



Uso de tecnología Blockchain en el sistema financiero para la presentación de documentación regulatoria

Profesora de Trabajo Final: Dra. Marcela Samela

Alumno: Nicolás Alejandro Di Rico

Trabajo Final de Carrera presentado para obtener el título de
Lic. En Gestión de Tecnología Informática

Diciembre 2024

Resumen

El presente trabajo constituye una intervención en el campo profesional, cuyo objetivo principal es promover la implementación de tecnología Blockchain en el sistema financiero Argentino, con el propósito de mejorar la transparencia en el manejo de la información durante el proceso de presentación de documentación regulatoria. Actualmente, distintos entes regulatorios de nuestro país, como el Banco Central de la República Argentina (BCRA), la Comisión Nacional de Valores (CNV) y la Unidad de Información Financiera (UIF), requieren y/o exigen a las entidades financieras que almacenen y presenten registros e información para controlar irregularidades en el ámbito financiero. Aquí es donde detectamos una oportunidad de mejora, ya que el proceso actual de presentación de cierta información en ocasiones es duplicado debido a los requerimientos de información idéntica por parte de distintas entidades regulatorias, lo cual lo convierte en un proceso tedioso y poco eficiente al momento de controlar la información en auditorías o procesos de revisión. Ante este contexto, durante el transcurso del presente trabajo se describirá nuestra propuesta de solución, aplicando el uso de una Blockchain que permita almacenar esta información en un entorno seguro y fiable, de fácil acceso para las partes interesadas y que optimice los tiempos de documentación y presentación ante las entidades competentes.

Palabras Clave: *auditorías, blockchain, documentación regulatoria, entidades financieras.*

Abstract

The following is a final degree project related to the financial environment of the Argentine Republic, whose main objective is to implement the use of Blockchain technology within the local financial framework to facilitate transparency of information during the presentation of regulatory documentation. Currently, various regulatory bodies in our country, such as the Central Bank of the Argentine Republic (BCRA), the National Securities Commission (CNV), and the Financial Information Unit (UIF), require and/or demand that financial institutions and insurance companies store and present accounting records to monitor irregularities in the financial sector. This is where we detect an opportunity for improvement, since the current process of presenting certain information is sometimes duplicated due to the requirements for identical information by different regulatory entities, which makes it a tedious and inefficient process at the time. to control information in audits or review processes. In this context, throughout the course of this work, we will describe our proposed solution or improvement, applying the use of a Blockchain that allows storing this information in a secure and reliable environment, easily accessible to interested parties, and optimizing the times for documentation and presentation to the competent authorities.

Keywords: *audits, blockchain, financial entities, regulatory documentation.*

Dedicatoria

A mi familia y amigos, que siempre me apoyaron y motivaron a llegar al final de esta carrera. También a mis compañeros y docentes de la facultad, de quienes aprendí muchísimo.

Índice General

Resumen.....	2
Abstract.....	3
Dedicatoria.....	4
Índice General.....	5
Índice de Figuras.....	7
Índice de Tablas.....	8
Estructura General del Trabajo Final.....	9
Capítulos.....	9
Referencias	9
Acrónimos.....	9
Capítulo 1.....	10
1.1 Descripción de la problemática.....	10
1.2 Propuesta de Solución	10
1.3 Objetivos del Trabajo Final	11
1.3.1 Objetivo General.....	11
1.3.2 Objetivos Específicos.....	11
1.4 Contribuciones Principales	11
Capítulo 2.....	13
2.1 Marco Institucional	13
2.1.1 Introducción.....	13
2.1.2 Entes Regulatorios	13
2.1.3 Normativas y Regulaciones Vigentes.....	14
2.2 Estado del Arte	15
2.3 Marco Teórico.....	19
2.3.1 Introducción.....	19
2.3.2 La tecnología Blockchain.....	20
2.3.3 Criptografía	23
2.3.4 Bloques y Transacciones.....	24
2.3.5 Protocolos de consenso.....	27
2.3.6 Contratos Inteligentes	30
2.3.7 Aplicaciones actuales de la tecnología.....	32
2.3.8 Resumen	39
Capítulo 3.....	41

