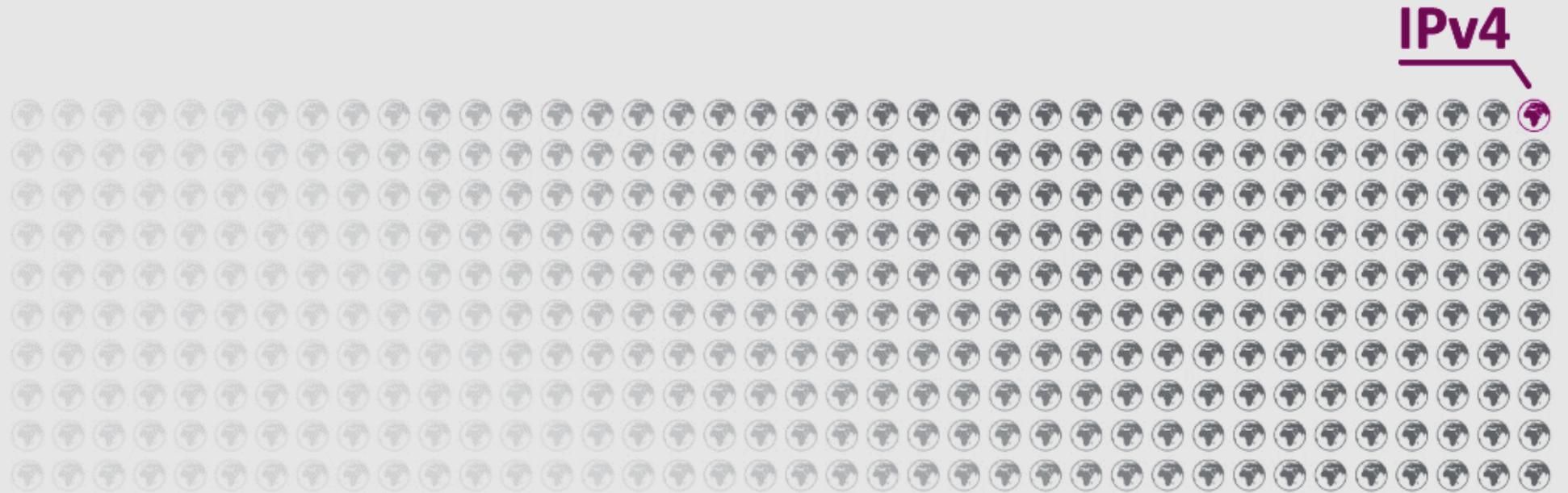
Internet tiene cada vez más usuarios, estos tienen cada vez más dispositivos, y ya no hay direcciones IPv4 para distribuir.



IPv6 al rescate



IPv6 viene a solucionar muchos de los problemas de IPv4 y permitir que la red siga creciendo gracias a la posibilidad de habilitar miles de millones de direcciones nuevas.



IPv6

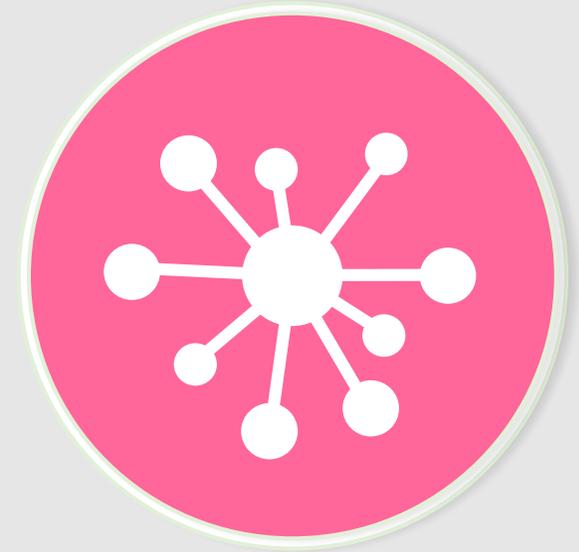
Ventajas de IPv6



**Mayor cantidad
de direcciones**



**Eliminación
del NAT**



**Desarrollo
IOT**



Coalición IPv6



Secretaría de Modernización
Presidencia de la Nación

ONTI

Oficina Nacional de
Tecnologías de Información

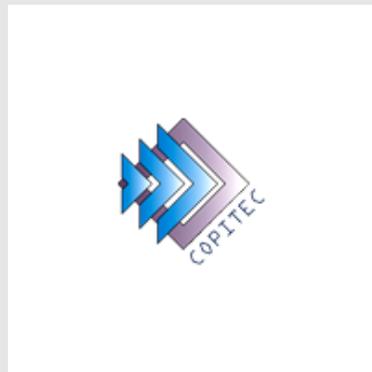
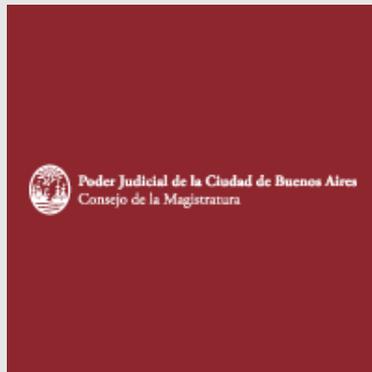
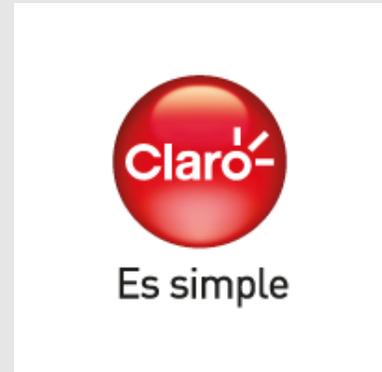


ENACOM

Ente Nacional de Comunicaciones



NIC Argentina



Comunidad de usuarios: Daniel Faure: Emprendedor freelance, Eduardo Molina Quiroga: Docente en Derecho Informático (UBA)

Objetivos



**Analizar
evolución
de IPv6**



**Articular
investigaciones
y desarrollo**



Participación



**Establecer
intercambios**



**Fomentar
buenas
prácticas**



**Trabajar de manera
colaborativa**



BLOCKCHAIN
FEDERAL ARGENTINA

¿Qué es blockchain?

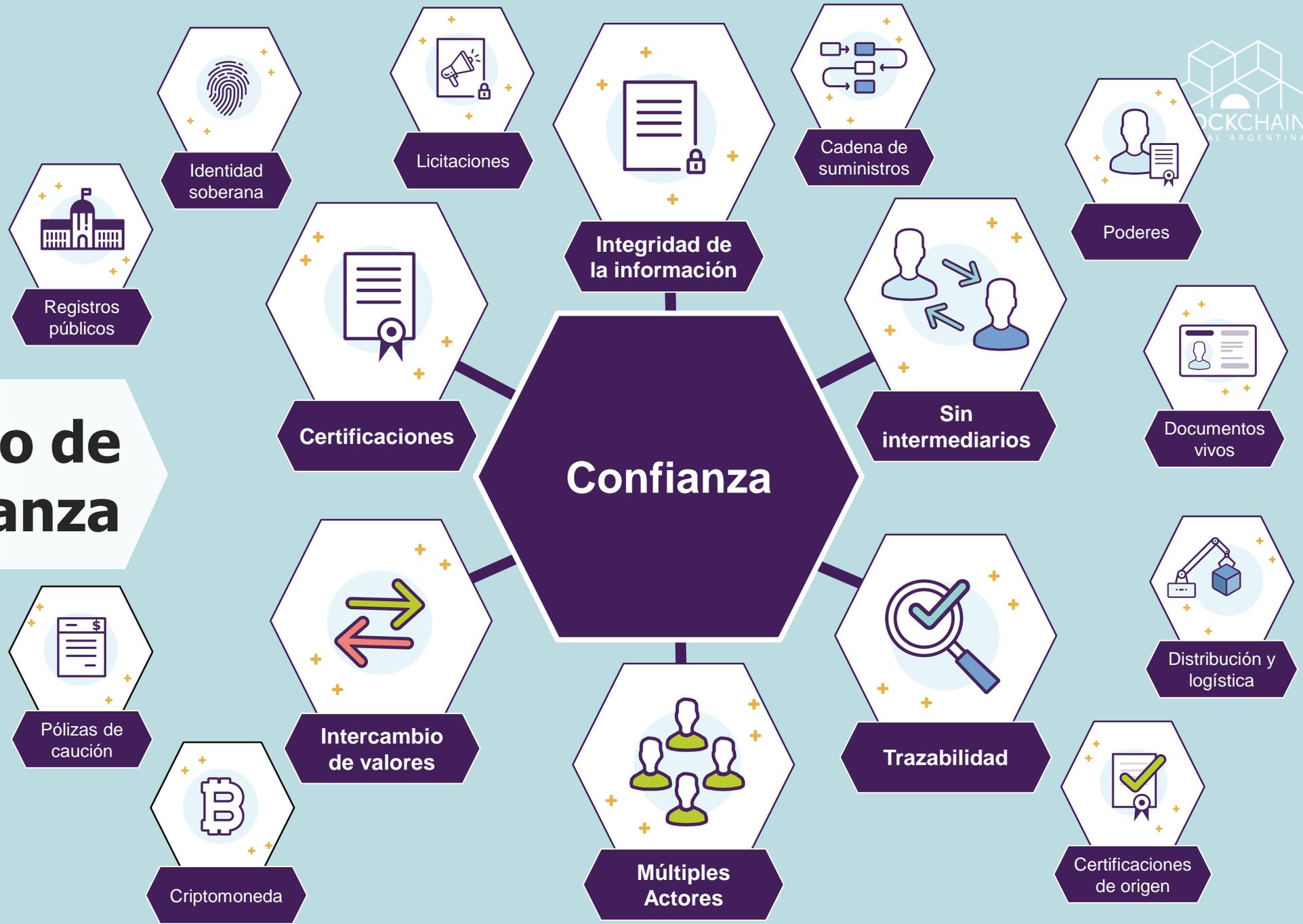
**Registro de
datos online
incorruptible**



