
BLOCKCHAIN
FEDERAL ARGENTINA

ÍNDICE

Introducción

Blockchain Federal Argentina es la primera plataforma multiservicios de alcance federal basada en *cadena de bloques*.

A través de esta iniciativa se constituye un espacio colaborativo y de vanguardia que no solo funcionará como soporte de ideas para empresas e instituciones, sino que será el primer espacio digital común de estas características en el país: un ecosistema ideal para emprendimientos que busquen una infraestructura sólida, transparente y confiable.

¿Qué es Blockchain?

Blockchain es, a grandes rasgos, una tecnología diseñada para administrar un registro de datos online, un libro contable, o una bitácora, caracterizada por ser prácticamente incorruptible.

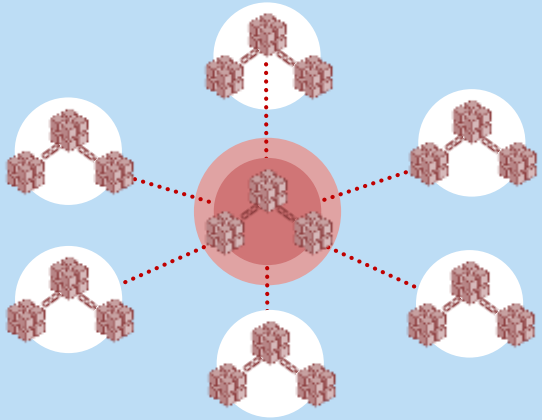
En lugar de tener información centralizada en una sola computadora y con unos pocos usuarios con capacidad de modificarla, una cadena de bloques está replicada a lo largo de toda una serie de computadoras bajo un modelo de red de pares, que agregan datos solo a partir del "consenso" (acuerdo) de las partes.

Blockchain tiene una particularidad que hasta el momento no se daba en el mundo digital: es imposible que ninguna persona, ni siquiera quienes almacenan una copia de la información puedan alterar datos en la cadena de bloques.

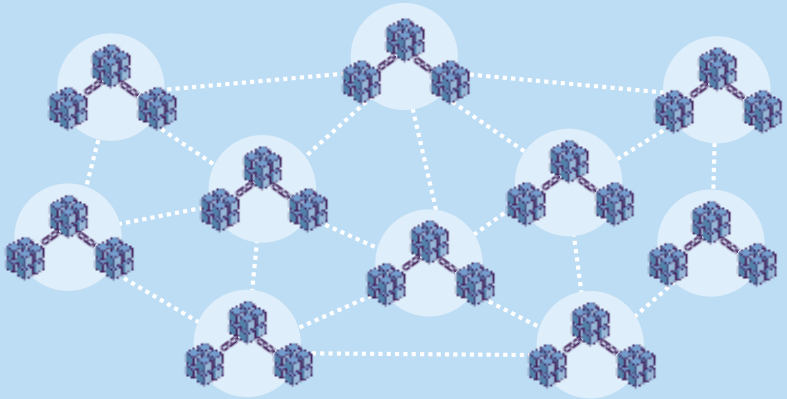
BLOCKCHAIN

¿Qué es Blockchain?

Blockchain es una tecnología diseñada para funcionar de forma horizontal.



En redes centralizadas, el ataque a un nodo crítico pondría en riesgo a toda la estructura.



En una red de Blockchain, todos los nodos que sellan transacciones (llamados selladores o mineros) acuerdan contribuir con el mantenimiento y el procesamiento del registro.

Y lo hacen bajo una plataforma distribuida: una estructura confiable y que puede sobrevivir tranquilamente si una de las partes de la red se ve comprometida.

BLOCKCHAIN

¿Qué es Blockchain?

Por su naturaleza, Blockchain permite realizar una serie de operaciones combinadas que por primera vez se pueden utilizar de manera conjunta en el mundo digital.

Autoría

Poder garantizar en cada transacción la identidad de las partes involucradas, ya que todas las transacciones son firmadas criptográficamente.

Fecha cierta

Certificación de la fecha y hora de la transacción

Inalterable

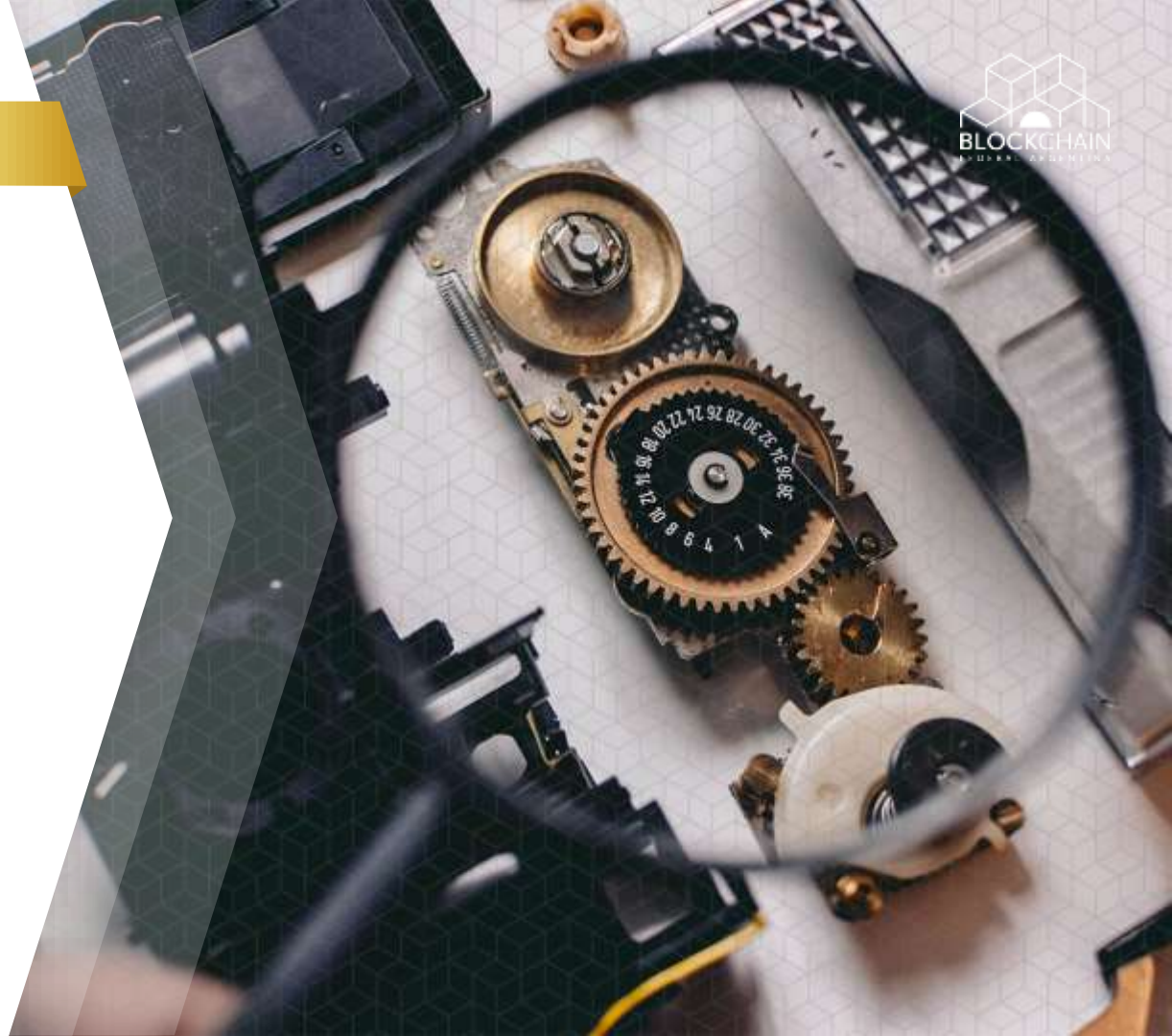
La información es inmutable e inalterable: no es posible modificarla ni borrarla, sin que los miembros de la red lo perciban.

¿Qué es Blockchain?

La función hash

Gran parte de la seguridad de la información en Blockchain se debe al uso de métodos criptográficos para encriptarla, y una de las principales herramientas para hacerlo son los llamados hash, o digestos criptográficos.

Un hash es un código que se obtiene al procesar información a través de una función. **Si modificamos aunque sea algo muy pequeño de esa información,** como el color de una foto, o simplemente agregar un acento en un documento de texto, **el hash va a cambiar completamente.** Los hash suelen llamarse digestos o resúmenes, porque normalmente tienen un tamaño fijo y de pocos dígitos, por ejemplo 64 caracteres en SHA-256.



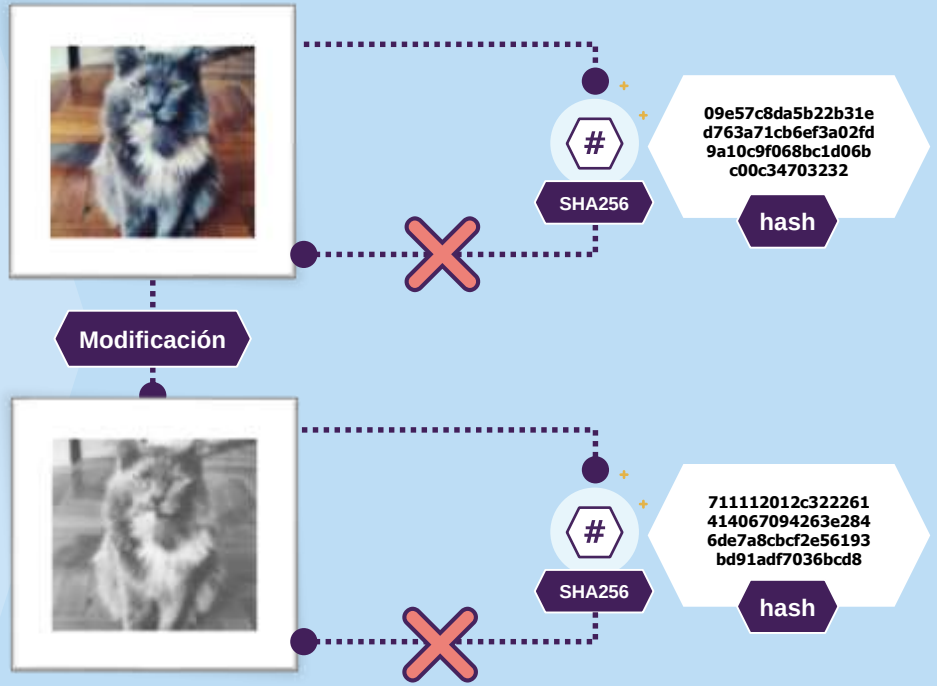
¿Qué es Blockchain?

La función hash

Así, **al registrar hashes de documentos, podemos tener la certeza de darnos cuenta si alguien cambia su contenido**, ya que esas modificaciones harían que el hash de la nueva versión sea completamente diferente.