3.1	Propuesta de Intervención	41
3.1.1	<i>Introducción</i>	41
3.1.2	<i>Estrategias y Recursos</i>	41
3.1.3	<i>Funcionamiento del Modelo</i>	43
3.1.4	<i>Infraestructura</i>	49
3.1.5	<i>Tecnología Utilizada</i>	52
3.1.6	<i>Administración de la Red</i>	61
3.1.7	<i>Impacto de la Intervención</i>	62
3.1.7.1	Impacto Económico.	63
3.1.7.2	Impacto Tecnológico.	63
3.1.7.3	Impacto en Terceras Partes.	64
Capítulo 4		65
4.1	Plan de Implementación	65
4.1.1	<i>Introducción</i>	65
4.1.2	<i>Cronograma</i>	65
4.1.3	<i>Recursos Necesarios</i>	66
4.1.4	<i>Estimación de Costos</i>	67
4.1.5	<i>Factores Externos Condicionantes</i>	69
4.2	Factibilidad del Proyecto	70
4.2.1	<i>Análisis de Factibilidad Operativa</i>	70
4.2.2	<i>Análisis de Factibilidad Técnica</i>	71
4.2.3	<i>Análisis de Factibilidad Económica</i>	71
4.2.4	<i>Análisis de Factibilidad Legal</i>	71
4.2.5	<i>Análisis de Factibilidad de Duración</i>	72
Capítulo 5		73
	Conclusiones	73
	Futuras Líneas de Trabajo	75
	Referencias	76
	Acrónimos	83
	Anexo I	85
	Anexo II	87

Índice de Figuras

Figura 1 <i>Tipos de redes</i>	22
Figura 2 <i>Esquema de blockchain basado en el árbol de Merkle.</i>	25
Figura 3 <i>Transacciones</i>	27
Figura 4 <i>Funcionamiento del protocolo PoW</i>	28
Figura 5 <i>Funcionamiento del protocolo PoA</i>	29
Figura 6 <i>Flujo de trabajo de Smart Contracts</i>	31
Figura 7 <i>Caso de uso en licitaciones.</i>	33
Figura 8 <i>Caso de uso en pólizas.</i>	35
Figura 9 <i>Caso de uso en títulos.</i>	36
Figura 10 <i>Caso de uso en trazabilidad de alimentos.</i>	38
Figura 11 <i>Archivo de texto de prueba</i>	45
Figura 12 <i>Función Sellar de la TSA de la BFA</i>	46
Figura 13 <i>Función Obtener Recibo de la TSA de la BFA</i>	47
Figura 14 <i>Función Verificar de la TSA de la BFA</i>	48
Figura 15 <i>Archivo de prueba modificado</i>	48
Figura 16 <i>Error en la función Verificar de la TSA de la BFA</i>	49
Figura 17 <i>Participantes por tipo de nodo.</i>	50
Figura 18 <i>Organizaciones con nodos selladores</i>	51
Figura 19 <i>Sello de tiempo.</i>	53
Figura 20 <i>Diagrama de flujo de Stamp</i>	55
Figura 21 <i>Diagrama de flujo de Verify - Certify</i>	56
Figura 22 <i>Función Sellar del TSA</i>	57
Figura 23 <i>Función Obtener Recibo del TSA</i>	58
Figura 24 <i>Función Verificar Hash del TSA</i>	58
Figura 25 <i>Función Verificar Documento del TSA</i>	59
Figura 26 <i>Destilería de Gas.</i>	60
Figura 27 <i>Cronograma de Actividades</i>	65
Figura 28 <i>Costo de servidor AWS para nodo sellador o transaccional</i>	67
Figura 29 <i>Costo de servidor AWS para nodo Gateway, Bootnode, Test o Read-only</i>	68
Figura 30 <i>Flujo de tratamiento de un evento por parte del NOC</i>	88

Índice de Tablas

Tabla 1 <i>Comparativa de tipos de privacidad en Blockchain</i>	23
Tabla 2 <i>Comparativa de protocolos de consenso</i>	30
Tabla 3 <i>Requerimientos técnicos mínimos para la instalación de un nodo.</i>	51
Tabla 4 <i>Estimación de costos de recursos humanos y materiales</i>	68
Tabla 5 <i>Comandos útiles para el manejo del nodo.</i>	86

Estructura General del Trabajo Final

Capítulos

El presente trabajo se encuentra formado por cinco capítulos principales. En el primero se hace una introducción al proyecto de intervención, describiendo la problemática abarcada y la posible solución que se plantea, junto con los objetivos generales y específicos que se establecen. Además, se incluye un apartado especial sobre las principales contribuciones que aporta el presente trabajo a la comunidad enfocada, finalizando con el estado del arte de la materia, que presenta los últimos antecedentes. El segundo capítulo describe el marco institucional, incluyendo los entes regulatorios existentes en la Argentina, junto a las normativas y regulaciones vigentes en la actualidad a nivel local. Además, se incorpora un marco teórico que brinda una introducción a los principales conceptos que se abarcarán a lo largo del trabajo.