**Imposible
alterar datos**

**Apoyado
en una
comunidad
de pares**

Servicio de confianza



El origen



Características



Autoría



Fecha cierta



**Información
inmutable**



Transparencia



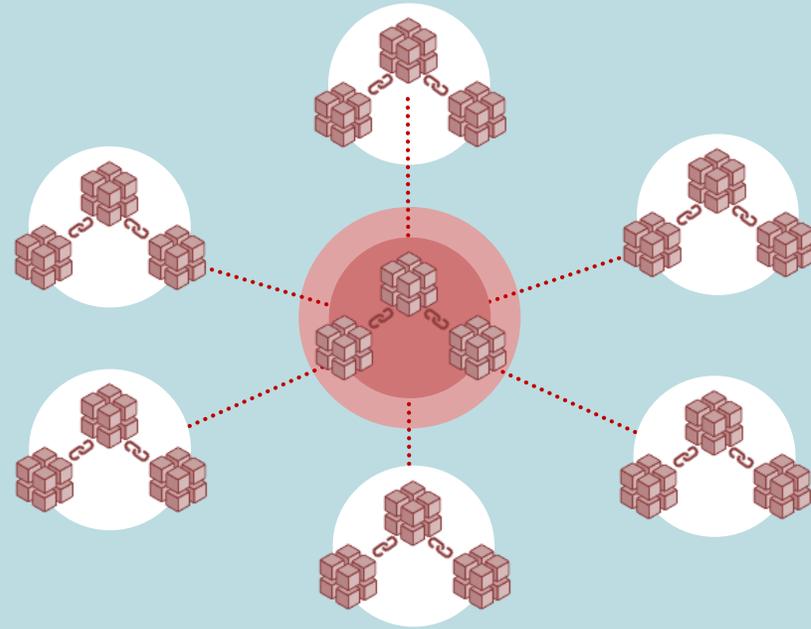
Sin Intermediarios



**Registro
Creciente**



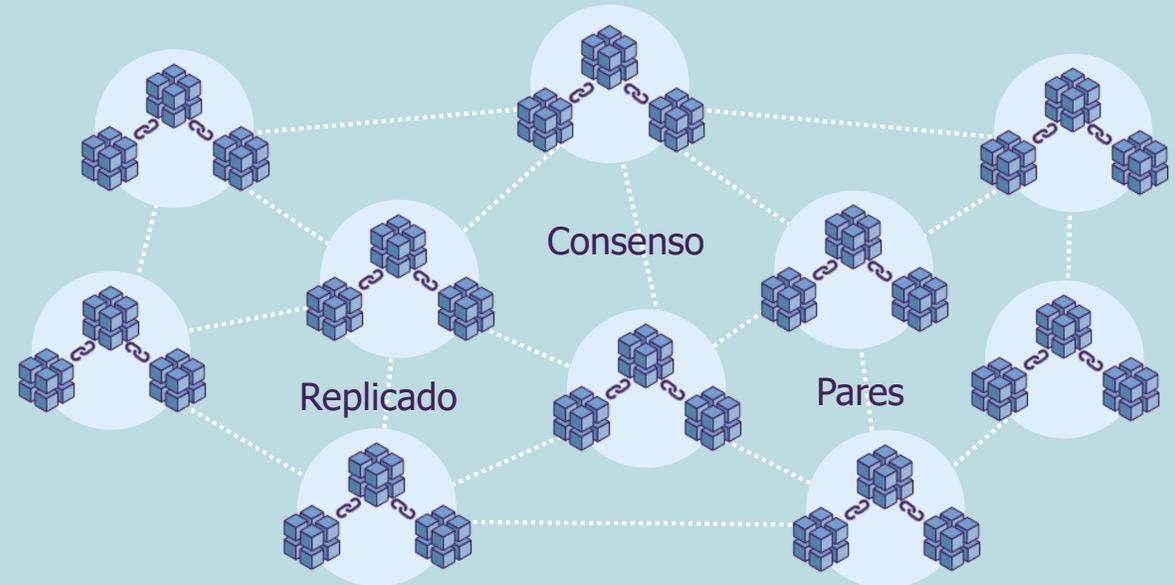
**Red
centralizada**



**¿Cómo
funciona?**
Una red de pares



**Red
distribuida**





Modificación



09e57c8da5b22b31
ed763a71cb6ef3a02
fd9a10c9f068bc1d0
6bc00c34703232

hash



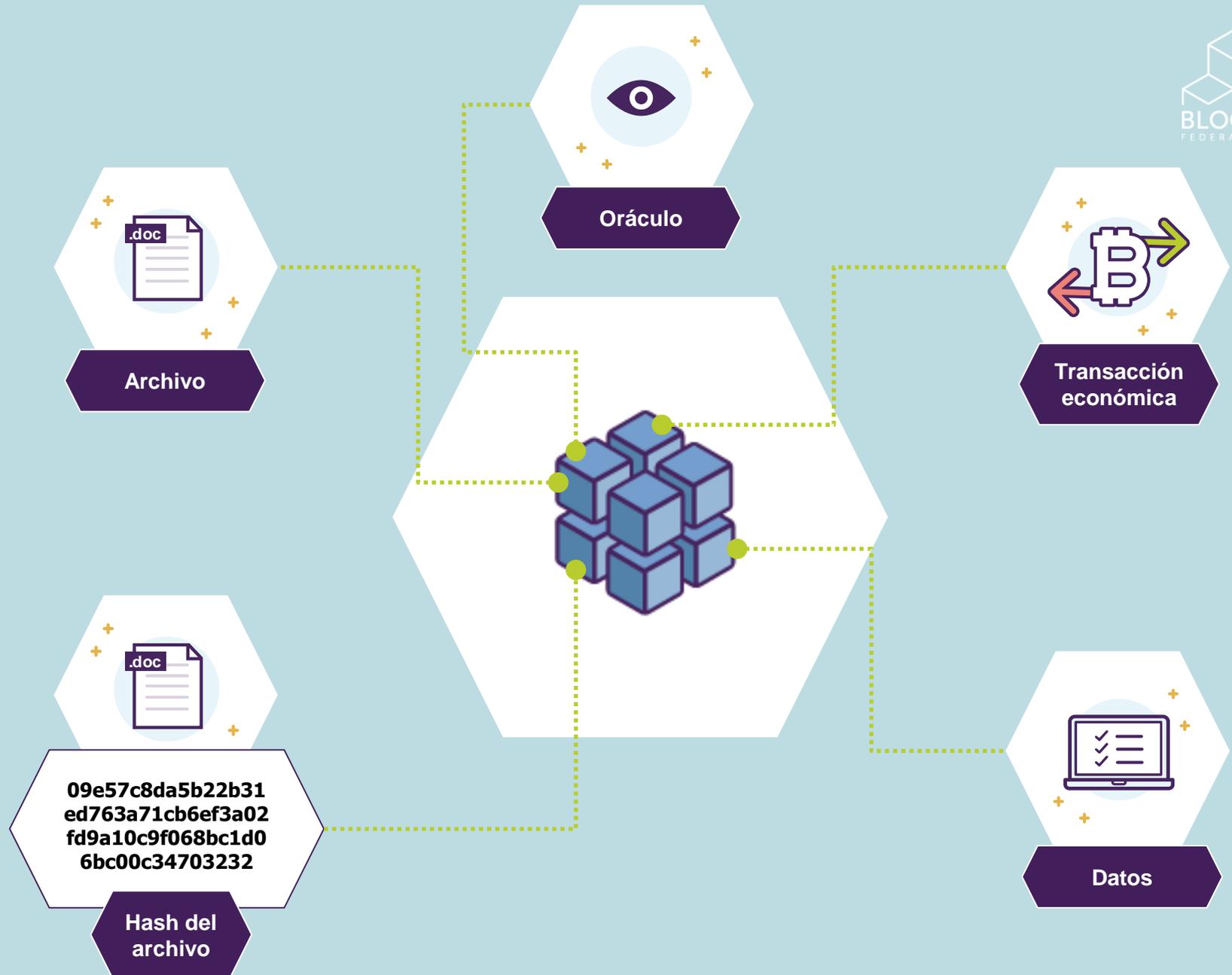
711112012c322261
414067094263e284
6de7a8cbcf2e56193
bd91adf7036bcd8

hash

¿Cómo funciona?
¿Qué es un hash?

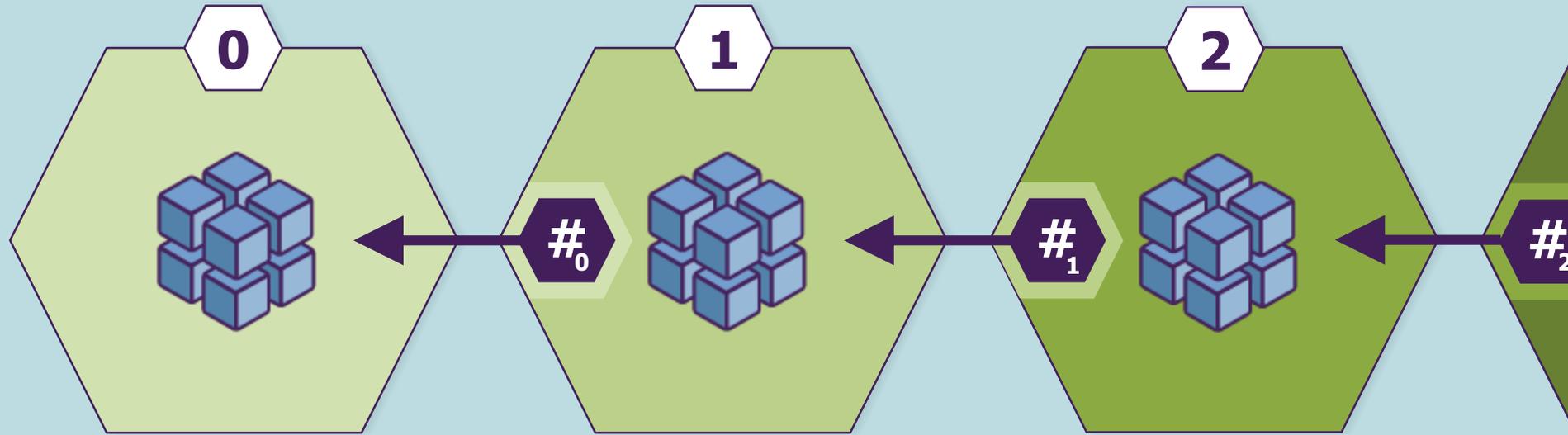
¿Cómo funciona?

Las transacciones



¿Cómo funciona?

El agregado de bloques

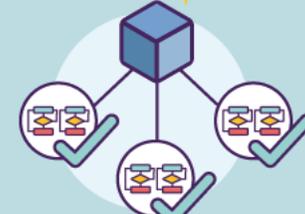




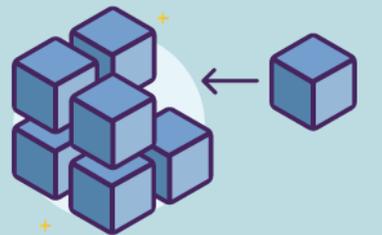
Se realiza una
Transacción



Se envía a la
Red de Pares



La red la verifica



Se suma a otras
transacciones...



Así, la transacción
queda completada.



Y se agrega a la cadena.

¿Cómo funciona?

El agregado de transacciones

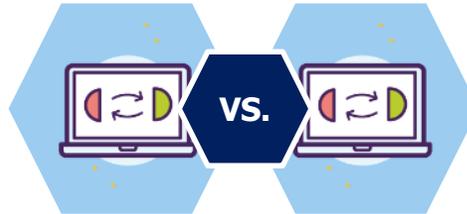
¿Cómo funciona?