Esta técnica nos permite dejar de lado la necesidad de almacenar, por ejemplo, fotos en Blockchain. Con solo almacenar el hash, y dejar esa foto en nuestra computadora, servidor o nube, tenemos la certeza de que vamos a darnos cuenta si alguien la modifica. O mejor aún**, le estamos ofreciendo al público la certeza de que nosotros, responsables de esa foto, no la podremos modificar sin que nadie se entere.**

Al mismo tiempo, como no se puede reconstruir la información original a partir de un hash, nos aseguramos que no le estamos brindando acceso a alguna persona no deseada, por más que ese hash esté registrado públicamente en la blockchain.

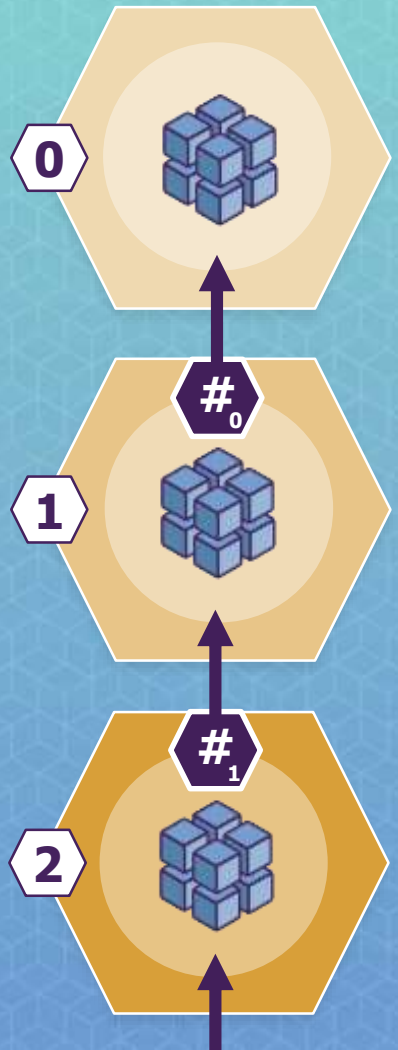


¿Qué es Blockchain?

La cadena de bloques

Los hash también juegan un papel elemental en la arquitectura de Blockchain. Cada bloque de información que se suma al registro posee necesariamente el hash del bloque de información anterior.

De nuevo, al procesar el hash de un bloque y almacenarlo en el siguiente, podemos tener la certeza de que el bloque anterior no puede ser modificado. Si alguien intentara cambiar algo, el hash de ese bloque sería completamente diferente al que ya tenemos registrado y toda esa red de pares que almacena el registro distribuido se percataría de ello.



¿Qué es Blockchain?

Las transacciones

Las operaciones que se realizan para agregar información a una blockchain son denominadas transacciones.

Su contenido puede ser muy variado y generalmente depende del tipo de red que se esté operando: hay blockchains que por medio de transacciones permiten subir archivos digitales al registro. Otras, orientadas estrictamente al intercambio de criptomonedas, toman forma de operaciones de compra-venta de activos. Una transacción puede ser simplemente una línea de texto, o incluso un hash de un documento almacenado fuera de la cadena de bloques.

Cada transacción es enviada a la red a través de un nodo, y se combina con otras transacciones para conformar un bloque. Cuando ese bloque se agrega a la cadena, la transacción queda incorporada definitivamente y se considera como "completada".

BLOCKCHAIN

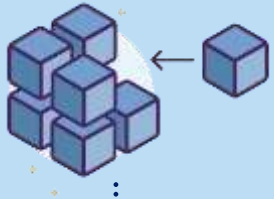
¿Qué es Blockchain?
Las transacciones

Alguien realiza una operación (conocida como transacción) en la blockchain.

Esa transacción se envía a una *red de pares*, formada por varias computadoras (nodos).

La red de nodos verifica tanto que la transacción esté firmada como que el usuario tenga recursos (combustible) para enviarla.

Una vez verificada, se combina con otras transacciones para crear un nuevo bloque de datos…



Así, la transacción queda finalizada (completada).

… y el nuevo bloque se agrega a la cadena, quedando ésta replicada en todos los nodos de forma permanente e inalterable.

¿Qué es Blockchain?

Criptomonedas

Si bien el uso de Blockchain no está estrictamente ligado al intercambio de bienes digitales, esta tecnología nació de la mano del Bitcoin, la primera criptomoneda.

Las criptomonedas son justamente monedas virtuales que se basan en cadenas de bloques para controlar la creación de unidades y verificar la transferencia de activos entre los usuarios. Como todas las divisas, su valor en gran parte está basado de la confianza que los usuarios pongan en ella. Pero al tener la particularidad de depender de Blockchain, esa confianza se apoya en las garantías que da la tecnología, en la criptografía, no en entidades centralizadoras, como un Banco Central.

La utilidad principal de las criptomonedas es el envío de valor mediante un sistema completamente seguro y digital. Cada cripto tiene una cotización propia que se basa en su oferta y demanda. Todas ellas puedan ser enviadas entre usuarios sin problemas e intercambiar valor en forma digital.

¿Qué es Blockchain?

Protocolos de consenso

En Blockchain, el proceso de armar un bloque de transacciones y sumarlo definitivamente en la cadena se llama sellado o minado. Cuando un bloque queda sellado, la información que contiene pasa a formar parte de la cadena de forma permanente, inmutable e inalterable. El Protocolo de Consenso es el mecanismo que regula la forma en que los nodos que sellan bloques llegan a un acuerdo entre sí para poder hacerlo (e incorporar ese bloque a la cadena).

Hay varias formas de implementar ese protocolo. La más común de todas se denomina *Proof of Work*, o *Prueba de Trabajo*. En este modelo todos los nodos son pares iguales en la red, y todos compiten para sellar un bloque antes que el resto y poder conseguir criptomoneda a cambio. Para realizar esto, deben resolver un algoritmo complejo. El que primero logre hacerlo y pueda agregar un bloque a la cadena es el obtendrá esa recompensa (criptomoneda). Pero para realizar ese trabajo se necesita un alto nivel de procesamiento, lo que se termina traduciendo en un mayor costo energético. Ver Anexo II.

Proof of Work

Participan todos los nodos de la red, de forma anónima

La probabilidad de minar un bloque depende de la cantidad de procesamiento que aporte el minero

Compiten para sellar un bloque

Consume más energía que otros modelos

El primer nodo que logre sellarlo obtiene una recompensa en criptomoneda

¿Qué es Blockchain?

Protocolos de consenso

En el modelo de Proof of Authority, o *Prueba de Autoridad*, solo hay una cantidad determinada de nodos que están autorizados a resolver el sellado de bloques.

Este protocolo no está basado en la competencia, sino en el hecho de que ese grupo reducido que tiene permisos para agregar bloques a la cadena se turne para hacerlo. Como aquí no hay necesidad de resolver algoritmos complejos, la cantidad de procesamiento es mínima. Por eso se considera a estos modelos como livianos y más eficientes en relación a consumo energético.

La otra gran característica es que generalmente en modelos de Prueba de Autoridad no hay circulación de criptomonedas con valor económico, ya que en realidad no es necesaria una recompensa por esa participación. Ver Anexo II.

Proof of Authority

Participan solo algunos nodos autorizados

Su identidad debe estar verificada

No hay criptomoneda circulante

Al no haber competencia, el consumo de energía es menor y más eficiente

Transparencia

Sobre esta arquitectura que garantiza un registro público e inalterable de transacciones se suma otra de las grandes ventajas de Blockchain: toda la información almacenada en la cadena es completamente auditable.

Si un usuario intenta alterar el contenido agregado en la cadena, no contará con el consenso de las partes selladoras.

No solo todo agregado al registro se incorpora de forma pública y visible para todos los usuarios, sino que cualquiera de ellos –inclusive de forma anónima- puede validarlo. En definitiva, cualquier persona puede velar por la integridad de la información contenida en la cadena de bloques.

Sin intermediarios

En Blockchain no hay terceros de confianza: no hace falta una persona, empresa o institución centralizadora que legitime la información guardada en la cadena, ya que es segura por naturaleza.

Está garantizada por la matemática, por la criptografía.

Registro creciente

Toda la información alojada en el registro es inamovible. De la misma forma que en un libro contable, no se puede borrar o modificar, solo agregar.

Por ello se trata de un registro en constante crecimiento. Cada dato que se suma a la cadena lo hace integrando un nuevo bloque. Si esa información se quiere modificar, solo puede hacerse mediante datos nuevos que corrijan los anteriores, pero los originales nunca se borran, permanecen siempre en la cadena y pueden ser fiscalizados.

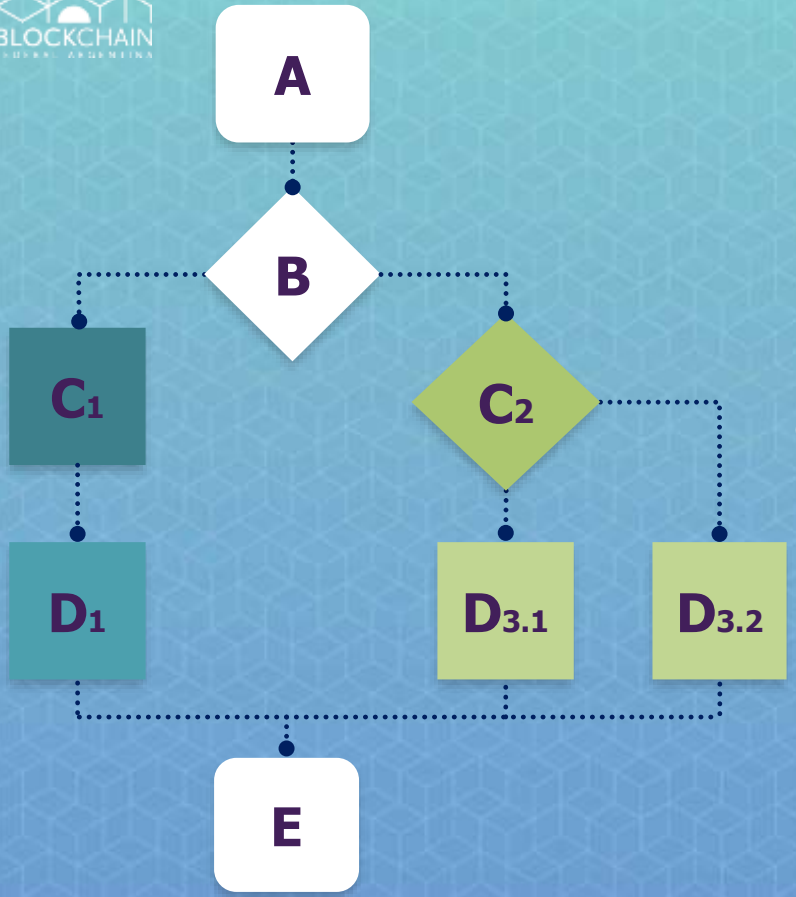
Así, de forma casi orgánica, una blockchain siempre suma nueva información a medida que se agregan nuevos bloques. Crece permanentemente.