Durante los capítulos 3 y 4 se desarrolla la propuesta de intervención y su plan de implementación, mediante el cual se dará solución a la problemática abordada en la introducción del trabajo, junto con el análisis de factibilidad del proyecto bajo distintos aspectos. Para concluir, el capítulo 5 introduce las conclusiones y posibles futuras líneas de trabajo que surgirán de la presente propuesta de intervención.

Referencias

En esta sección se encontrará la bibliografía utilizada y citada para la construcción de este trabajo.

Acrónimos

Los acrónimos utilizados a lo largo del trabajo estarán listados y definidos en este apartado.

Anexos

La sección de anexos estará formada por información adicional que facilitará la comprensión de la propuesta de intervención.

Capítulo 1

1.1 Descripción de la problemática

Para comenzar, es fundamental contextualizar la situación de las entidades financieras en Argentina. Nuestro país se destaca como uno de los más complejos en términos de cumplimiento financiero, principalmente debido a la extensa cantidad de regulaciones vigentes. Aunque este aspecto no constituye el objeto de análisis del presente trabajo, resulta pertinente mencionarlo ya que representa la base de la problemática planteada. En este marco normativo, se exige la presentación de diversa documentación ante organismos reguladores como el Banco Central, la Comisión Nacional de Valores (CNV) o la Unidad de Información Financiera (UIF).

En este contexto es habitual que las entidades financieras deban presentar información ante los requisitos provenientes de un ente regulatorio. Pero si a esta situación le sumamos que normalmente los bancos son auditados en paralelo por consultores externos, su propia área de auditoría interna, o incluso otras entidades regulatorias, nos encontramos con una situación donde el banco debe responder a varias auditorías en simultáneo, y como suele suceder, debe presentar en cada una la misma información. Esto conlleva demostrar la originalidad e integridad de la documentación provista a cada parte interesada, lo cual puede traducirse en una pérdida de tiempo para el usuario auditado, ya que debe repetir un mismo proceso en reiteradas ocasiones.

1.2 Propuesta de Solución

En el presente trabajo propondremos a lo largo de los distintos capítulos una alternativa a este proceso de presentación de documentación regulatoria, donde planteamos la posibilidad de utilizar una tecnología de vanguardia y en constante auge como lo es Blockchain, brindando principalmente transparencia y fiabilidad al proceso gracias a las características propias de esta nueva tecnología. El proyecto se basa en la aplicación de un hash a la documentación que deben presentar las entidades financieras, con el posterior almacenamiento del hash generado en una Blockchain, de modo que cualquier parte interesada en el documento pueda verificar la originalidad del documento comparando el hash que genera el mismo contra el que se encuentra resguardado en la Blockchain. Con la solución planteada la parte auditada se ahorraría tiempos

administrativos respecto a la presentación de la misma documentación ante distintos reguladores.

1.3 Objetivos del Trabajo Final

1.3.1 *Objetivo General.*

Implementar un mecanismo basado en blockchain que permita validar la documentación presentada ante entes reguladores del ámbito financiero argentino.

1.3.2 *Objetivos Específicos.*

- Especificar cómo la solución planteada se integrará con los métodos existentes.
- Presentar un plan de implementación del sistema de validación de documentos con su respectivo cronograma.
- Analizar la factibilidad de implementación del proyecto, describiendo posibles limitaciones, en términos operativos, técnicos y económicos.

1.4 Contribuciones Principales

Esta propuesta brindará una herramienta para gestionar y agilizar el proceso de presentación de documentación regulatoria por parte de entidades financieras frente a los requisitos establecidos por los entes controladores, ofreciendo una plataforma basada en blockchain que promueva la transparencia, seguridad, eficiencia y descentralización. La solución presentada eliminará la redundancia en la entrega y verificación de información, permitiendo que los datos sean certificados y validados directamente a través de la Blockchain. Además, al automatizar los procesos de verificación documental, se logrará una significativa reducción de la carga administrativa y el tiempo invertido en tareas repetitivas.