Protocolos de consenso

Prueba de Trabajo



Participan todos los nodos de la red, de forma anónima



Compiten para sellar un bloque



El primer nodo que logre sellarlo obtiene una recompensa en criptomoneda

Prueba de Autoridad



Participan solo algunos nodos autorizados

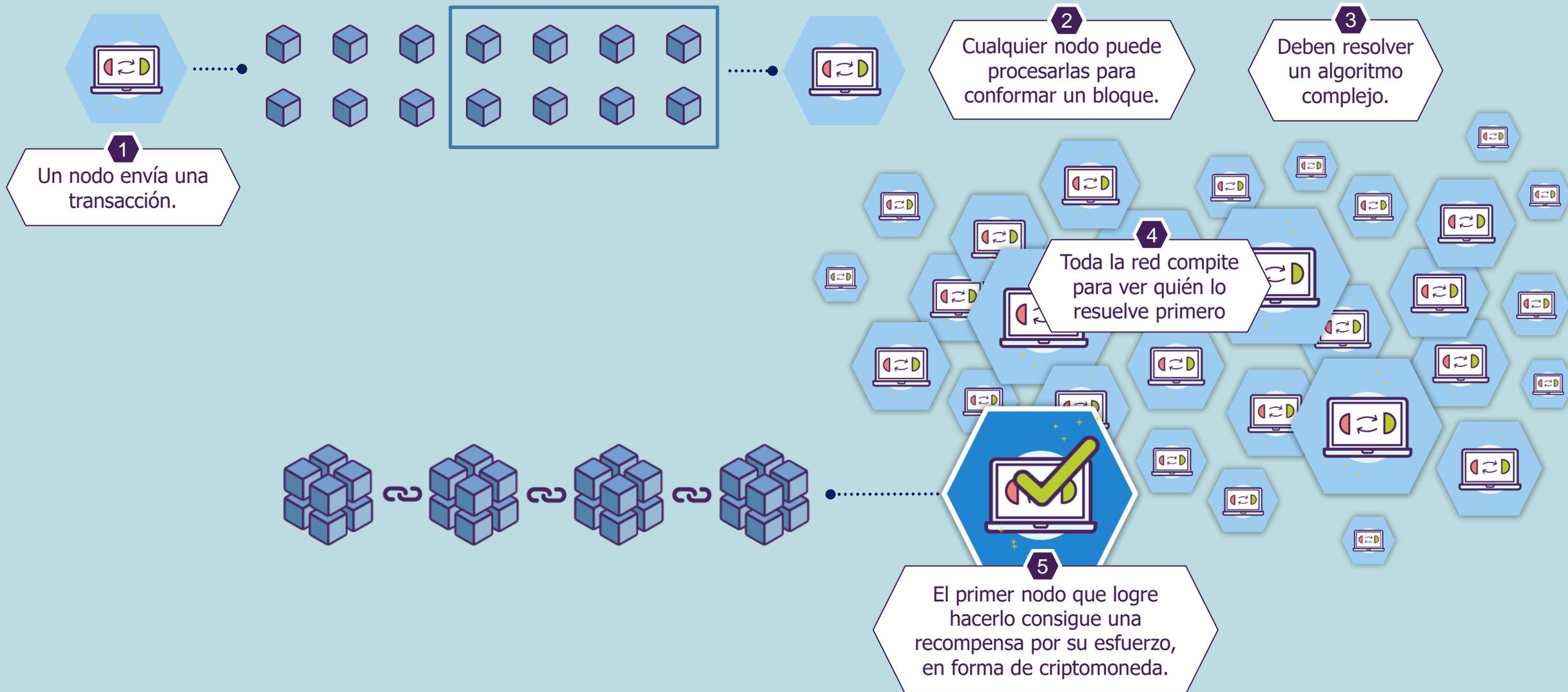


Su identidad debe estar verificada

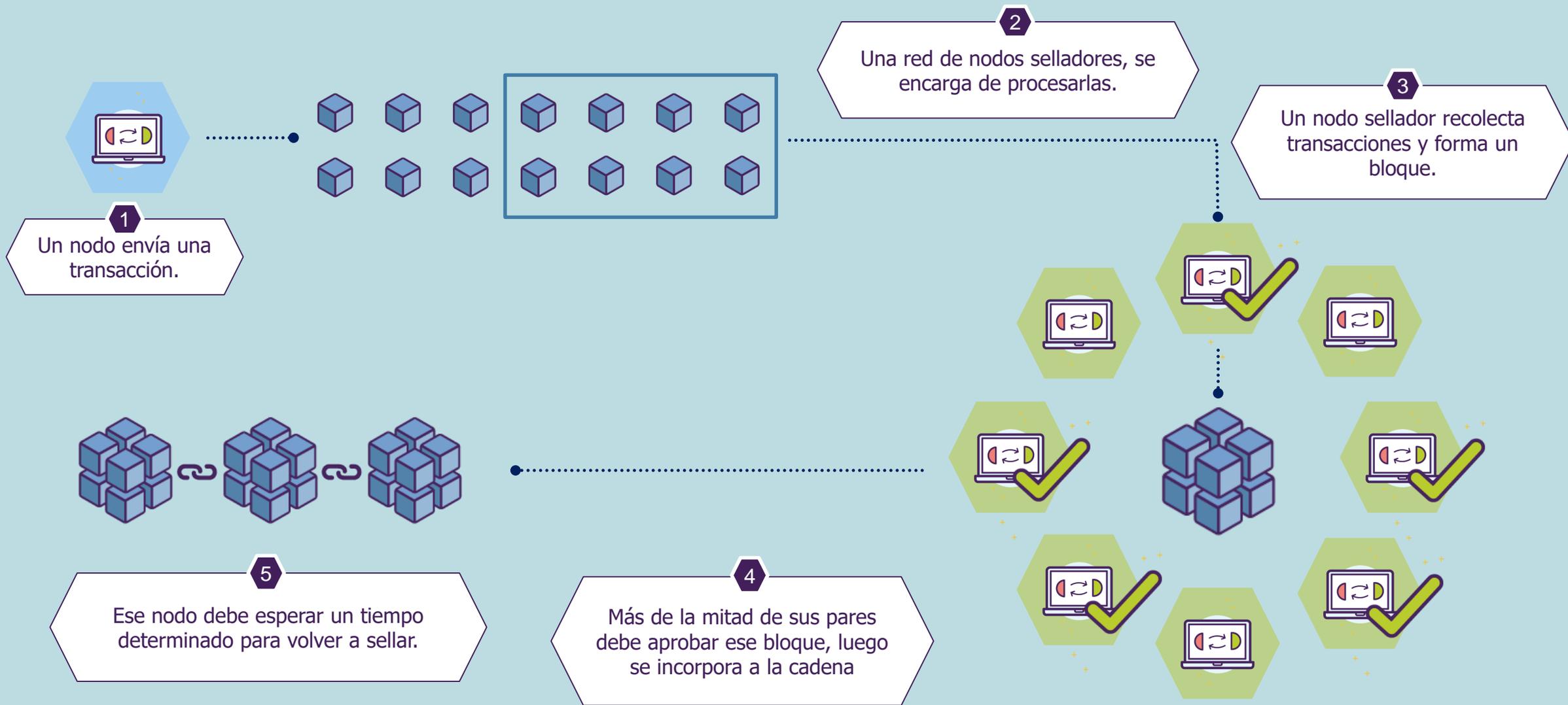


No hay criptomoneda circulante

Cómo funciona el modelo Proof of Work (Prueba de Trabajo)



Cómo funciona el modelo Proof of Authority (Prueba de Autoridad)





Smart Contracts

Licitaciones públicas



1

Publicación del pliego

Los términos de la convocatoria son públicos e inalterables.



2

Oferentes

Todo aquel que compre el pliego de la licitación lo puede hacer de forma digital.



3

Presentación de ofertas

Garantía de ofertas secretas.



4

Cierre

El *smart contract* deja de aceptar ofertas en una fecha determinada.



5

Apertura de sobres

Se asegura la transparencia y confidencialidad del proceso.



6

Evaluación

Aquellas propuestas que no cumplan con los requerimientos pueden ser automáticamente descalificadas y todo se puede fiscalizar.



7

Adjudicación

Se puede notificar automáticamente al ganador y ejecutar los procesos administrativos vinculados.

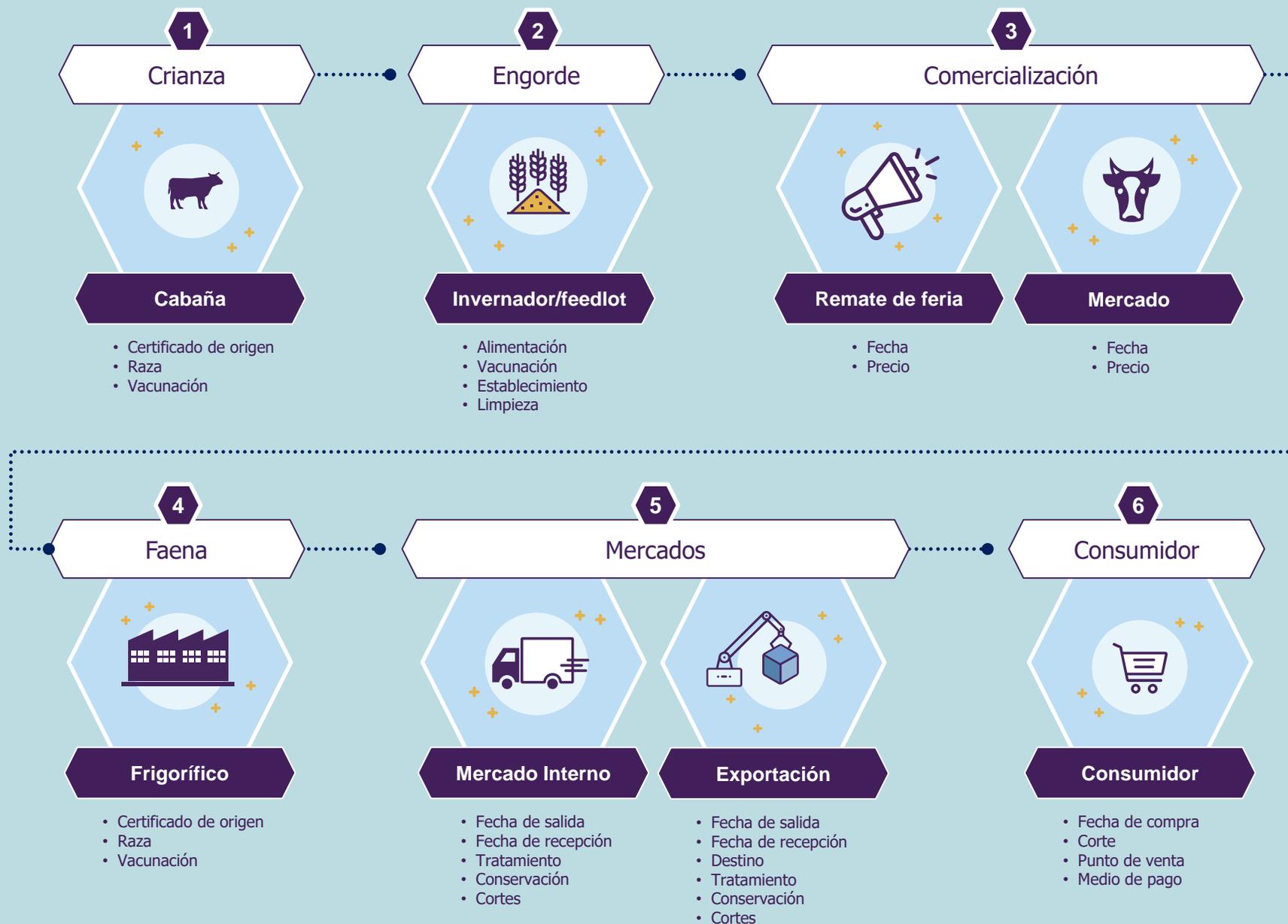


8

Ejecución del contrato

Se pueden fiscalizar las ordenes de compras y las etapas de cumplimiento hasta el fin del proceso.

Cadena de producción de carne vacuna



Trazabilidad de productos mediante Blockchain

BLOCKCHAIN



Registro

Información inalterable y verificable



- Certificado de origen
- Fecha de producción
- ...



- Número de lote
- Fecha de envasado
- Dirección
- ...



- Llegada y salida de planta
- Dirección
- Rutas
- ...



- Fecha de recepción
- Dirección
- Fecha de puesta en góndola
- ...



Smart Contract

Acciones preestablecidas entre las partes y ejecutadas automáticamente

- Control de pedido
- Control de calidad contra especificaciones
- Pago al proveedor

- Control de pedido
- Control de calidad contra especificaciones
- Pago al proveedor

- Control de pedido
- Control de calidad contra especificaciones
- Pago al proveedor