Contratos inteligentes

Sabemos que Blockchain funciona como un registro de transacciones, pero también habilita la programación de aplicaciones a través de los llamados "contratos inteligentes" (*smart contracts*). Estos desarrollos pueden tanto ejecutarse como consecuencia de transacciones como generar, ellos mismos, transacciones nuevas.

Es verdad que el término puede ser un poco confuso, porque no son justamente contratos. Son más bien flujos de tareas programables dentro de Blockchain, que abren la posibilidad de desarrollar aplicaciones.

Contratos inteligentes



A diferencia de una App tradicional, donde tenemos que confiar en las garantías que nos da su desarrollador, en un smart contract es posible programar un flujo de tareas pre establecido entre partes interesadas, apoyado en todas las garantías de confianza y transparencia que nos da una red de cadena de bloques.

Gracias a los *smart contracts* se pueden realizar tareas cada vez más complejas. Así, podemos dejar de pensar en Blockchain como un mero registro y comenzar a pensar procesos como seguimiento de licitaciones, sistemas de trazabilidad de productos, plataformas de documentos "vivos", y mucho más.

Identidad soberana

Los sistemas de identidad en línea se crean con la finalidad de asociar datos con los individuos, pero esta información no suele ser propiedad del usuario y tampoco está bajo su control.

Blockchain nos ofrece la posibilidad de consolidar un sistema de identidad distribuida, donde la autoridad no es única, sino que se distribuye entre una multitud de actores de confianza. Al descentralizar el proceso y darle el control al usuario, ninguna institución podría poner en compromiso los datos de su identidad. Se deja de depender de entidades de control y procesamiento de datos y el ciudadano pasa a ser el verdadero dueño de ellos: puede elegir qué datos facilitar, a quién facilitárselos, y revocar su permiso para acceder en cualquier momento.


BLOCKCHAIN
FEDERAL ARGENTINA

Blockchain Federal Argentina

El avance de Blockchain ha demostrado que esta tecnología guarda una enorme capacidad para garantizar seguridad, resiliencia y transparencia en diferentes tipos de procesos. Estas características, sumadas a la posibilidad de programar flujos de transacciones y *smart contracts* nos permiten dejar de pensar solamente en un mero registro y empezar a pensar en la posibilidad de desarrollar todo un ecosistema de aplicaciones confiables y efectivas, garantizadas por la cadena de bloques.

BFA se propone justamente eso: desarrollar una plataforma multiservicios abierta y gratuita pensada para integrar servicios y aplicaciones que puedan heredar todas las características de Blockchain. Una iniciativa confiable y completamente auditable que permita optimizar procesos y funcione como herramienta de empoderamiento para toda la comunidad.

Múltiples partes interesadas

Blockchain Federal Argentina fue concebida dentro de un espacio de trabajo colaborativo, y apunta a reproducir ese patrón como columna vertebral de la plataforma.

Trabajar bajo un **modelo de Múltiples Partes Interesadas** representa tanto una ventaja como una responsabilidad. Escuchar diferentes voces y construir un esquema a partir de distintas perspectivas es una obligación asumida como necesaria para desarrollar proyectos que atraviesan a todos los sectores de la sociedad. Pero al mismo tiempo es una estrategia que toma forma de ventaja diferencial para hacer frente a los diferentes desafíos que se presenten en nuestro camino.

Diseñada para potenciarse a través de los aportes de sectores públicos, privados, académicos y de la sociedad civil, **BFA** opta por una estrategia donde la participación de toda la comunidad es esencial, desde la ingeniería organizacional hasta el despliegue de la infraestructura.

Modelo

Sin criptomoneda

Blockchain Federal Argentina está diseñada específicamente para no poseer criptomoneda asociada.

El incentivo para participar en **BFA** es favorecer el desarrollo de servicios e iniciativas basadas en la innovación tecnológica y en un trabajo horizontal entre diversos actores.

No es necesaria la implementación de una moneda virtual para aprovechar las ventajas que Blockchain nos proporciona. Se opta por un camino que no se alimenta de la competencia entre las partes: el objetivo para participar no es la acumulación de moneda virtual, no es la ganancia.

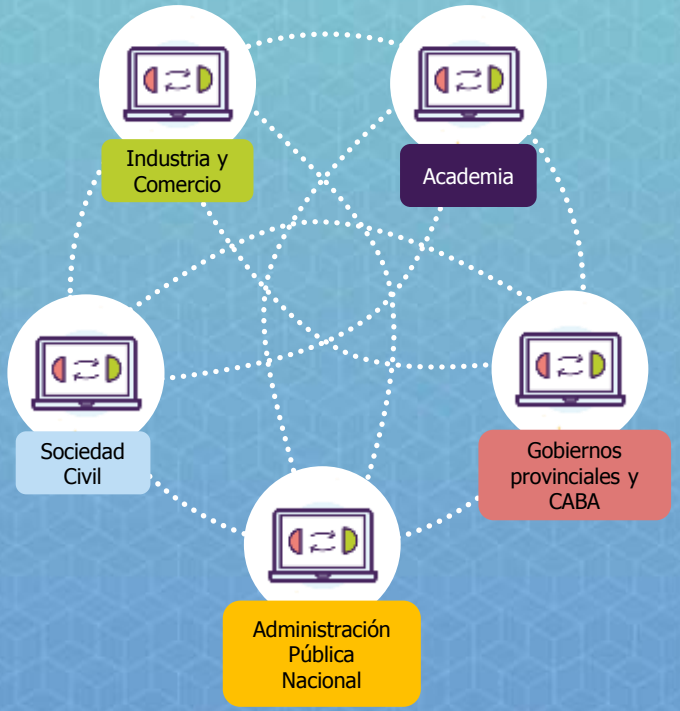
Modelo

Modelo liviano

Al no requerir la resolución del algoritmos complejos para el minado de criptomonedas, se habilita la implementación de mecanismos de consenso eficientes, tanto en lo relativo a cantidad de transacciones por unidad de tiempo como en el consumo eléctrico.

Como **BFA** está basada en un protocolo de Prueba de Autoridad, requiere de muchos menos recursos que una blockchain tradicional que utiliza Prueba de Trabajo.

Modelo

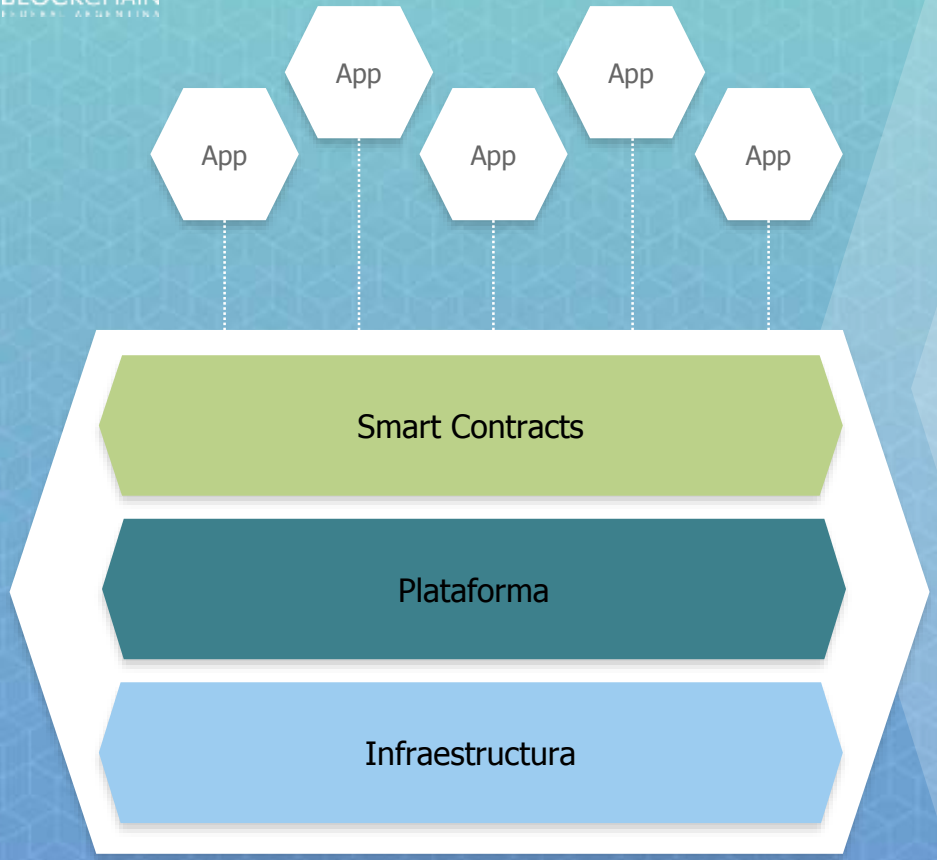


Permisionada

BFA funciona bajo el modelo de una blockchain permisionada. Al utilizar un método de Prueba de Autoridad, se puede estructurar una red en base a un conjunto confiable, una determinada cantidad de nodos selladores autorizados, en lugar de basar el procesamiento en un conjunto de mineros anónimos compitiendo por la creación de un bloque.

Además, en **Blockchain Federal Argentina** la distribución de nodos selladores está garantizando la representatividad de los sectores en el procesamiento de la cadena.

Modelo



Infraestructura - Aplicaciones

La utilización de la **BFA** es pública. Las organizaciones que deseen desarrollar servicios y/o aplicaciones sobre la blockchain solo deberán aceptar un acuerdo de utilización y buenas prácticas, pero no estarán obligados a desplegar nodos selladores. **BFA** se encargará de la infraestructura mientras que los usuarios desarrollarán las aplicaciones.

Modelo

Transacciones gratuitas

Las transacciones realizadas sobre **Blockchain Federal Argentina** no tienen costo.