Otro aspecto relevante será la seguridad y transparencia que aporta la tecnología blockchain. Este sistema incrementará la integridad y trazabilidad de los documentos, garantizando su inalterabilidad y permanencia. Esto proporcionará un registro inmutable que minimiza los riesgos de fraude y manipulación, fortaleciendo la confianza en los procesos de certificación documental.

Desde el punto de vista operativo, la propuesta contribuirá a la optimización de recursos. Al reducir las tareas operativas relacionadas con la presentación y validación de documentación, las instituciones podrán enfocarse en actividades de mayor valor estratégico. Asimismo, el proyecto tendrá un impacto positivo en la confianza pública y el cumplimiento normativo, ya que al garantizar la autenticidad de los documentos mediante el uso de blockchain, se fomentará la transparencia en los sistemas de control regulatorio y se asegurará el cumplimiento de las normativas vigentes, contribuyendo a fortalecer la percepción de confiabilidad en los procesos regulatorios.

Capítulo 2

2.1 Marco Institucional

2.1.1 Introducción

La Argentina ha formado con el transcurso de los años un marco institucional financiero constituido por un conjunto de leyes, regulaciones y entidades gubernamentales encargadas de supervisar y regular las actividades relacionadas con el sector financiero en el país. Estas regulaciones son fundamentales para garantizar la estabilidad y la integridad del sistema financiero, proteger a los inversores y consumidores, y promover un entorno económico saludable.

El marco regulatorio financiero en Argentina abarca una amplia gama de áreas, desde la banca y los mercados de valores hasta los seguros y las inversiones. Estas regulaciones son fundamentales para proteger a los consumidores, prevenir el lavado de dinero y la financiación del terrorismo, y promover la estabilidad del sistema financiero.

Es importante destacar que este marco regulatorio está en constante evolución para adaptarse a las necesidades cambiantes de la economía y la sociedad argentinas, así como para cumplir con los estándares internacionales y las mejores prácticas en el ámbito financiero.

2.1.2 Entes Regulatorios

Existen varias entidades y organismos regulatorios que desempeñan un papel crucial en la supervisión y regulación de las actividades financieras. Algunos de los organismos más destacados son:

El Banco Central de la República Argentina (BCRA) es la entidad central encargada de la regulación y supervisión del sistema financiero argentino. Entre sus responsabilidades se encuentra la emisión de moneda, la regulación de bancos y entidades financieras, la formulación de políticas monetarias y cambiarias, y la protección de la estabilidad financiera. (BCRA, s. f.,)

La Comisión Nacional de Valores (CNV) es la entidad que regula y supervisa los mercados de valores y las actividades relacionadas con valores negociables en Argentina. Su objetivo es garantizar la transparencia y la integridad de los mercados financieros. (CNV, s. f.).

La Superintendencia de Seguros de la Nación es una entidad que supervisa y regula el mercado de seguros en Argentina, protegiendo los intereses de los asegurados y asegurando la solvencia y el cumplimiento de las compañías de seguros. (SSN, s. f.)

La Superintendencia de Entidades Financieras y Cambiarias (SEFyC) es la autoridad encargada de supervisar y regular las actividades de las entidades financieras, incluyendo bancos, cooperativas de crédito y otras instituciones financieras. (SEFyC, s. f.)

La Unidad de Información Financiera (UIF) es la entidad encargada de prevenir y combatir el lavado de dinero y la financiación del terrorismo en Argentina. Supervisa y regula las actividades financieras y comerciales para identificar y prevenir actividades sospechosas. (UIF, s. f.)

2.1.3 Normativas y Regulaciones Vigentes

Dada la magnitud de los entes regulatorios antes mencionados, evidentemente existen una infinidad de normativas que regulan a las sociedades financieras en la argentina. Entre ellas, mencionaremos especialmente el art. 61 de la ley 19.550 de Sociedades Comerciales, y su posterior modificatoria, la ley 27444, que en su artículo 21 autoriza la utilización de medios no tradicionales de registración (ordenadores, medios mecánicos, magnéticos u otros) previa autorización del órgano de control, para llevar los libros societarios y contable (Boletín Nacional, 2018).