Oráculos

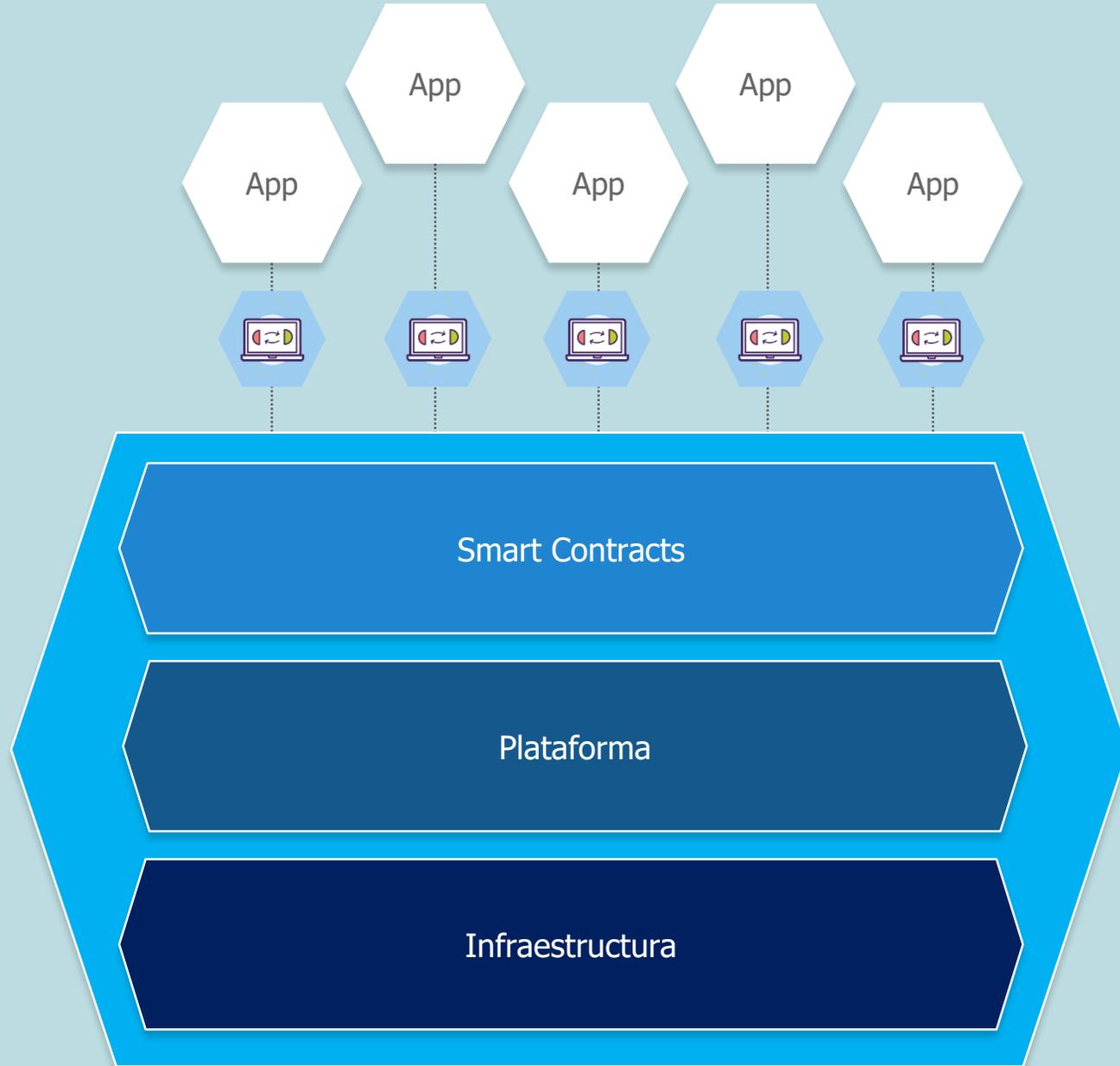


Oráculos



Oráculos

Una plataforma sobre blockchain



DNI

Licencia de
conducir

Historia académica

Casos de uso

Identidad Digital Soberana

Historia clínica

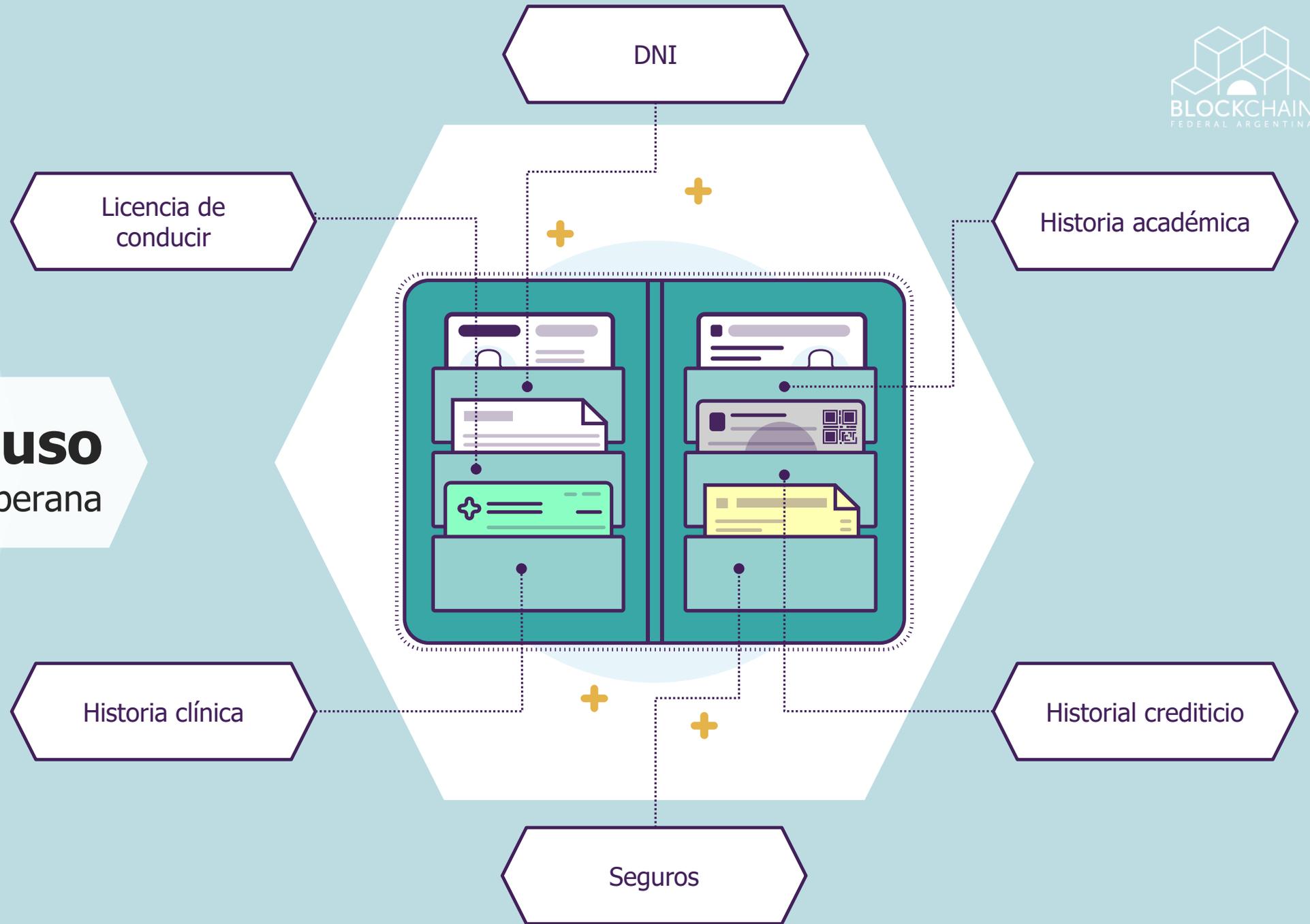
Historial crediticio

Seguros



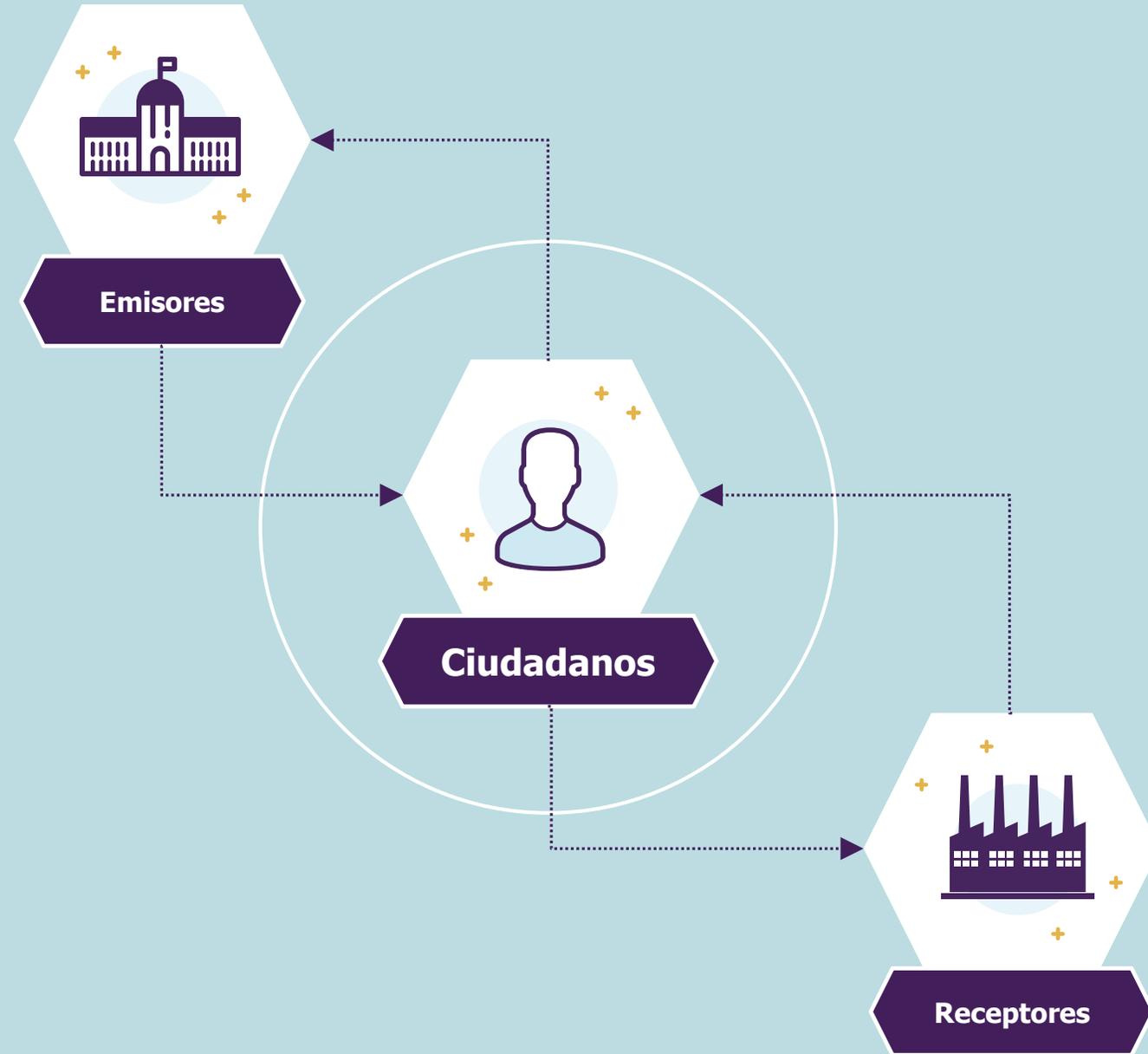
Casos de uso

Identidad Digital Soberana



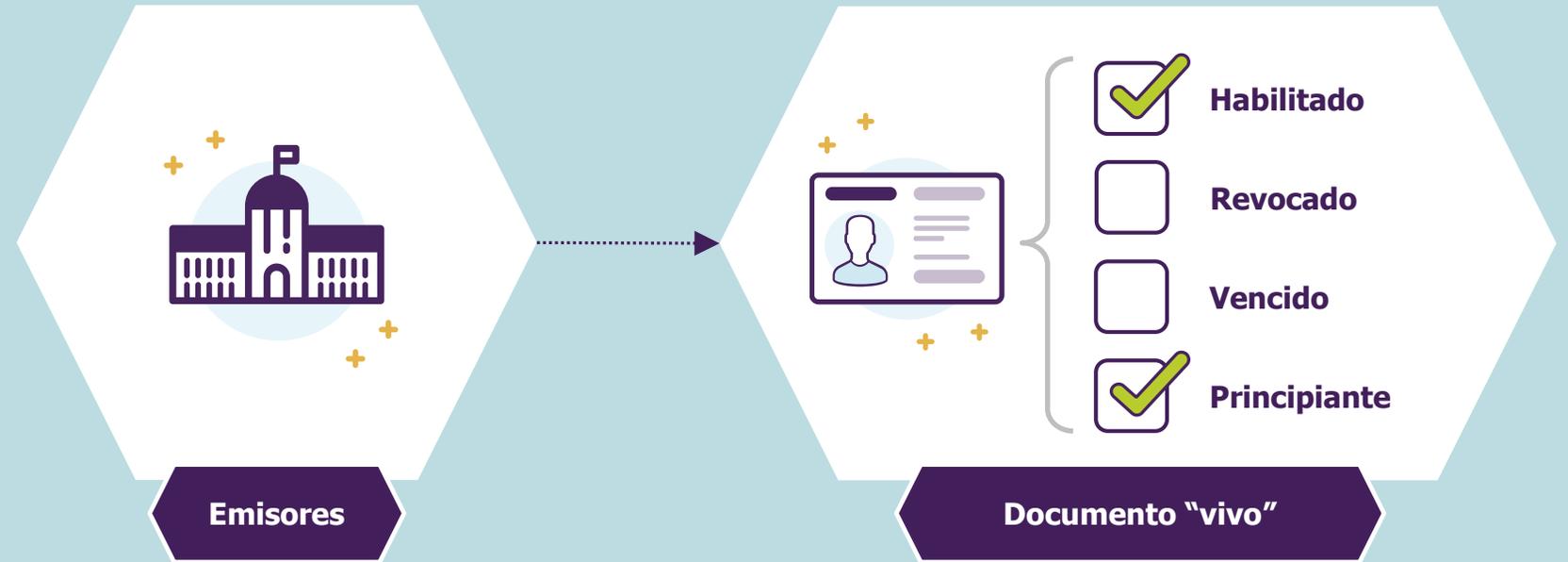
Casos de uso

Identidad Digital Soberana



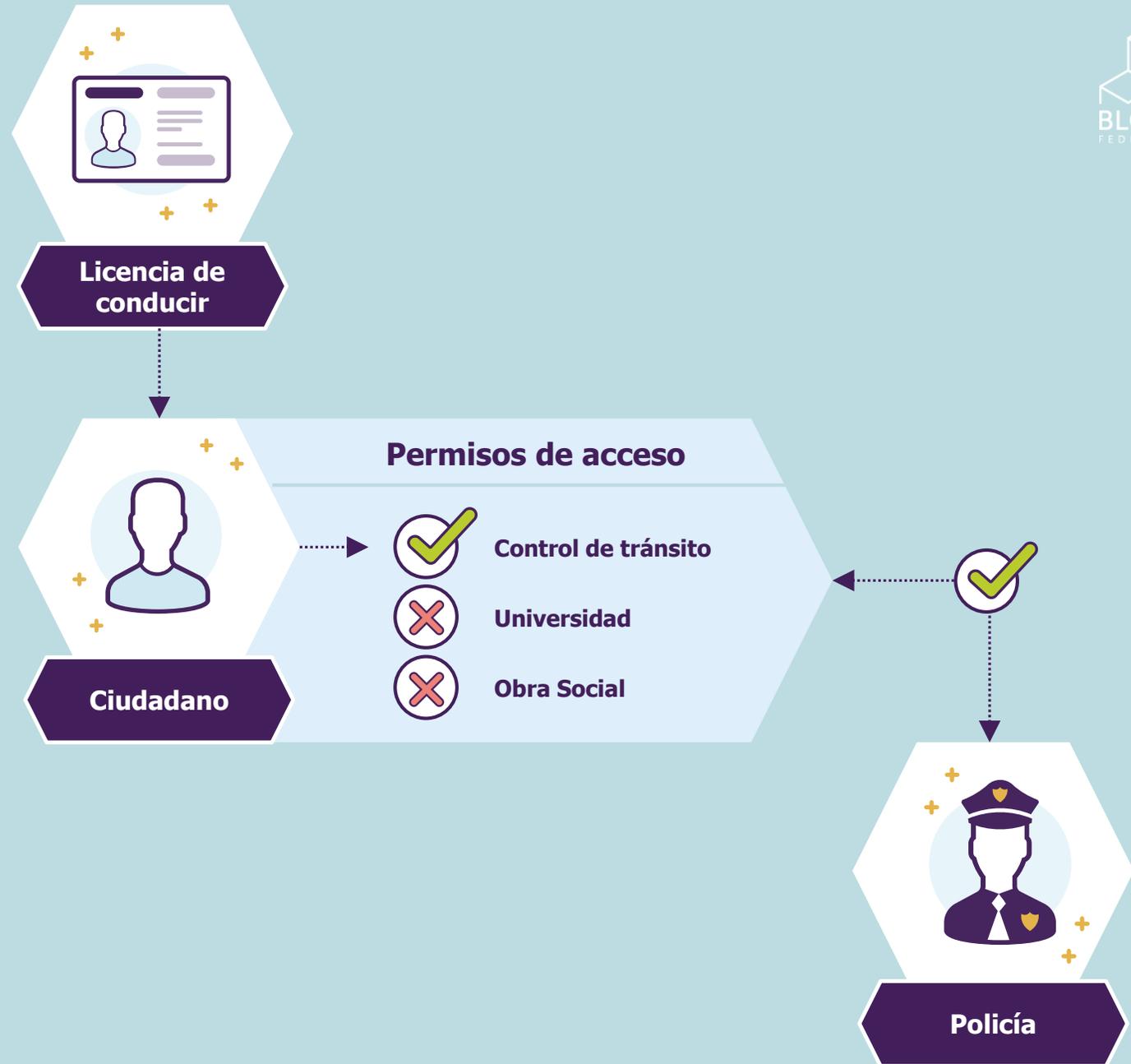
Casos de uso

Identidad Digital Soberana



Casos de uso

Identidad Digital Soberana



Casos de uso

Identidad Digital Soberana

Documento en papel



- Estático