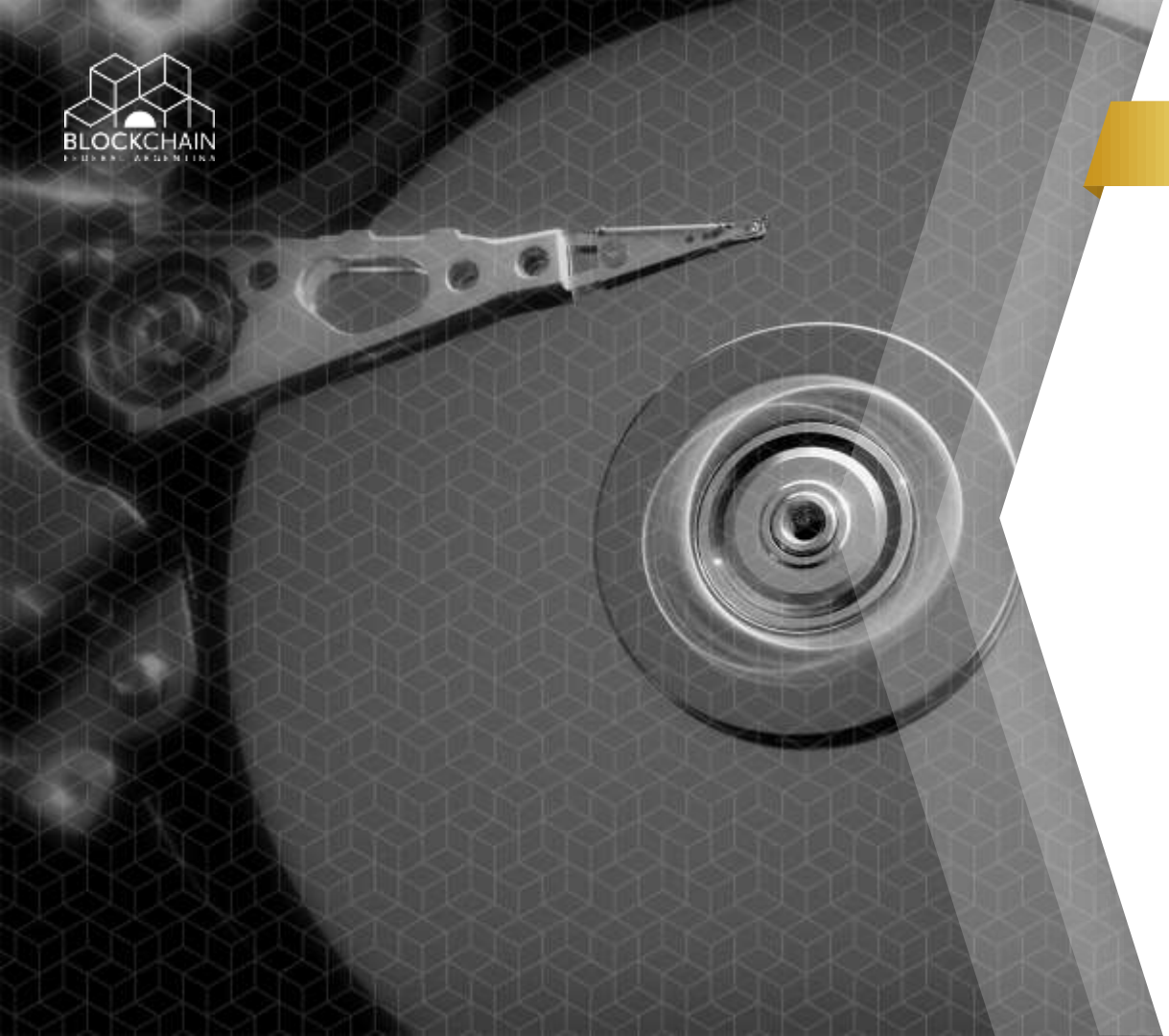
Al no poseer una criptomoneda asociada, y estructurar la red bajo el modelo de Prueba de Autoridad con un costo de infraestructura marginal, las transacciones en **BFA** son gratuitas. El "combustible" necesario para realizarlas será provisto, sin ningún costo asociado, por **Blockchain Federal Argentina**. Ésta asegurará también las medidas para evitar abusos (ver "Destilería de Gas").

Modelo

Software Libre

El software de **Blockchain Federal Argentina** se basa en una implementación abierta y robusta. Todos los desarrollos y modificaciones que se realicen serán igualmente abiertos, de modo que puedan ser públicamente auditados por cualquier interesado, más allá de los participantes de la organización.

La transparencia inherente en el modelo queda también garantizada desde el código.



Modelo

Almacenamiento *off-chain*

En **BFA** no se almacenan documentos o archivos dentro de la blockchain, solo se guardan los hashes de esos documentos.

Los usuarios, los servicios, son responsables de resguardarlos de la manera que consideren más adecuada, pero al tener los digestos criptográficos sellados en la blockchain encuentran la forma de demostrar que esos documentos no fueron modificados luego de que ese hash se obtuvo.

Tecnología

Ethereum

BFA está basada en la tecnología Ethereum, una de las blockchains públicas más difundidas a nivel internacional. Es una plataforma descentralizada que funciona bajo Prueba de Trabajo y permite a cualquier desarrollador crear y publicar aplicaciones distribuidas para ejecutar *smart contracts* garantizados por la cadena de bloques. La red posee una infraestructura de nodos a nivel global.

Como el desarrollo está basado en código abierto, toda la comunidad puede participar en las pruebas de concepto existentes para mejorar la plataforma, o tomar todo ese trabajo y adaptarlo a otros contextos y necesidades.

Blockchain Federal Argentina toma el software de Ethereum, utilizando Prueba de Autoridad, sin criptomoneda asociada.

Tecnología

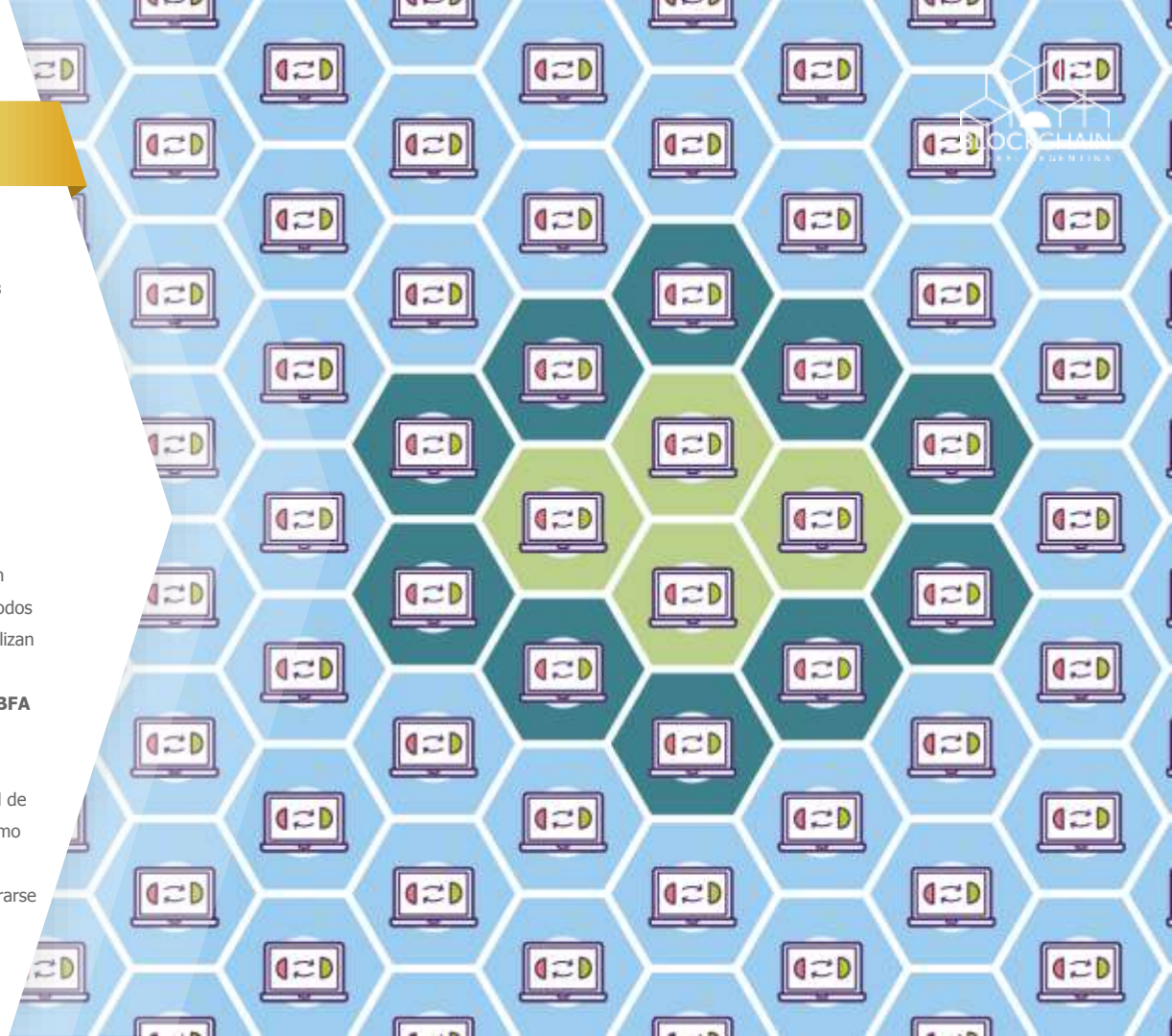
Nodos

La red está integrada por distintos tipos de nodos. **Los nodos selladores** conforman la estructura central de la red confiable de **BFA** ya que son los únicos que pueden sellar (agregar) bloques a la cadena. Todos ellos están desplegados por miembros de la organización. **BFA** estará inicialmente estructurada a partir de 23 nodos selladores.

Los selladores están conectados solamente entre sí, y a los nodos tipo **gateway**, que actúan como buffer entre ellos y el resto de la red.

Los **nodos transaccionales** (*transaction nodes*) son aquellos que pueden enviar transacciones para que luego sean agregadas a la cadena por los nodos selladores. Usualmente son ejecutados por operadores de servicios que utilizan la blockchain (los que implementan aplicaciones). Cualquier usuario puede correr este tipo de nodos. Solo debe contar con una cuenta registrada en **BFA** y aceptar las políticas de uso.

Existen también nodos **solo lectura** (*read-only*). Estos son parte de la red de pares, reciben todos los bloques y sus transacciones. Pueden funcionar como validadores o auditores, verificando que todos los bloques sean válidos. Cualquier usuario puede correr este tipo de nodos, sin necesidad de registrarse (anónimo) ni contar con autorización de **BFA**. También podrían servir para acceder a la información por parte de una aplicación o servicio.



Tecnología

Nodos operativos

La red se encuentra operativa. Al día de hoy están funcionando nodos selladores de al menos las siguientes organizaciones miembro de **BFA**.

- ARIU
- UN Córdoba
- UN San Juan
- UN Rosario
- UN La Plata
- DGSI
- Prefectura Naval
- ONTI
- ASI GCBA
- CABASE
- EVERIS
- SYT
- Universidad de Palermo

Tecnología

Destilería de Gas

Para enviar transacciones a la blockchain se necesita un "combustible" llamado Ether, que **BFA** distribuye a aquellos operadores registrados de nodos transaccionales que desplieguen aplicaciones sobre la plataforma -ver Anexo 2-.

El Ether no tienen ningún tipo de valor económico y se envía periódicamente mediante un espacio operado por la organización. Así, se implementa un modelo donde se evita la especulación y/o el tráfico, además de posibilitar métodos para detectar el abuso.

Al mismo tiempo, para reafirmar la transparencia, cualquier nodo solo lectura que se integre a la red podrá verificar la fidelidad de la información, sin necesidad de poseer Ether para realizarlo.

Tecnología

Monitoreo

Cada entidad que administre un nodo de **BFA** es responsable de su mantenimiento y monitoreo. De hecho no existe en la red un sistema central de administración.

Como apoyo, **Blockchain Federal Argentina** sí implementará un esquema de monitoreo a través del NOC (*Network Operation Center*), que estará atento al funcionamiento de los nodos selladores y *gateway*. El mismo no tendrá un única ubicación centralizada sino que estará distribuido geográficamente y entre varias partes de la organización.