También están las comunicaciones del Banco Central, entre las más importantes en el ámbito de sistemas de la información están las Comunicaciones “A” 4609 y 6375, reemplazadas durante el año 2023 por la Com. “A” 7724, la cual establece los requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información, la prevención del fraude y la ciberresiliencia para las Entidades Financieras (BCRA, 2023a). También debemos mencionar la Comunicación “A” 6017, y su posterior modificatoria, la Com. “A” 7783, que establece una nueva base de “requisitos mínimos de gestión, implementación y

control de los riesgos relacionados con tecnología informática y seguridad de la información” (BCRA, 2023b) aplicables a Entidades Financieras y Proveedores de Servicios de Pago.

Cabe mencionar que destacamos estas normativas ya que son las principales utilizadas como base de las auditorías que anualmente reciben las entidades bancarias, ya sea por parte del Banco Central, el auditor externo o la propia área de auditoría interna.

2.2 Estado del Arte

La adopción de la tecnología blockchain en el sector bancario ha llevado a diversas innovaciones y mejoras en procesos financieros clave, como, por ejemplo, la implementación de la “JPM Coin” por parte del banco JPMorgan. Esta innovación presenta un sistema que funciona como una vía de pago y un registro de cuentas de depósito, que permite a los clientes participantes de J.P. Morgan transferir dólares estadounidenses mantenidos en depósito con J.P. Morgan dentro del sistema, facilitando el movimiento de financiación de liquidez y pagos en tiempo real. Estas soluciones tecnológicas utilizadas por JPM Coin tienen la capacidad de respaldar tipos de pago avanzados como DvP (Delivery versus Payment), PvP (Payment versus Payment) y machine-to-machine payments, ayudando a resolver los obstáculos comunes de los pagos transfronterizos tradicionales (JPMorgan, 2019, Sección “About Coin Systems”, párr. 2-3). En los últimos años, JP Morgan sigue trabajando en las soluciones blockchain y ha creado Kinexys, la primera plataforma del mundo basada en blockchain dirigida por un banco, y que tiene la finalidad de optimizar y agilizar el intercambio de activos e información por todo el mundo (Kinexys by JP Morgan, 2024). Algunos grandes bancos de inversión ya han hecho uso de este servicio de JP Morgan, como BlackRock para tokenizar acciones de uno de sus fondos y transferirlas a Barclays (CoinDesk, 2023)

De forma similar, el banco HSBC (2019) publicó un artículo donde indica que está aprovechando los beneficios de la tecnología blockchain en áreas importantes como la introducción de contratos inteligentes, lo que da más rigor a las órdenes de compra y pago. Según HSBC (2021), a finales del año 2019 la sede en Hong Kong realizó la primera operación de una carta de crédito blockchain denominada en renminbi, esto con el objetivo de empezar a utilizar la tecnología para optimizar el financiamiento en el comercio exterior. En este sentido, el mecanismo implementado, de acuerdo con lo que indica HSBC (2019) funciona con un

contrato de venta entre exportador e importador que se comparte con el banco del importador mediante un contrato inteligente en blockchain. En tiempo real, el banco del importador revisa el contrato de venta, redacta los términos de la carta de crédito y presenta la obligación de pago al banco del exportador. El banco del exportador revisa la obligación de pago proporcionada y, una vez aprobada, se generará un contrato inteligente en blockchain para cubrir los términos, condiciones y las obligaciones de bloqueo. Después de recibir las obligaciones, el exportador firmará digitalmente una carta de crédito en blockchain dentro del contrato inteligente para iniciar el envío. Los bienes serán inspeccionados por terceros y el agente de aduanas en el país exportador, y todos proporcionarán su respectiva firma digital de aprobación en el contrato inteligente de blockchain. Las mercancías se transportarán del país A al país B y en el momento de la entrega, el importador acusará digitalmente el recibo de la mercancía y activará el pago. Ya con el acuse proporcionado, la blockchain realizará el pago automático del importador al exportador a través de un contrato inteligente (Sección “Mecanismo de transacción basado en blockchain”, párr. 1-7).