- Estado inmutable
- Permisos irrevocables
- Sin garantías



Documento digital



- Digital
- Estático
- Estado inmutable
- Permisos irrevocables
- Firma digital



Documento en portadocumentos



- Digital
- Vivo
- Estados dinámicos
- Permisos modificables
- Verificado minuto a minuto
- Garantías de Blockchain

Identidad Digital Soberana

Emisores

Ciudadano



Receptores



Compañía de seguros



Gimnasio



Dirección General de Licencias



Agencia Nacional de Seguridad Vial



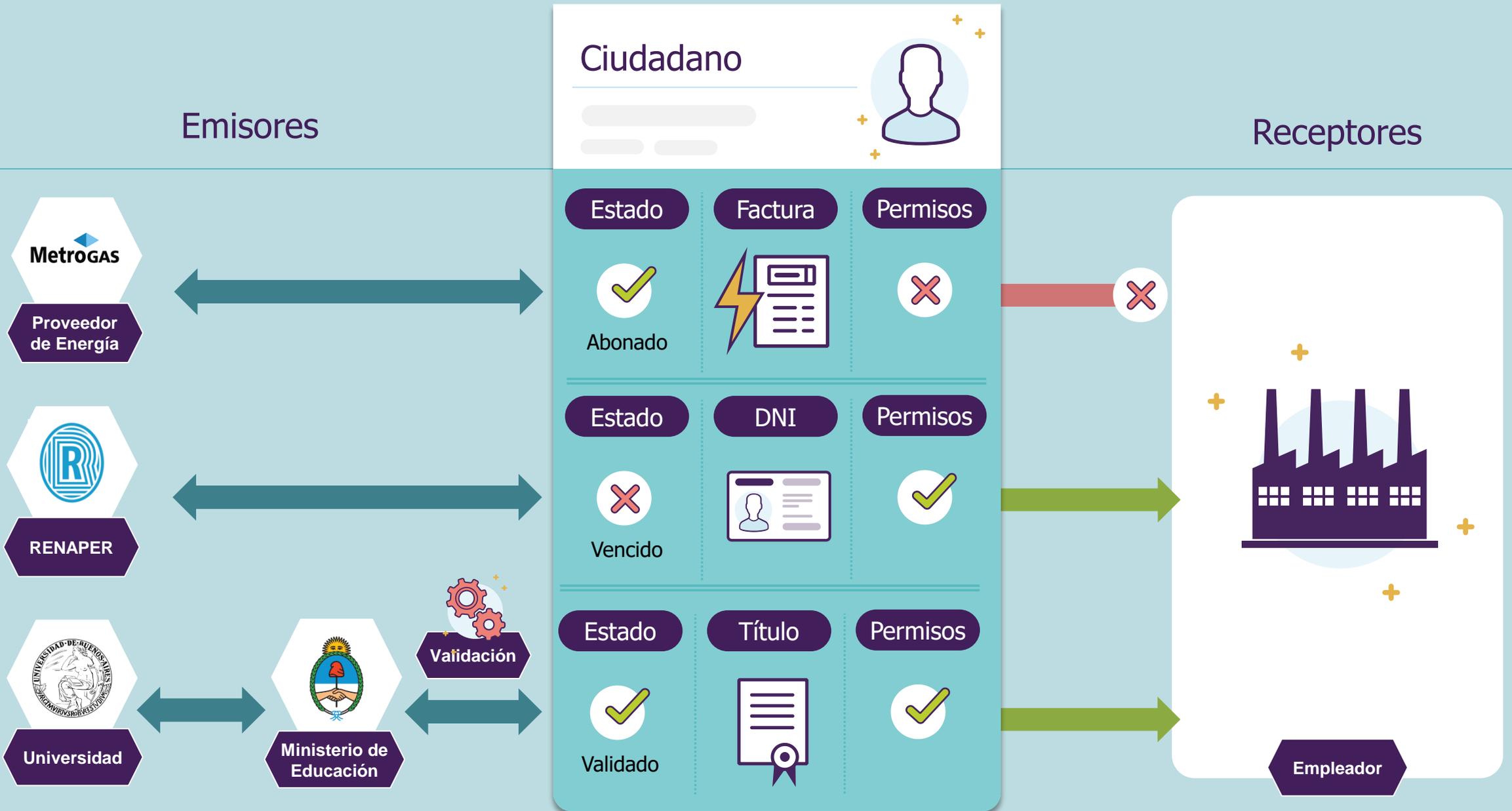
Validación

Estado	Póliza	Permisos
 Abonado		
Estado	Membresía	Permisos
 Vencido		
Estado	Licencia de conducir	Permisos
 Habilitado		