Tecnología

Sello de Tiempo

Existen modos de certificar contenidos a través de Blockchain. Estos mecanismos permiten generar una "prueba de existencia", algo así como un sello digital que demuestra que el contenido de un mensaje existía antes de una fecha y hora determinada y no fue modificado.

El servicio de TSA *(Time Stamping Authority)* desarrollado por **BFA** -ver Anexo 2- permite demostrar o evidenciar que un determinado archivo digital se ha mantenido inalterado en el tiempo a partir de una determinada fecha.

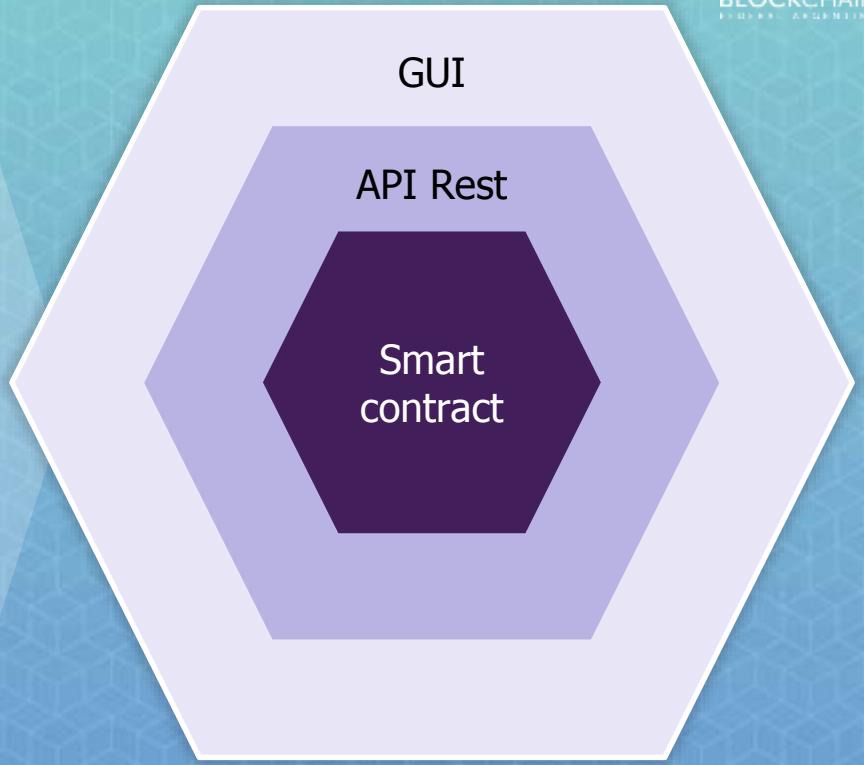
Tecnología

Sello de Tiempo

Hay varias formas de utilizar la TSA de **Blockchain Federal Argentina**, de acuerdo a las necesidades y posibilidades de cada usuario.

- Una GUI está disponible en bfa.ar/sello. Permite sellar documentos sin ningún tipo de conocimiento sobre Blockchain o programación.
- También se encuentra disponible una API REST para facilitar desarrollos que quieran conectarse con este servicio.
- Y por supuesto, de fondo se encuentra funcionando el Smart Contract que posibilita todo esto.

Si alguien desea desarrollar un nuevo *smart contract* y volcarlo en la blockchain, puede hacerlo perfectamente.



Gobernanza

¿Quiénes pueden participar?

Toda la comunidad tiene las puertas abiertas para participar en **Blockchain Federal Argentina**. Individuos, organismos, instituciones o empresas de cualquier sector interesados en desplegar aplicaciones y servicios aprovechando todas las características de la plataforma, o simplemente contribuir al primer desarrollo de esta índole en el país, pueden sumarse a la iniciativa y comenzar a participar.

Gobernanza

¿Cómo puedo participar?

Hay dos grandes formas de integrarse a la **Blockchain Federal Argentina:** como usuarios del servicio o como partes de la organización.

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.

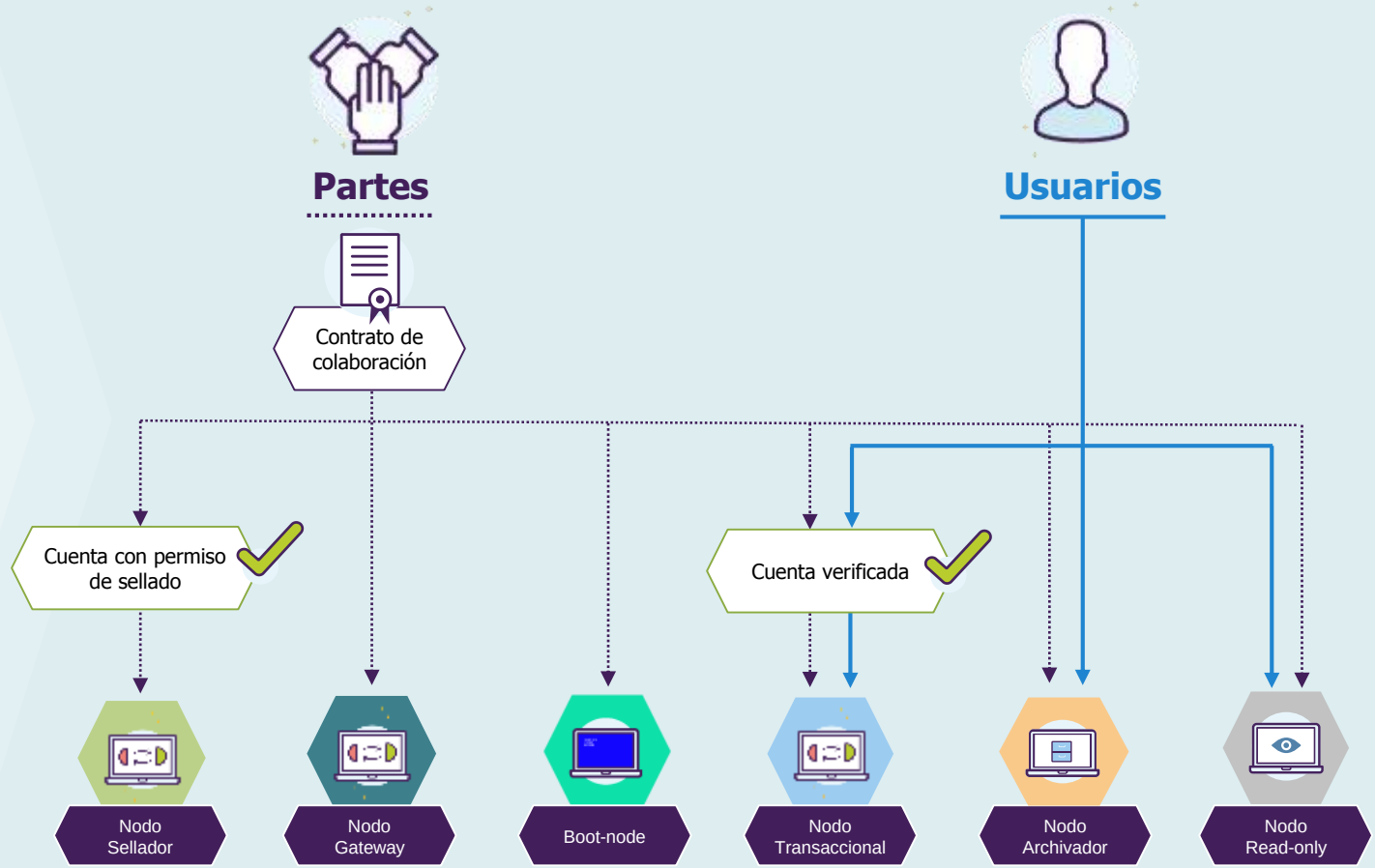
Pueden aportar a la infraestructura del core de la red con nodos selladores o Gateway.

Deben firmar un formulario.

Tienen las mismas facilidades de los usuarios para desarrollar aplicaciones

BLOCKCHAIN FEDERAL ARGENTINA

¿Cómo puedo participar?



Gobernanza

Contrato de Colaboración

La **BFA** se consolidó mediante la firma de un Contrato de Colaboración Público-Privada. Mediante la presentación del "Formulario de Solicitud de Incorporación como Parte", las nuevas partes declaran conocer y aceptar todos y cada uno los términos del Contrato y las modificaciones aprobadas por las Addendas I y II, aceptando expresamente sus objetivos como así también los derechos y obligaciones establecidos en el mismo y en el Reglamento Interno.

El acuerdo tendrá un plazo de vigencia de 5 años y puede ser prorrogado antes de su vencimiento por un mismo período de tiempo.

Gobernanza

Recisión del contrato

Para aquellas partes que no deseen prorrogar el contrato se incluyó en el mismo una cláusula que habilita el derecho para que no sea renovado.

Así mismo, cualquiera de las partes podrá dar por finalizado el contrato en lo que a ella respecta, para lo cual deberá comunicar su decisión a **BFA** con un preaviso de sesenta días. Durante dicho plazo deberá seguir cumpliendo con las obligaciones a su cargo.

BLOCKCHAIN FEDERAL ARGENTINA

Gobernanza

Estructura de trabajo

Consejo de Administración (CdA)

Constituido por cinco miembros titulares y cinco suplentes, representando a cada uno de los sectores:

Industria y Comercio, Academia, Gobierno Nacional, Gobiernos Provinciales y CABA, y Sociedad Civil

Reunión de Partes

Integra a todas las partes de BFA y se reunirán al menos una vez al año. Es la encargada, por ejemplo, de la elección de los miembros del CdA o de analizar y modificar el Contrato de Colaboración.

Comité Técnico (CT)

Formado por expertos que asesoran al CdA. No posee capacidad ejecutiva o legislativa por sí mismo.

NOC distribuido

BFA establecerá al menos tres centros de control independientes operados por organismos parte de BFA que apoyarán en el monitoreo y control de las partes críticas de la red, de forma pública y abierta.

Grupos de trabajo

Son espacios de debate. La participación será abierta para las partes e interesados

Tecnología – Casos de uso – Legal – Comunicación – Seguridad – Monitoreo

Gobernanza

Antecedentes

CABASE, ARIU y NIC Argentina decidieron emprender esta iniciativa, que hereda años de experiencia en proyectos conjuntos. Antecedentes como la primer red Anycast de DNS autoritativo en el país se fueron gestando a partir de la multiplicidad de visiones y de un mismo compromiso: potenciar y democratizar el espacio tecnológico en nuestro país para que pueda transformarse en una economía de vanguardia de cara a los desafíos del siglo XXI.

Estos organismos traen la experiencia de un modelo de Gobernanza y Múltiples Partes Interesadas, regido por el trabajo colaborativo y la cooperación entre miembros de diferentes sectores del Ecosistema de Internet.

Gobernanza

Perspectiva regional

Esta experiencia histórica, reforzada por el trabajo en espacios de colaboración regional e internacional como ICANN, ISOC, LACNIC, LACTLD e IGF, deja su marca en el camino de **Blockchain Federal Argentina**.