Otro antecedente se da con R3 y el consorcio Corda (2023). R3 es una empresa de software que lidera un consorcio diseñado para desarrollar y fomentar las aplicaciones de la tecnología blockchain en los negocios, mientras que Corda es un sistema de contabilidad distribuida diseñado por R3 desde cero para operar dentro de las empresas y entre ellas. Según R3 (2023), a diferencia de muchas otras plataformas blockchain, Corda no busca crear una cadena de bloques pública y abierta que cualquiera puede ver y acceder. En cambio, está configurada para ser utilizada dentro de redes privadas en las que los participantes tienen acceso controlado a datos específicos, conservando la privacidad y cumpliendo con las regulaciones (p. 3).

Corda se ha utilizado en una variedad de aplicaciones, desde financiamiento comercial hasta seguros y salud. Por ejemplo, el proyecto "Marco Polo", que de acuerdo con Michael Glaros (2019), usa Corda para digitalizar y automatizar el financiamiento del comercio internacional, optimizando así los flujos de trabajo y reduciendo los riesgos. El desarrollo de Corda por R3 representa uno de los esfuerzos más significativos hacia la adopción de la tecnología blockchain en el sector empresarial, ofreciendo innovaciones que resuelven problemas específicos relacionados con la privacidad, la escalabilidad y la integración de sistemas corporativos (párr. 1).

Otro caso para mencionar es el de BNP Paribas, el banco más grande de Francia, que ha sido durante años el más grande de Europa y se encuentra entre los más grandes del mundo por volumen de activos. Junto a los ya mencionados JP Morgan y HSBC, BNP Paribas ha sufrido sanciones tras la crisis financiera del 2008 al ser juzgados por blanqueo de capitales. Quizá esta fue una de las razones que llevó a BNP Paribas a comenzar la implementación de medidas en materia de transparencia y seguridad de la información y las operaciones. Johann Palychata, director de producto de BNP Paribas, cree que el blockchain debería considerarse un invento del calibre del motor de combustión, pues tiene el potencial de revolucionar el mundo financiero (Crosby et al., 2016, p. 8).

Palychata considera también que el proceso de micro financiación de un banco de inversión puede beneficiarse notoriamente incorporando blockchain, pues la cadena de bloques facilita la gestión y registro de acciones financiadas de esta forma al crear estandarización, aumentando también la transparencia y la confianza del mercado (Muneeza & Mustapha, 2020, p. 24).

Además de la gestión de fondos, BNP Paribas avanza en el uso de esta tecnología empleándola en la compartición segura de datos personales gracias a la alianza con la empresa emergente Pikciochain, pues a través de esta entidad blockchain el banco logra transferir datos de una forma segura, ofreciendo transparencia a los clientes en la trazabilidad de su información, su uso, y los usuarios por los que pasa (Badiss et al., 2019, p. 1).

Por otra parte, el Banco Santander también tuvo su aporte al ecosistema con el lanzamiento del servicio Santander One Pay FX (2018). Si bien fue anunciado en 2018, no fue hasta 2020 que se consolidó como un servicio internacional disponible en España, Reino Unido, Brasil, Polonia, Chile y Portugal. Se trata de un servicio de transferencias internacionales con el uso de tecnología basada en blockchain que permite hacer transferencias internacionales entre particulares de forma más rápida, ya que llegan a destino el mismo día en muchos casos o al día siguiente. Además, permite a los clientes conocer el importe exacto que llegará en la moneda del destinatario antes de confirmar la transacción (Banco Santander, 2018, p. 1).

Algo similar ocurre con el caso de Goldman Sachs, uno de los grupos de banca de inversión y de valores más relevantes a nivel mundial, destacado en sus servicios de asesoramiento en fusiones y adquisiciones. Ya en el año 2016, Goldman Sachs Investment