Oficial

Identidad Digital Soberana





Características de blockchain



Autoría



Fecha cierta



Información inmutable



Transparencia

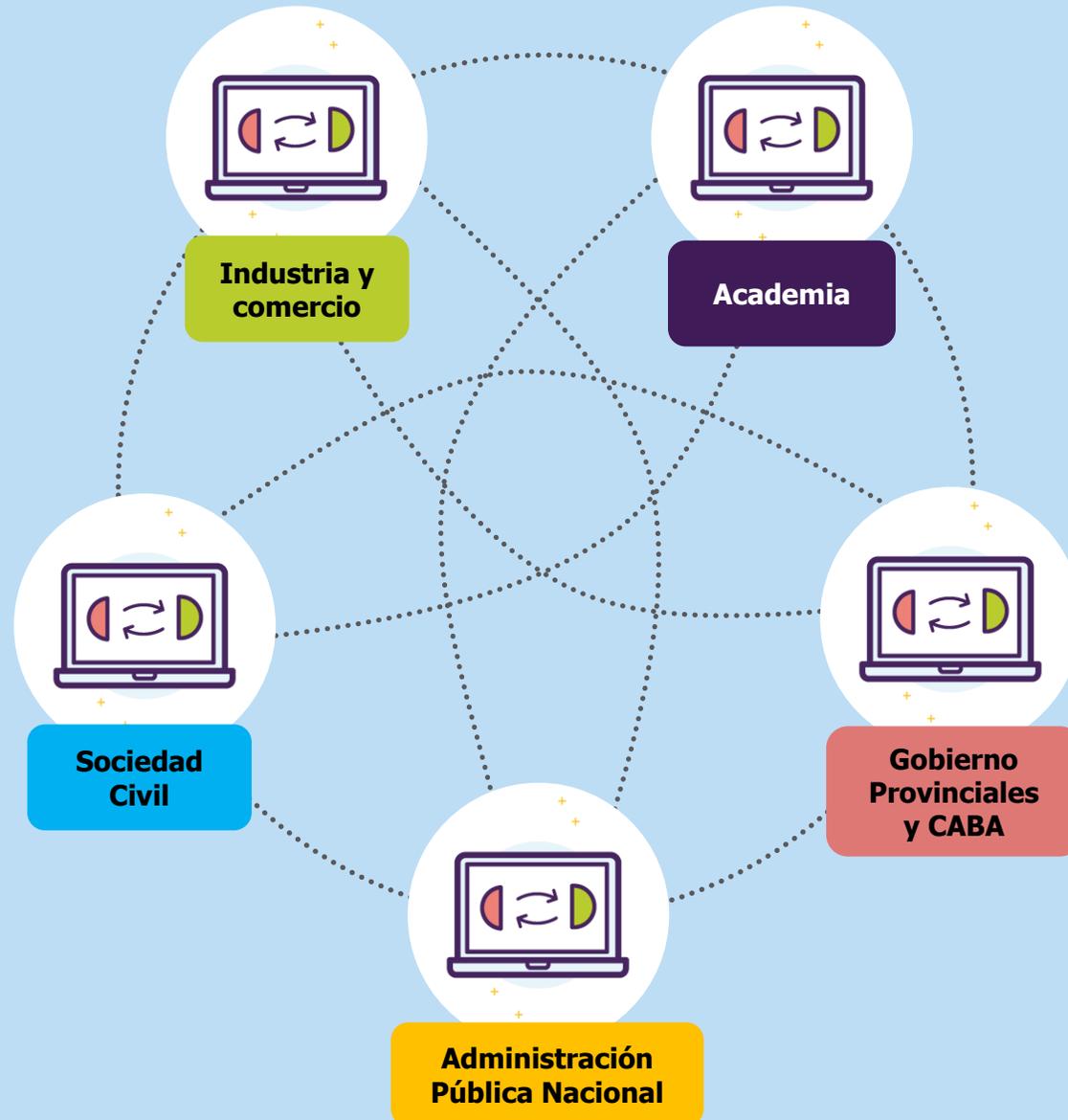


Sin Intermediarios

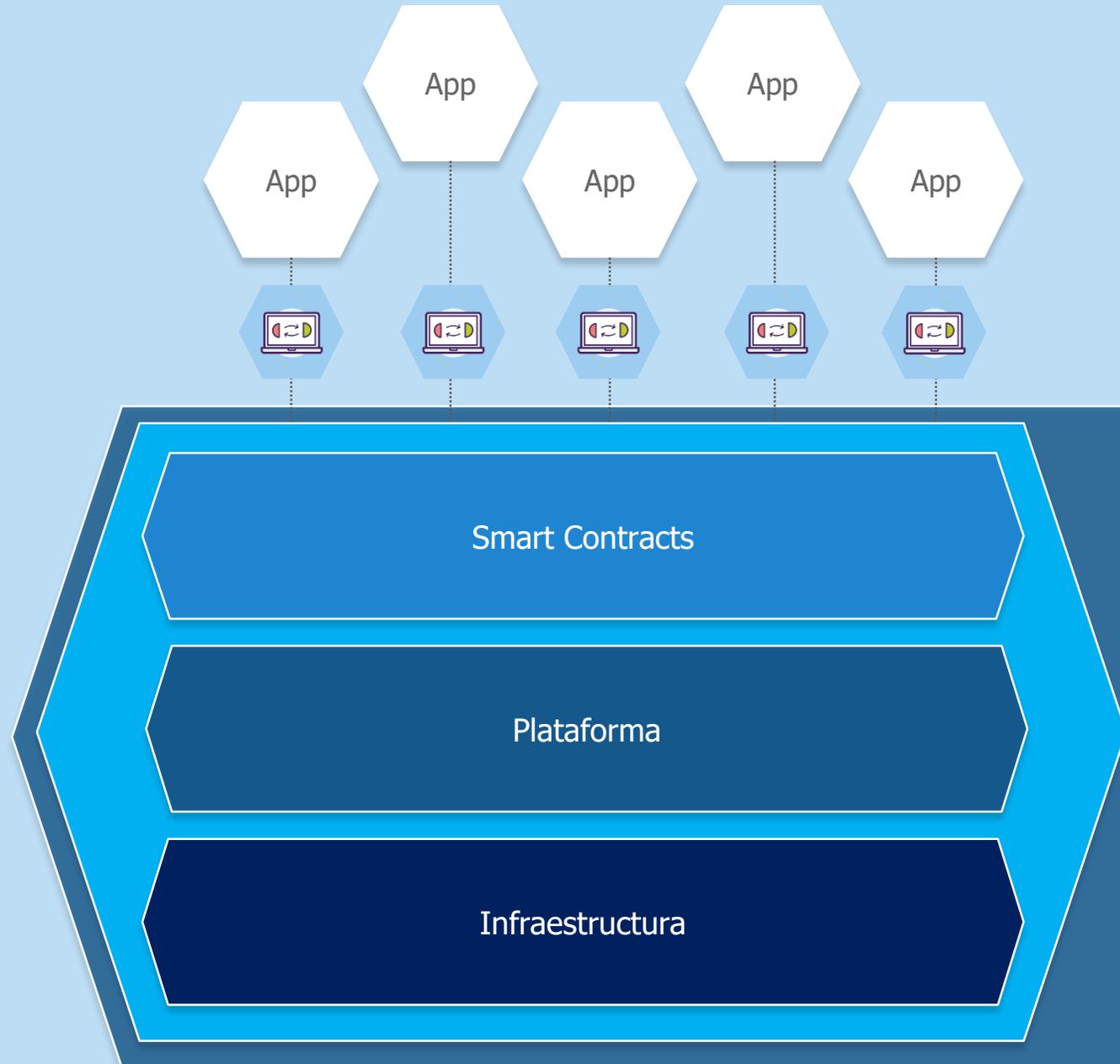


Registro Creciente

Múltiples Partes Interesadas



Modelo



Modelo



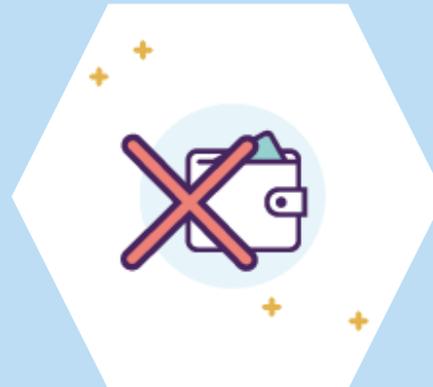
Permisiónada



Modelo liviano



**Sin
criptomonedada**



**Transacciones
gratuitas**



Software libre



**Almacenamiento
Off-chain**

Tecnología

Ethereum



ethereum

Tecnología

Nodos



Selladores



Transaccionales



Verificadores

Tecnología

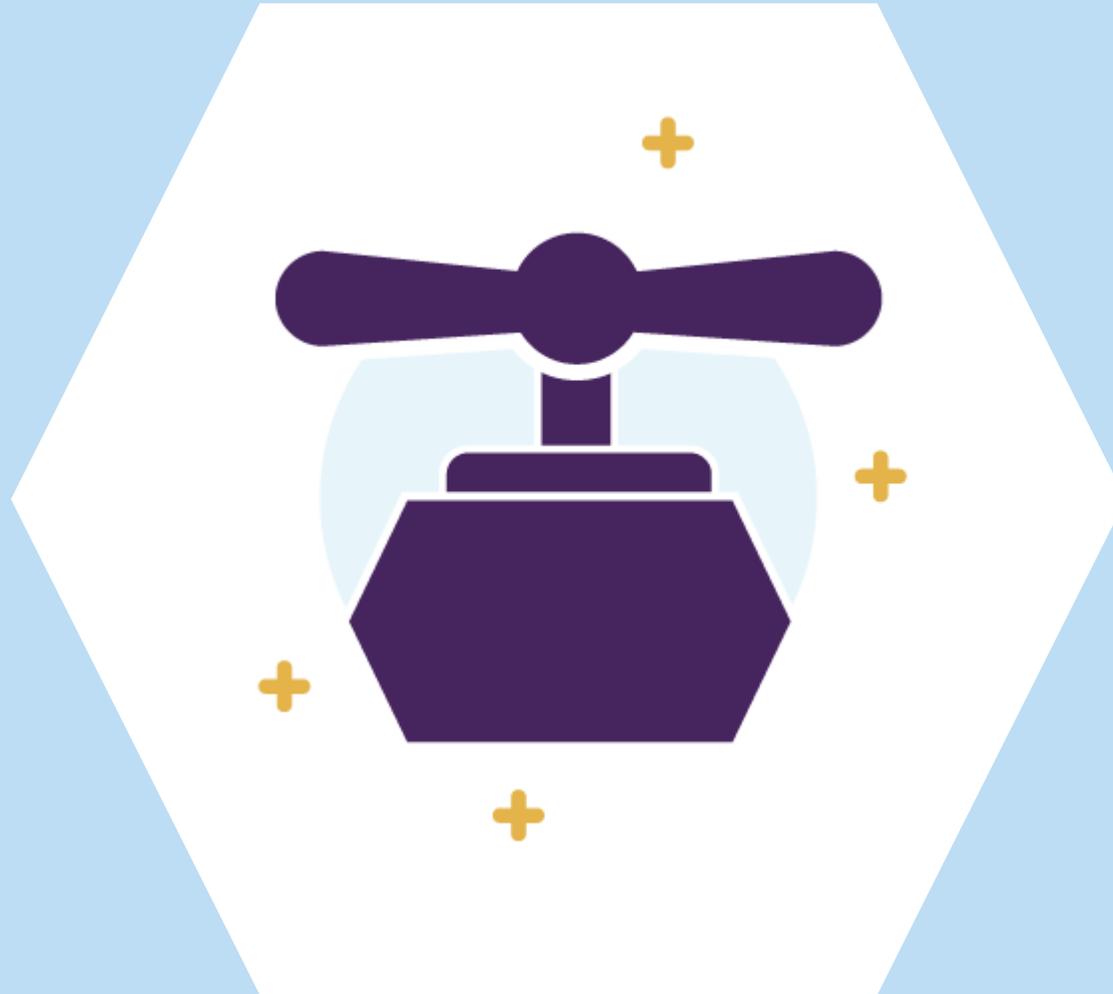
Nodos Selladores



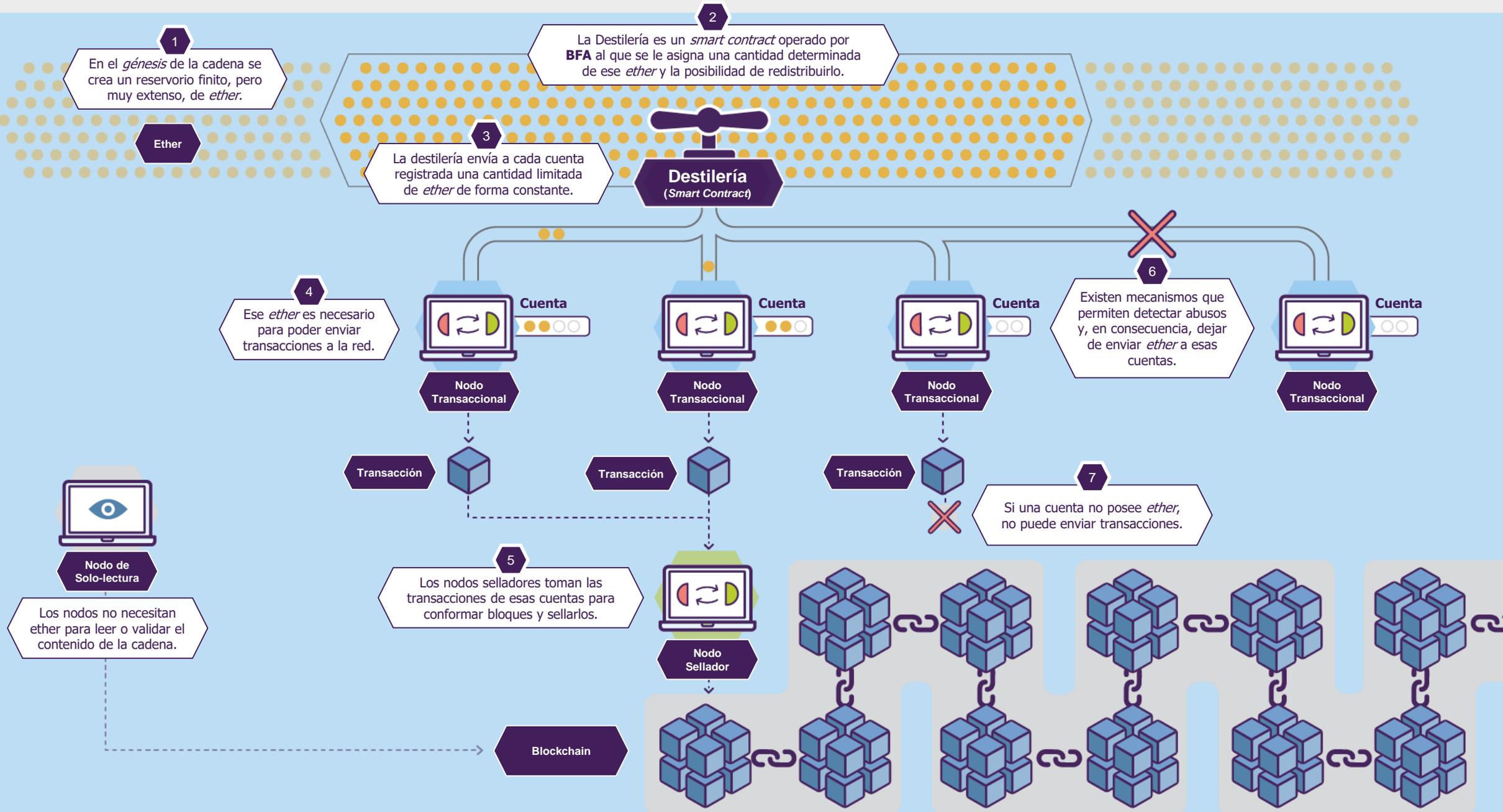
- ❖ **ARIU**
- ❖ **UN Córdoba**
- ❖ **UN San Juan**
- ❖ **UN Rosario**
- ❖ **UN La Plata**
- ❖ **DGSI**
- ❖ **Prefectura Naval Argentina**
- ❖ **ONTI**
- ❖ **ASI GCBA**
- ❖ **CABASE** (Bs. As., Bahía Blanca, Mendoza, Puerto Madryn y Posadas)
- ❖ **EVERIS**
- ❖ **SYT**
- ❖ **Universidad de Palermo**
- ❖ **Marandu Comunicaciones SE**
- ❖ **SMGP**
- ❖ **Última Milla S.A.**
- ❖ **Superintendencia de Riegos del Trabajo**
- ❖ **IPLAN**
- ❖ **Agencia Nacional de Seguridad Vial**
- ❖ **Belatrix**
- ❖ **Red Link**
- ❖ **Colegio de Escribanos de la Provincia de Bs. As.**