La plataforma está diseñada pensando en una infraestructura que garantice la interoperabilidad y la sinergia entre emprendimientos similares en toda América Latina y el Caribe.

Imaginar una blockchain regional nos permite tomar todas sus ventajas y multiplicar exponencialmente sus beneficios y su solidez, transparencia y seguridad.

Gobernanza

Continuidad

El diseño tanto técnico como de gestión de **Blockchain Federal Argentina** no solo fue pensado para garantizar que la iniciativa fuera escalable gracias a la incorporación de nuevos participantes, sino también a asegurar su continuidad en el tiempo: que perdure más allá de las personas e instituciones que lo gestaron gracias a un modelo de trabajo horizontal y colaborativo.

Blockchain Federal Argentina

Las cadenas de bloques nos dan las herramientas para construir una plataforma segura y transparente, características que, por la arquitectura de **Blockchain Federal Argentina**, se trasladan necesariamente a todas las iniciativas desarrolladas sobre la misma.

Todas las ventajas de esta tecnología se fortalecen al estructurarlas en torno a un proyecto participativo, que evoluciona y se fortalece a través de la incorporación de nuevos integrantes. Esta ambición por sumar nuevas partes es la que también garantiza la continuidad en el tiempo de **BFA**: que perdure más allá de las personas e instituciones que lo gestaron gracias a un modelo de trabajo multisectorial y distintos actores involucrados.

Así, nos encontramos frente la posibilidad de consolidar una herramienta colaborativa y de vanguardia. **BFA** no solo funcionará como soporte de ideas para empresas e instituciones, sino que será el primer espacio digital común de estas características en el país: un ecosistema ideal para productos y servicios que busquen una infraestructura sólida, abierta, transparente y confiable.

Anexo I
Casos de uso

ANEXO I

Casos de Uso

Pese a ser una tecnología relativamente nueva, a lo largo del mundo ya empiezan a aparecer casos de éxito de implementación de Blockchain en diferentes tipos de procesos, servicios y aplicaciones.

Desde **BFA** se están explorando constantemente nuevas posibilidades e ideas que puedan nutrirse de esta infraestructura, y se apunta al desarrollo de casos de uso para mostrar todo su potencial.

Al ser una tecnología tan novedosa, el trabajo de investigación es esencial como apoyo de todo lo mencionado y es un factor clave en el que se está trabajando día a día. En este sentido también se apunta a consolidar una estructura de monitoreo para poder evaluar el funcionamiento de la iniciativa en su totalidad.

ANEXO I

Casos de uso

Trazabilidad

La solidez y la inmutabilidad de Blockchain ofrecen un nivel de apertura y transparencia de los datos que hacen a la tecnología ideal para su implementación en sistemas de trazabilidad de mercaderías.

En el caso de los alimentos, se puede realizar el seguimiento del producto desde su fabricación hasta consumo de forma completamente confiable, pudiendo detectar, por ejemplo, productos contaminados en cuestión de segundos.

Pagos transfronterizos

A través de Blockchain se han desarrollado plataformas de micropagos P2P (*peer-to-peer*, redes de pares), especialmente destinados a transacciones transfronterizas.

Este tipo de servicios es muy útil para aquellos trabajadores migrantes que envían día a día parte de sus salarios a sus familias en sus países de origen, y corren con la ventaja de tener honorarios considerablemente más bajos que las transferencias tradicionales y de que pueden ser utilizados por la población no bancarizada.

ANEXO I

Casos de uso

Gestión de ayuda humanitaria

La Organización de las Naciones Unidas comenzó a utilizar *blockchain* para la gestión de transacciones en campos de refugiados de su *World Food Programme*.

Mediante un sistema basado en *Ethereum*, el programa gestiona la entrega de alimentos a refugiados sirios en Jordania. El proyecto piloto iba a finalizarse originalmente en mayo de 2017 pero debido a su éxito se ha extendido de forma indefinida.

Sistema integral de gestión pública

Luego del hackeo sufrido en la administración pública en 2007, el gobierno de Estonia implementó un sistema de Blockchain a nivel estatal.

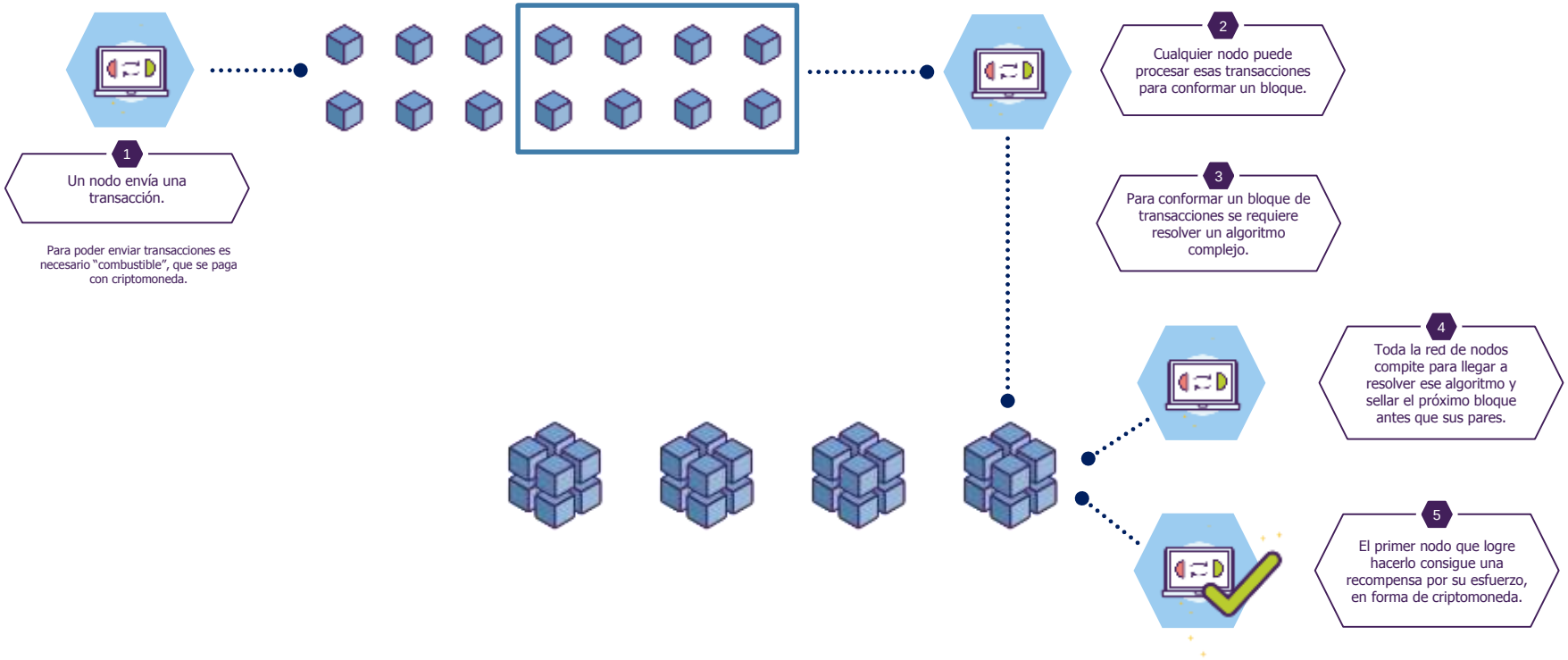
El resultado fue el proyecto e-Estonia, un programa que llevó a digitalizar el 99% de los trámites públicos, certificando identidad digital y garantizando la confiabilidad y estabilidad de la información pública mediante cadenas de bloques.

Hoy en día Estonia es el 1er país en el mundo en uso de Blockchain a nivel nacional.

Anexo II
Infografías

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

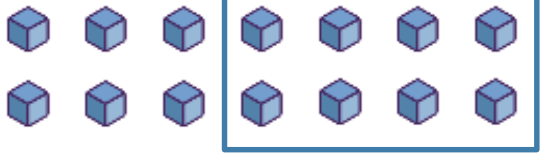
Los modelos más tradicionales de Blockchain son denominados Proof of Work y se basan en la competencia entre distintos nodos para agregar el siguiente bloque a la cadena a cambio de un incentivo económico.



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

Hay redes de Blockchain que optan por un modelo de Proof of Authority donde solo algunos nodos autorizados pueden crear bloques que contengan transacciones.

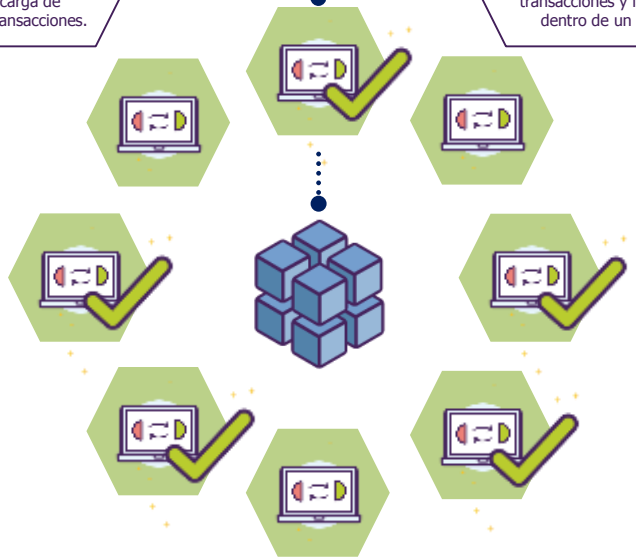
1. Un nodo envía una transacción.



Todas las transacciones de la red eventualmente pasarán a formar un bloque.