Research realizó un informe en el que detallaba muchos de los beneficios que la implantación de la tecnología Blockchain podía aportar a los diferentes sectores en los que sus fondos y líneas de inversión operaban. Destacó que no sólo supondría una reducción de intermediarios, sino que ofrecía la posibilidad de minimizar el fraude y la corrupción, aumentando la transparencia y la eficiencia en las transacciones, además de los múltiples ahorros en costes que significaría su aplicación (Rizzo, 2016). En 2019 anunció su intención de crear una nueva stablecoin, al igual que hizo JP Morgan con su JPM Coin. Esto se enmarca perfectamente con el nuevo rumbo de la compañía pues, como indicó su director ejecutivo David Salomon, Goldman Sachs se encuentra realizando profundas investigaciones en tokenización, monedas digitales, transformación de monedas o gestión de activos mediante contratos inteligentes en cadenas de bloques. Considera también que el futuro de los sistemas de pagos pasa por la descentralización y el empleo de stablecoins vinculadas a monedas fiduciarias reales (Broome, 2019, p. 8), además de considerar que en los próximos años el sector financiero pasará por el uso de las redes privadas, pues las transacciones de alto valor requerirán privacidad y la confianza de los participantes en la transacción (Rizzo, 2016). El mercado de los criptoderivados está ganando cada vez más interés por parte de los clientes y es algo que Goldman Sachs sabe y pretende explotar (Howcroft, 2023). Es por eso que su director global de gestión de activos digitales, Mathew McDermott, expresa que no se limitan solo a las criptomonedas, sino que se centran también en el desarrollo y emisión de tokens basados en blockchain que representen activos digitales, como los bonos tradicionales. De hecho, un 16% de los clientes del banco espera que al menos el 10% del mercado se tokenice en un periodo inferior a cinco años (Howcroft, 2023). Esto se da ya que el banco de inversión percibe gran potencial en el mercado debido a la eficiencia operativa y de liquidación que ofrece la tecnología blockchain, la reducción del riesgo, y la mayor precisión y rapidez en las garantías con los clientes (Howcroft, 2023).

Hasta aquí hemos presentado los antecedentes encontrados en el sistema financiero, pero existen otros autores que proponen que el uso de la tecnología blockchain, por fuera del ámbito bancario, brindaría grandes beneficios a la eficiencia de ciertos procesos administrativos relacionados a la verificación de documentación. Entre ellos encontramos a Marta Jiménez (2019), quien asegura que es posible utilizar la tecnología Blockchain en un sistema confiable que permita a las financieras validar si una factura está en un proceso de adelanto de pago o ya se ha pagado, evitando cualquier tipo de fraude (p. 13). Además, Jiménez (2019) afirma que:

Todas las entidades de financiación y empresas pagadoras en general pueden consultar el estado real del pago de una factura de una manera confiable y segura dejando un registro de los cambios que se han producido sobre el documento desde su inserción en la cadena de bloques por parte de una entidad autorizada. (p. 13)

Otros autores aseguran que el uso de blockchain puede ser implementado en el proceso de certificación de títulos académicos. Santiago Gómez (2023) plantea “un modelo para preservar y verificar criptográficamente los documentos requeridos para la emisión de una certificación académica dentro de una institución universitaria” (p. 1). Gómez se enfoca en el hecho de que las sociedades actuales “se basan en el uso de credenciales verificables para que los individuos puedan probar afirmaciones sobre su identidad” (p.1), para lo cual propone una solución llamada “VeriDoc-Chain”, para el aseguramiento y verificación de documentos basado en blockchain, con un almacenamiento de documentos descentralizado en IPFS y un sistema de identificación y autenticación que utiliza identificadores descentralizados implementados bajo el meta-sistema SSI de Veramo (Gómez, 2023, p. 2). Por su parte, Ian Martínez (2023) propone “crear la arquitectura y diseño de una plataforma tecnológica que, utilizando la tecnología blockchain, permita a las instituciones académicas y entes reguladores simplificar y mejorar los procesos de emisión, representación gráfica, entrega, trazabilidad, seguridad y validación” (p. 5) de títulos académicos. Martínez (2023) afirma que “la implementación de este tipo de solución para la emisión de certificados académicos (...) puede ayudar en gran medida a solucionar las problemáticas de falsificación y tramitología asociadas al proceso” (p. 83). Además, Martínez (2023) menciona que esta solución logra disminuir tiempos y recursos en instituciones académicas, dando como ejemplo la eliminación de los procesos de imprenta y firma en físico de certificados académicos (p. 83).

2.3 Marco Teórico

2.3.1 Introducción

La tecnología blockchain ha irrumpido en el mundo con un potencial revolucionario, alterando las nociones tradicionales de confianza, transparencia y seguridad en una amplia gama de industrias y aplicaciones. Esta innovación, inicialmente concebida como la

infraestructura detrás de las criptomonedas como Bitcoin, ha evolucionado para convertirse en una fuerza transformadora que impacta en áreas que van desde las finanzas y la cadena de suministro hasta la atención médica y la gobernanza.