Tecnología

Destilería



Destilería



Tecnología

Monitoreo



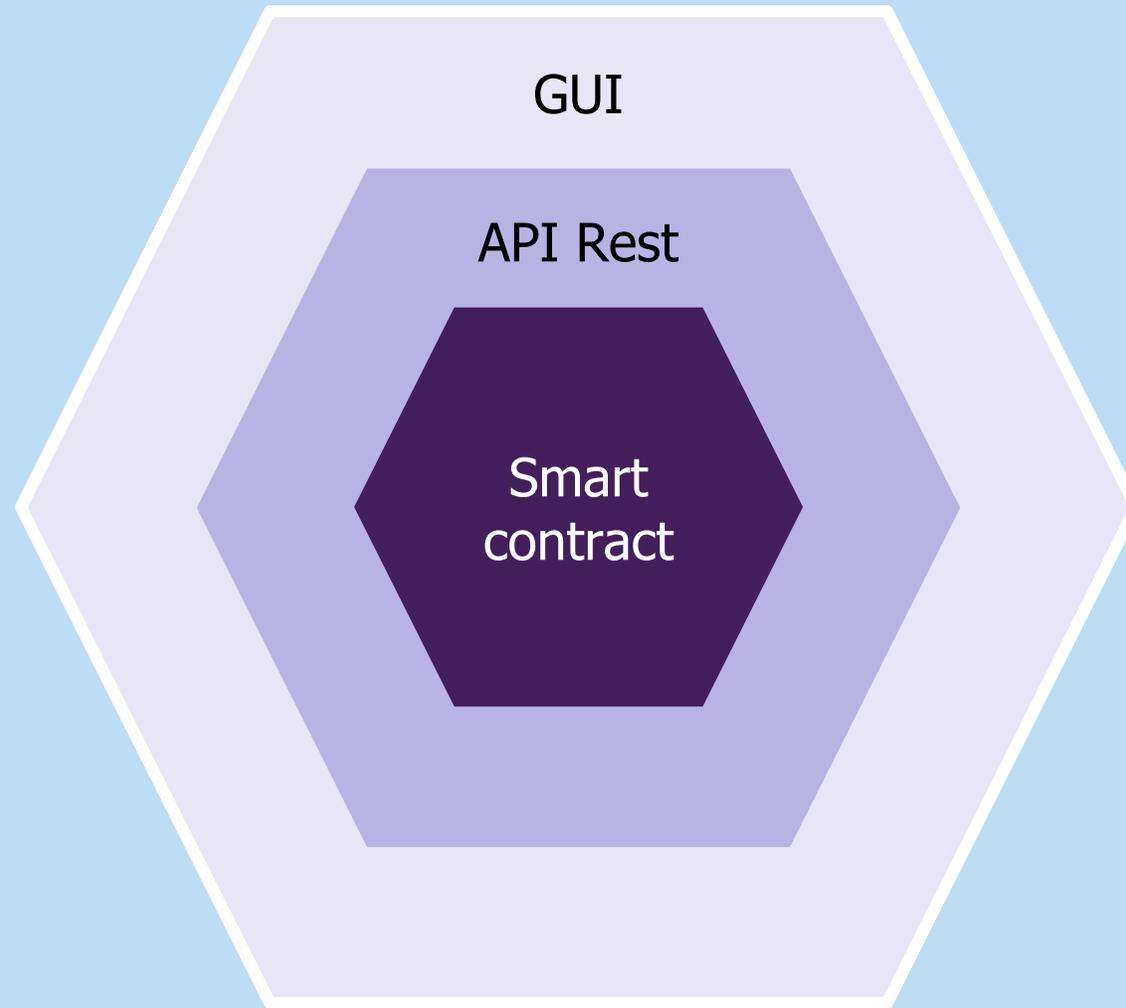
Tecnología

Sello de Tiempo



Tecnología

Sello de Tiempo



Tecnología

Sello de Tiempo en el BORA



1

Las secciones del BORA obtienen el Sello de Tiempo de BFA



2

Se publican en la web junto con un comprobante digital



3

Cualquier usuario puede verificar el sellado en la web de BFA

Tecnología

Sello de Tiempo

Sello de Tiempo

El servicio de Sello de Tiempo de BFA permite demostrar digitalmente que el contenido de cualquier documento existió en un momento y que desde entonces, no ha cambiado.

1. Sellar

2. Obtener recibo

Verificar

Paso 1: Iniciar sellado

Seleccioná un archivo para generar un Sello de Tiempo. El servicio generará un *hash* (un código criptográfico asociado a dicho documento) y lo enviará a la blockchain. A continuación, se descargará automáticamente un recibo digital **temporario** (.rd.temp) que luego podrás usar para obtener el recibo digital **definitivo** (.rd) en la pestaña Obtener recibo.

Importante: El documento seleccionado nunca se sube a la red, garantizando su privacidad.



Arrastrá un archivo aquí

ó

Seleccioná un archivo

Tecnología

Sello de Tiempo

Sello de Tiempo

El servicio de Sello de Tiempo de BFA permite demostrar digitalmente que el contenido de cualquier documento existió en un momento y que desde entonces, no ha cambiado.

1. Sellar

2. Obtener recibo

Verificar

Paso 2: Obtener recibo digital definitivo

Para obtener el recibo definitivo (.rd) de un Sello de Tiempo se debe tener el documento original y el recibo digital temporario (.rd.temp). Al seleccionar ambos archivos, el recibo se descargará automáticamente y podrás visualizar en este sitio el día y la hora en que el hash del documento original fue sellado en la Blockchain Federal Argentina.

Seleccioná el archivo original



Arrastrá el archivo **original** aquí

ó

Seleccioná un archivo

Seleccioná el recibo digital temporario



Arrastrá el archivo **.rd.temp** aquí

ó

Seleccioná un archivo

Tecnología

Sello de Tiempo

Sello de Tiempo

El servicio de Sello de Tiempo de BFA permite demostrar digitalmente que el contenido de cualquier documento existió en un momento y que desde entonces, no ha cambiado.

1. Sellar

2. Obtener recibo

Verificar

Verificar un sello de tiempo

Para verificar un Sello de Tiempo se debe tener el documento original y el recibo digital definitivo (rd). Podrá verificar el día y la hora en que el hash del documento original fue sellado en la Blockchain Federal Argentina.

Seleccioná el archivo original

Nombre del archivo: **Brief BFA.pdf**
Hash del archivo:
d9d145af4a78148f67fddd9ccbafebced3722b7c94453
5b8970d4bb092a9668d6

Seleccioná otro archivo

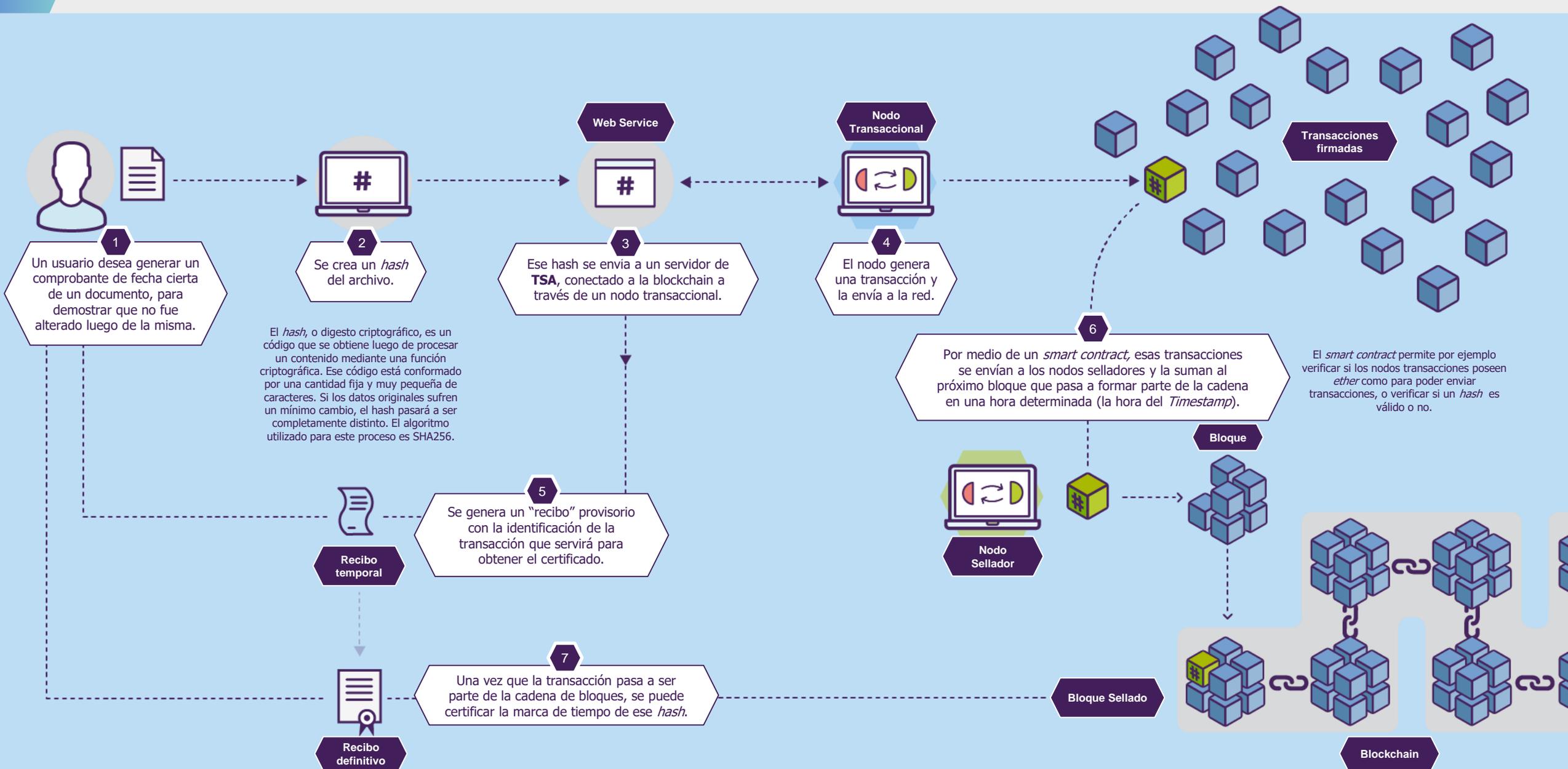
Seleccioná el recibo digital definitivo

Brief BFA.pdf.rd

Seleccioná otro archivo

✓ El archivo Brief BFA.pdf fue ingresado en el bloque 414890 el 22/10/2018 18:01:08