2. Una red de nodos autorizados, o selladores, es la que se encarga de procesar esas transacciones.

3. Un nodo sellador recolecta una determinada cantidad de transacciones y las compila dentro de un bloque.

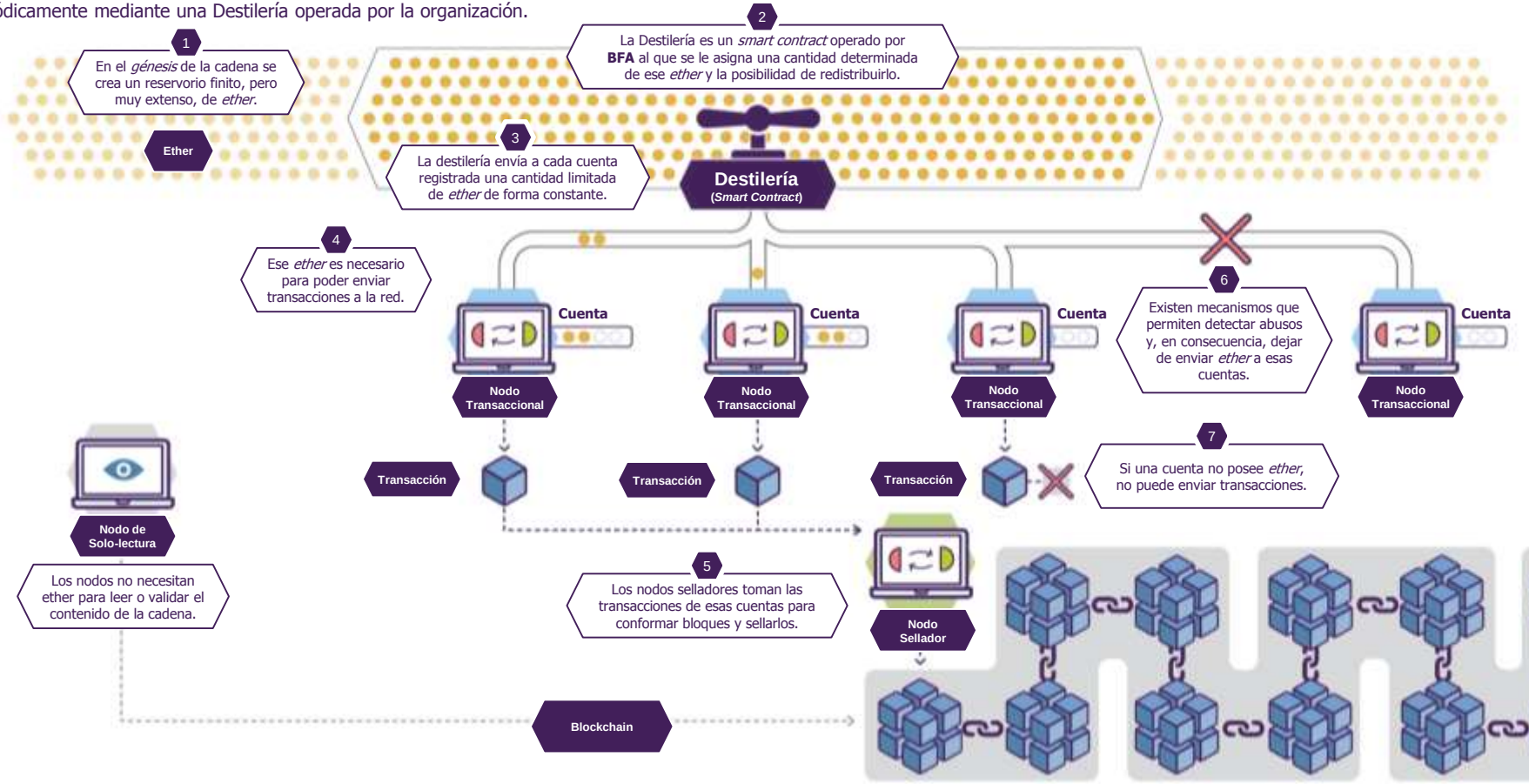


4. Una vez que más de la mitad de sus pares aprueba ese bloque, es sellada y pasa a ser el siguiente bloque de la cadena. A partir de aquí, la información contenida es inmutable.

5. Ese nodo debe esperar un tiempo determinado para volver a sellar: la mitad de los nodos deben agregar un bloque a la cadena antes de que él pueda volver a intentarlo.

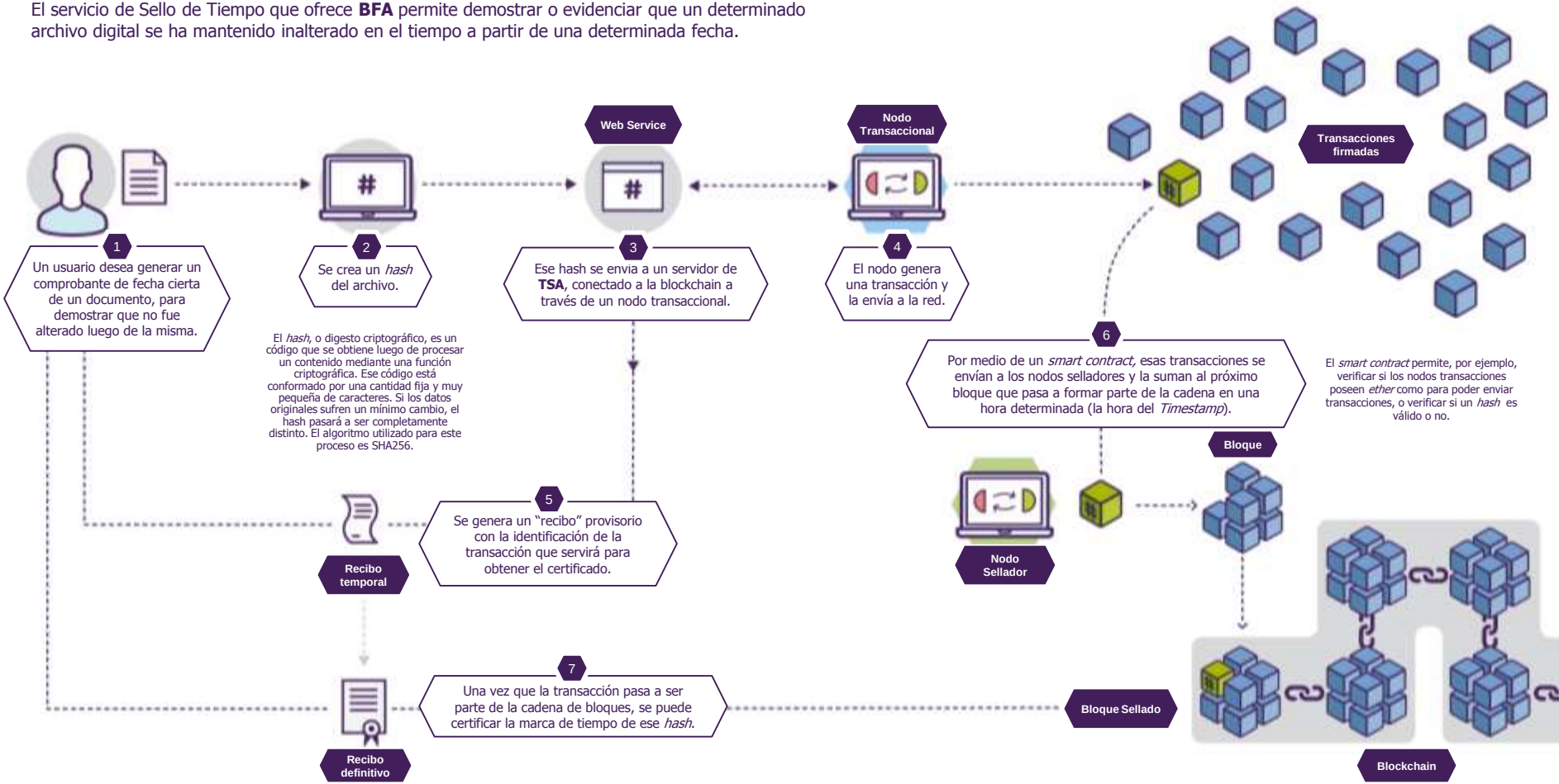
Destilería de Ether

Para enviar transacciones a la blockchain de **BFA** se necesita un "combustible". El mismo toma la forma de tokens virtuales (ether) que se distribuirán a aquellos operadores de nodos transaccionales que desplieguen aplicaciones sobre la plataforma. No tienen ningún tipo de valor económico y se enviarán periódicamente mediante una Destilería operada por la organización.



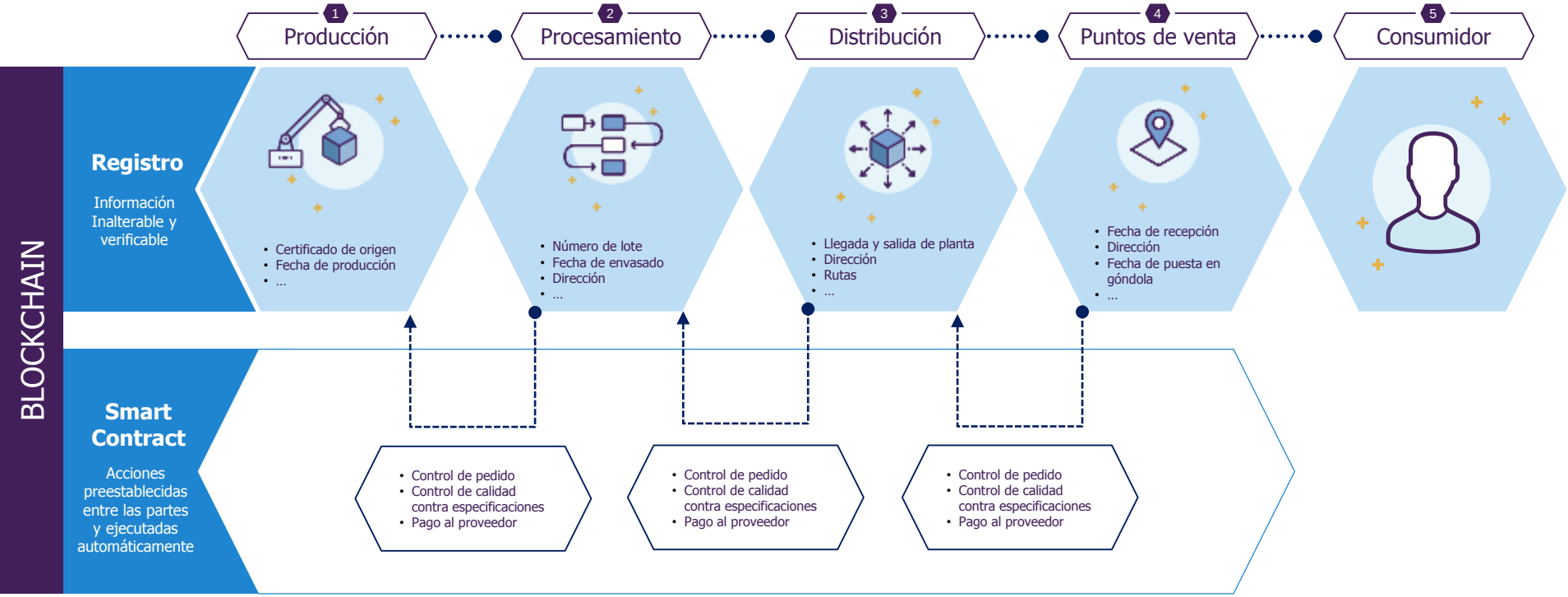
Sello de Tiempo BFA

El servicio de Sello de Tiempo que ofrece **BFA** permite demostrar o evidenciar que un determinado archivo digital se ha mantenido inalterado en el tiempo a partir de una determinada fecha.



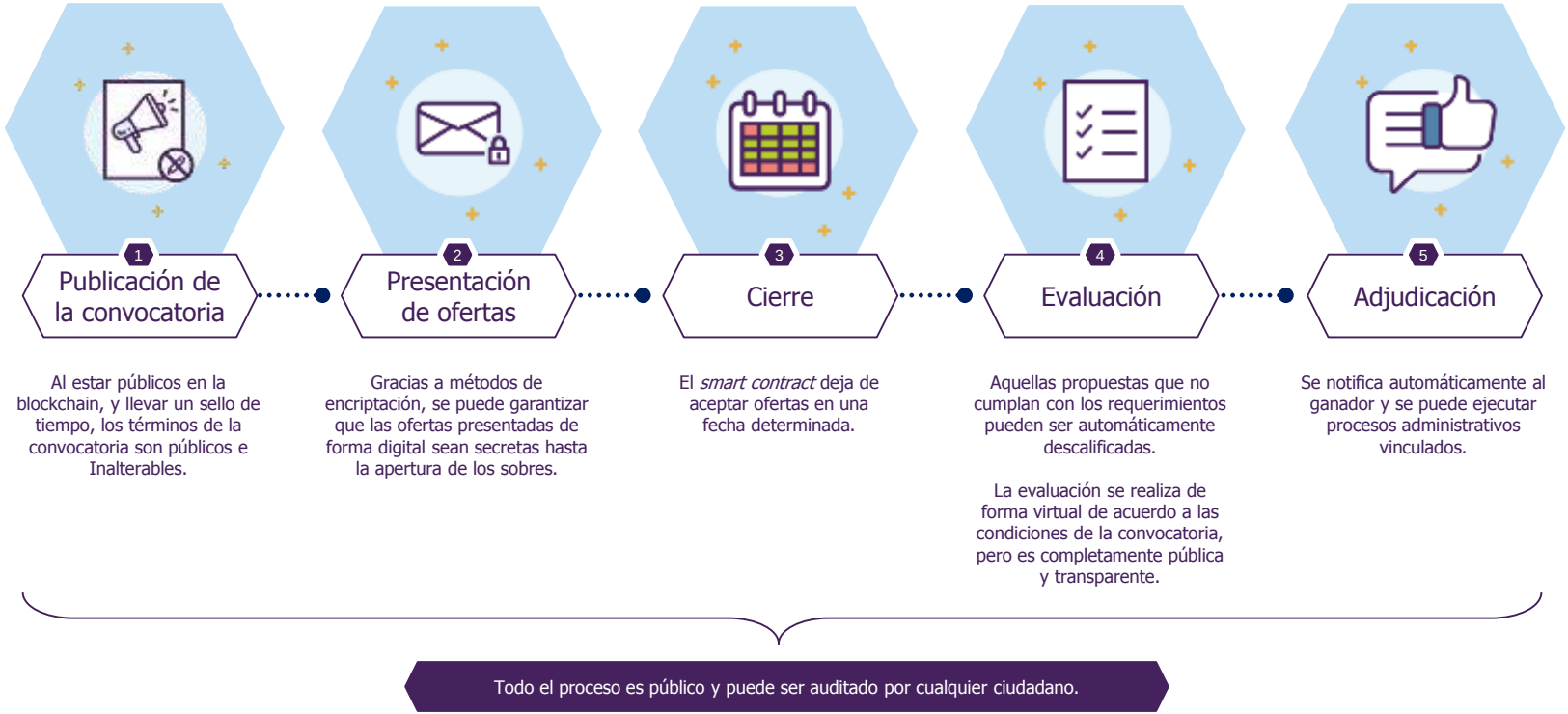
Trazabilidad de productos mediante Blockchain

Blockchain nos permite optimizar procesos a lo largo de toda la cadena de producción y distribución. Al tener un registro inalterable de las acciones que se llevan en cada eslabón, cada participante, incluso el consumidor final, podría rastrear un producto a lo largo de toda la cadena. Incluso, mediante la implementación de *smart contracts*, se pueden automatizar tareas bajo condiciones pre establecidas por las partes.



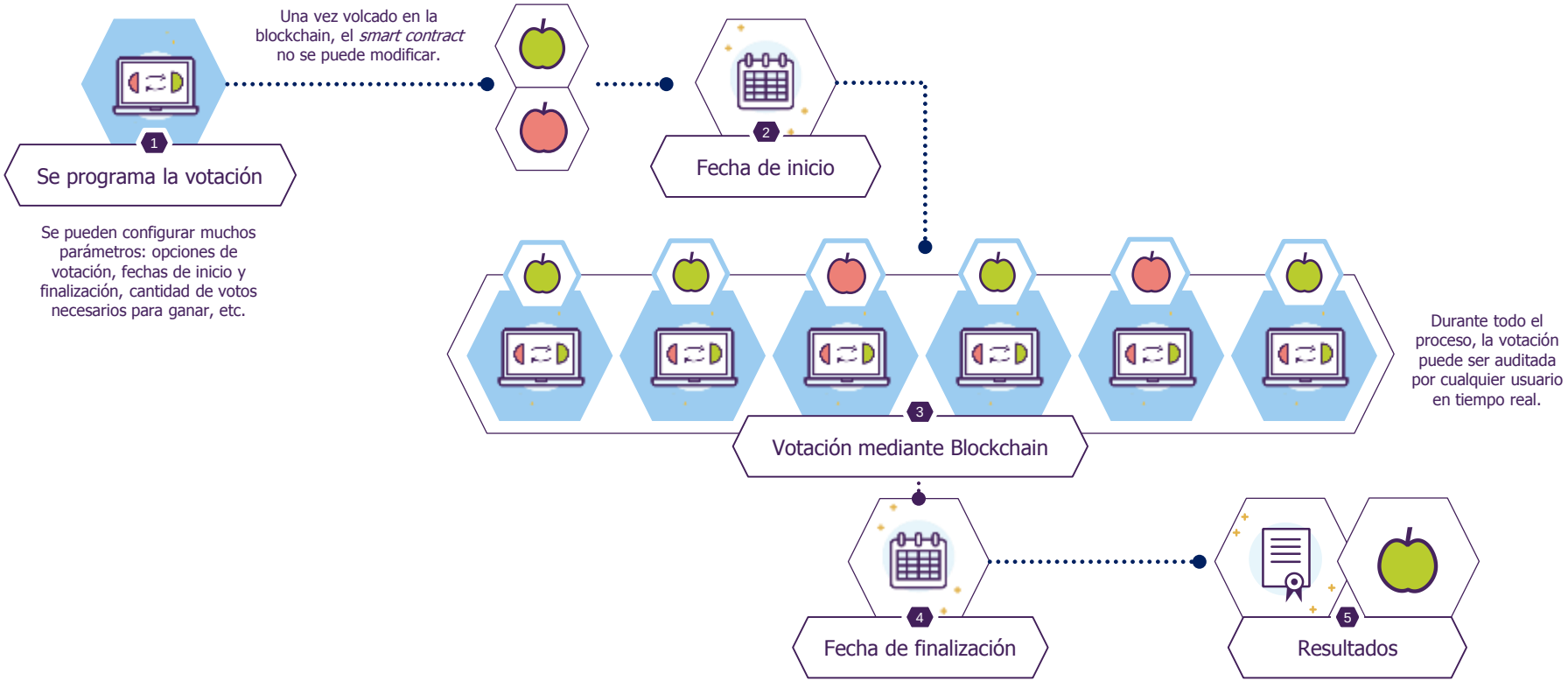
Licitaciones públicas

Blockchain posibilita el desarrollo de una plataforma de licitaciones públicas que garantice transparencia e impida cualquier tipo de fraude. Mediante la implementación de *smart contracts* gran parte de una licitación puede ser automatizada, y gracias a las características de las cadenas de bloques, cualquier individuo puede auditar todo el proceso dentro de la blockchain.



Smart Contracts

Los *smart contracts* no son justamente contratos, son más bien flujos de tareas que pueden programarse dentro de la blockchain. Estos pueden tanto ejecutarse como consecuencia de transacciones como generar, ellos mismos, transacciones nuevas. Este es un ejemplo, muy esquemático, de cómo mediante estos flujos se puede programar una votación sobre Blockchain. En este caso, no se refiere a una elección nacional, sino más bien una votación sencilla: los presentes en una reunión podrían votar si están de acuerdo con la minuta, o evaluadores podrían calificar una tesis.



Anexo III

Análisis de Riesgos

ANEXO III

Análisis de Riesgos

¿Qué ocurre en caso de abusos de transacciones?

Al ofrecer transacciones sin costo, **Blockchain Federal Argentina** entiende que se pueden presentar riesgos de abusos que pueden atentar contra el normal funcionamiento de la red.

Para prevenir este tipo posibilidades, **BFA** dispone de diferentes herramientas:

- Un conjunto de nodos *gateway* que funciona como mediador entre la red y los nodos *selladores,* impidiendo que se pueda acceder directamente a estos últimos.
- Un NOC (*Network Operation Center)* distribuido entre miembros de la organización y a lo largo del país, que apoya el monitoreo de los nodos.
- Una "Destilería de Gas" que regula el envío de *ether* a nodos transaccionales y permite tomar acciones frente a abusos detectados.
- Un Grupo de Trabajo de Casos de Uso, que analiza las diferentes implementaciones en la blockchain.

ANEXO III

Análisis de Riesgos

¿Puede un modelo gratuito ser sostenido en el tiempo?

Blockchain puede existir sin una criptomoneda asociada. **BFA** partió de este principio y desarrolló un modelo liviano que funciona a partir del aporte de las partes.

Al requerir una muy baja capacidad de procesamiento, a diferencia de otras blockchains basadas en Prueba de Trabajo, el costo de esos aportes (servidores, ancho de banda, soporte técnico) es marginal para las infraestructuras tecnológicas de integrantes de la organización.

Si en algún momento **BFA** decide cambiar su estructura financiera, es decir, por ejemplo cobrar por las transacciones, podrá hacerlo siempre y cuando 2/3 de las partes estén de acuerdo.

ANEXO III

Análisis de Riesgos

¿Blockchain entra en conflicto con el derecho al olvido?

Si bien regulaciones internacionales como el GDPR han encontrado aristas de conflicto con Blockchain en cuestiones de derecho al olvido (dado que es prácticamente imposible borrar datos de la cadena de bloques), no es un problema con el que Blockchain Federal Argentina se encuentre.

En **BFA** el almacenamiento de información es off-chain, esto quiere decir que la plataforma no funciona como una nube para almacenar archivos, sino que cada servicio desplegado es responsable de los mismos. En el registro de **BFA** sólo se almacenan los digestos criptográficos, los hash, de esos archivos, lo que basta para garantizar que los mismos no han sido modificados por fuera de la blockchain.

ANEXO III

Análisis de Riesgos

Riesgos técnicos

La estructura de una blockchain esta especialmente diseñada para ser resiliente y resolver gran parte de las vulnerabilidades de otro tipo de redes. Sumado a esto, **Blockchain Federal Argentina** trabaja constantemente para estar preparada frente a todo tipo de riesgos y/o ataques y por ello ha desarrollado toda una serie de políticas tales como:

- Mantener un *core* 23 nodos selladores distribuidos geográficamente.
- Tener preparados nodos selladores de contingencia.
- Sostener una red de nodos Gateway que impide el acceso directo al *core.*
- Un NOC distribuido en el que varias instituciones van a estar monitoreando el desempeño de la red y emitiendo alarmas ante problemas.
- Constituir un comité técnico de expertos que asesora constantemente a la organización.
- Analizar constantemente casos de uso e implementaciones de terceros en la red a través de un Grupo de Trabajo.