Sello de Tiempo

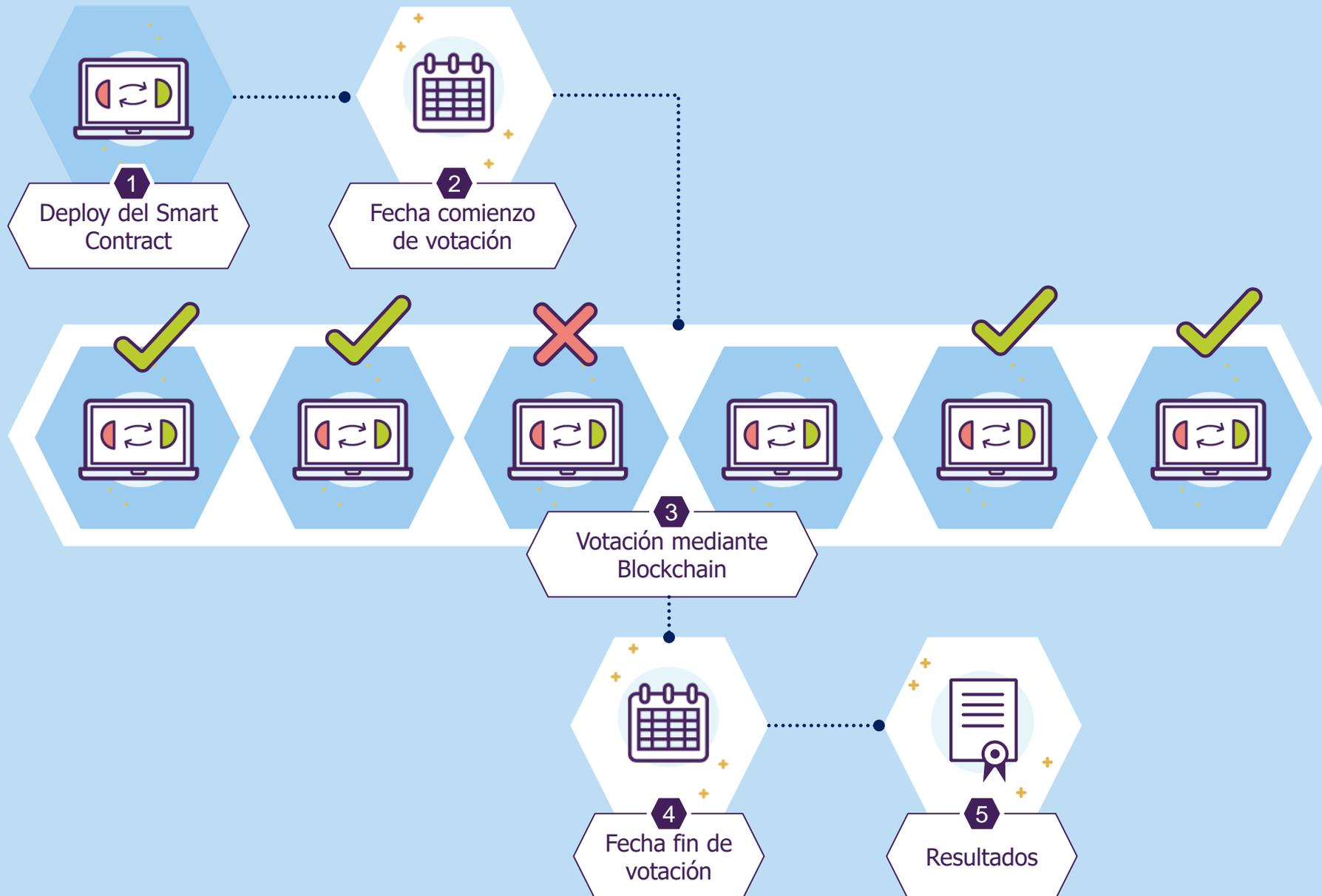


Tecnología

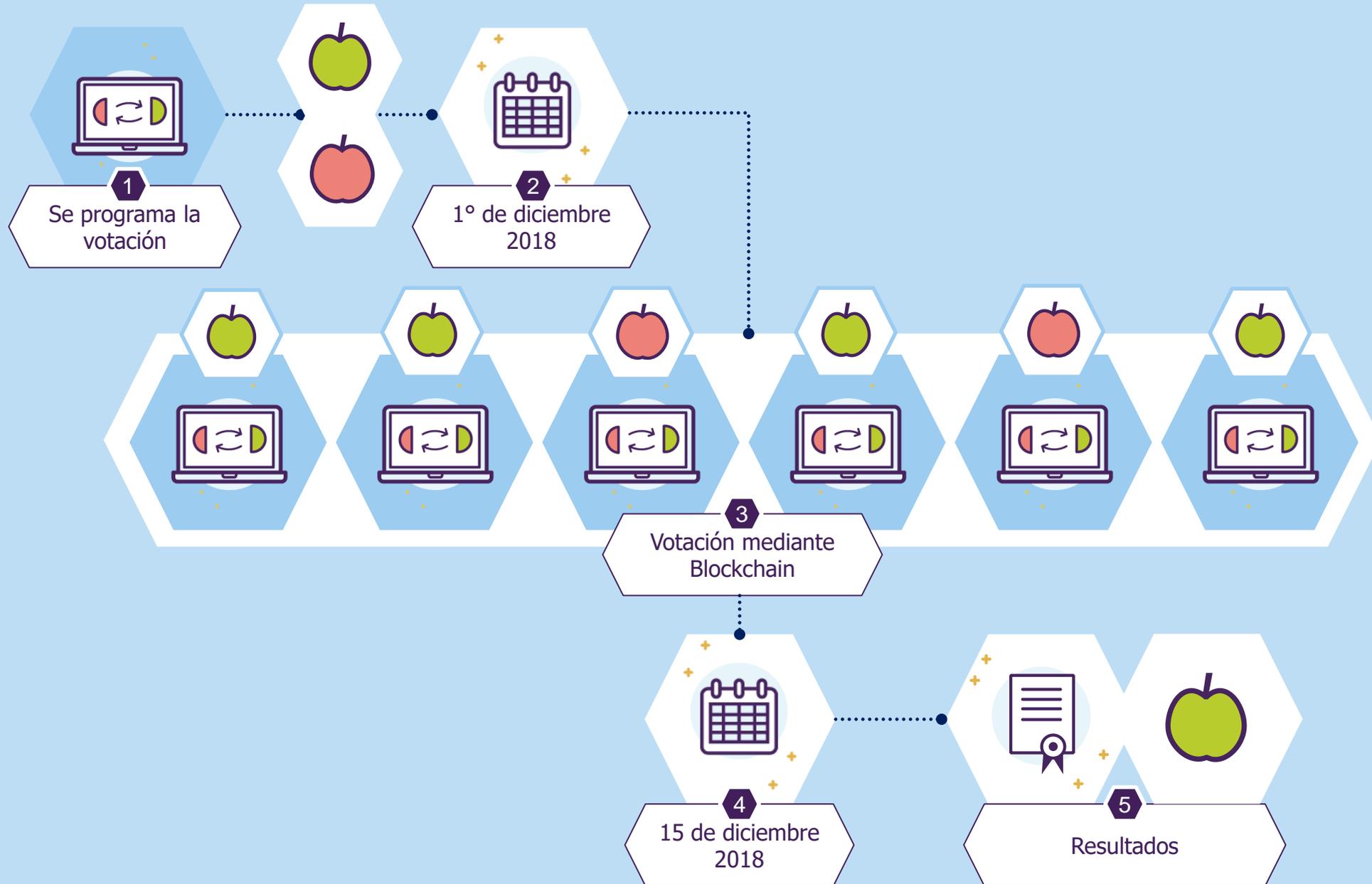
Votación



Smart Contracts



Smart Contracts



Gobernanza



**¿Quiénes pueden
participar?**

Gobernanza

¿Cómo se puede participar?

Usuarios



Pueden enviar transacciones a la red de forma gratuita.



Solo pueden desplegar nodos transaccionales o read-only.

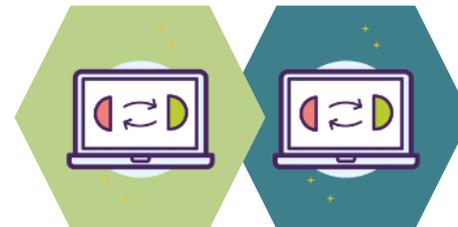


Pueden desarrollar sus propias aplicaciones sobre la red.

Partes



Pueden participar en la toma de decisiones respecto al futuro de la iniciativa.



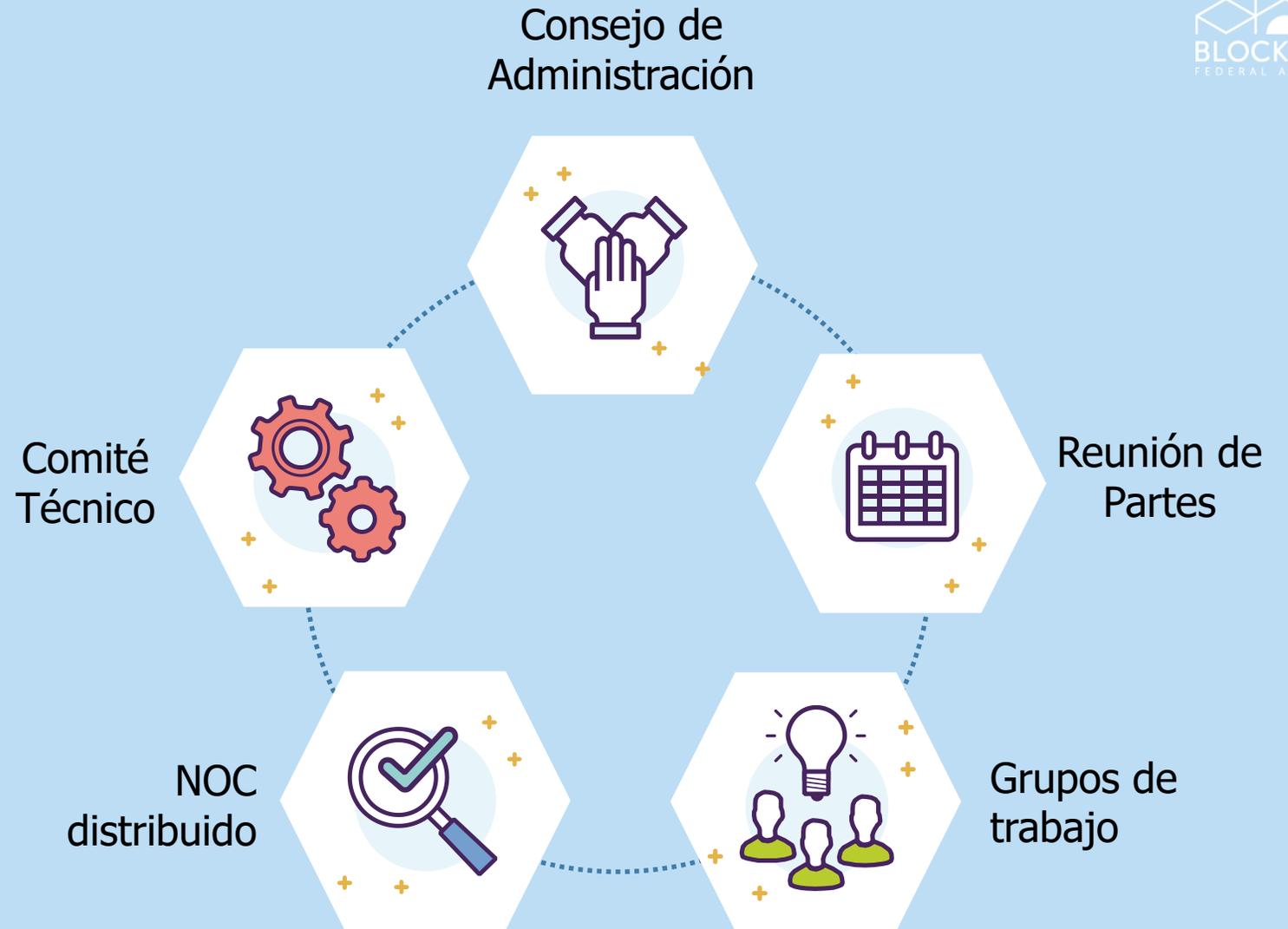
Pueden aportar a la infraestructura del core de la red con nodos selladores.



Deben firmar un acuerdo de participación.

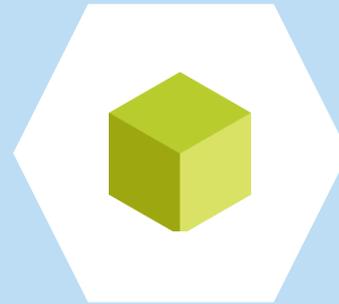
Gobernanza

Órganos de
Participación y Gestión



Gobernanza

Grupos de Trabajo



Grupos de
trabajo

Tecnología

Casos de Uso

Monitoreo

Comunicación

Legales

Gobernanza

Antecedentes



CÁMARA ARGENTINA DE
Internet

A R I U

Asociación Redes de Interconexión Universitaria

Partes

Academia



Administración Pública Nacional



Gobiernos Provinciales y CABA



Industria y Comercio



Sociedad Civil



Desarrollo Digital

Casos de Uso

- 📦 **Sello de Tiempo** (BFA)
- 📦 **Smart Voting** (BFA)
- 📦 **Firma Conjunta de Documentos** (GDE)
- 📦 **Libros Digitales SAS** (Secretaría de Modernización)
- 📦 **Carpeta Ciudadana** (Ciudad de Buenos Aires)
- 📦 **Portadocumentos Digital** (RedLink)
- 📦 **Actas Universitarias** (Universidad Nacional de Córdoba)
- 📦 **Edición digital del Boletín Oficial de la República Argentina** (Secretaría Legal y Técnica)
- 📦 **Publicación de Altas y Transferencias de Dominios de Internet** (NIC Argentina)
- 📦 **Pagarés Digitales** (Garbarino)
- 📦 **Publicación de Altura de Ríos** (Prefectura Naval Argentina)
- 📦 **Licitaciones Públicas** (Oficina Nacional de Compras)
- 📦 **Pólizas Digitales** (Superintendencia de Riegos del Trabajo)
- 📦 **Publicación de Datos Abiertos** (ENACOM)
- 📦 **Títulos Universitarios** (SIU)
- 📦 **Sistema de Documentos Notariales Digitales - GEDONO** (Colegio de Escribanos CABA)

Perspectiva Regional





<https://bfa.ar>



contacto@bfa.ar

Taller de Casos de Uso



Juntarse en grupos

Taller de Casos de Uso

2

Pensar en 1 caso de uso por grupo e identificar:

- **Actores involucrados:** diferentes empresas, organizaciones, dependencias, direcciones o unidades, entre otros, que interactúan entre sí.
- Cuál es **el activo en juego** a lo largo de la cadena: algún bien, material o inmaterial, que posea algún tipo de valor. Puede ser información.
- Cuáles son las **certificaciones** que se emiten a lo largo de la cadena: certificados que garanticen la validez de cierta información, procesos o activos.
- Si hay instancias en las que se requiere asegurar **la integridad de la información:** hitos a lo largo de la cadena en los que se necesita garantizar la integridad de la información que se registra.

Taller de Casos de Uso

3

Diagramar el proceso del caso



Taller de Casos de Uso

4

Identificar qué puede aportar
Blockchain en ese proceso



Taller de Casos de Uso

5

Puesta en común



¡MUCHAS GRACIAS!