A medida que avancemos en este marco teórico, exploraremos los principios de descentralización, consenso y criptografía que son la columna vertebral de la blockchain. Analizaremos cómo las transacciones se registran de manera segura en bloques encadenados y cómo los contratos inteligentes están redefiniendo la automatización de acuerdos y procesos. Además, se iremos descubriendo cómo la blockchain está sentando las bases para una nueva era de confianza descentralizada y cómo puede abrir la puerta a una multitud de innovaciones que aún están por descubrirse.

2.3.2 La tecnología Blockchain

Blockchain es una tecnología diseñada para administrar un registro de datos online, caracterizada por ser transparente y prácticamente incorruptible (Franca, 2019, p. 4).

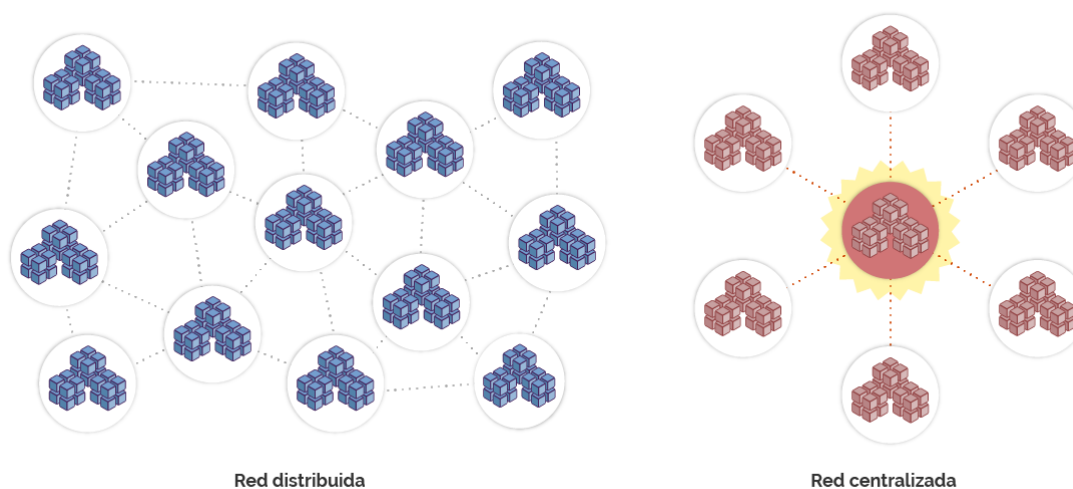
De acuerdo con Satoshi Nakamoto (2008), el concepto de Blockchain fue introducido por primera vez como una solución entre pares (peer-to-peer), para poder enviar y recibir pagos directamente sin necesidad de la participación de un intermediario, como lo es un banco o cualquier institución financiera. La primera implementación de esta tecnología fue la criptomoneda Bitcoin (p. 1).

En términos generales, como menciona la Daniel Franca (2019), el concepto de Blockchain puede asimilarse a un registro financiero, un diario o una base de datos en la que únicamente es posible introducir nuevas entradas, y donde ninguna de las entradas existentes puede ser alterada ni eliminada. Estas entradas, conocidas como transacciones, son agrupadas en bloques que se añaden de manera consecutiva al registro, formando una cadena secuencial en la que cada bloque está intrínsecamente vinculado al anterior (p. 4).

Bajo esta estructura, afirma la Blockchain Federal Argentina (BFA, s. f.) que:

Si quisiéramos corregir información ya registrada, solo lo podemos hacer mediante el agregado de nueva información. Los datos originales siempre van a permanecer y pueden ser fiscalizados en cualquier momento.

Ahora pensemos que ese registro en lugar de estar almacenado en un solo servidor, se replica permanentemente en un conjunto de computadoras -conocidos como “nodos”- que forman una red de pares. Cada vez que alguien agrega una entrada al registro, esa transacción se suma a otras para componer un bloque. Este se agrega a la cadena y de forma casi automática se replica en todas esas computadoras conectadas. (Sección “Cómo funciona”, párr. 2-3)

Figura 1*Tipos de redes*

Nota. El gráfico de la izquierda representa una red distribuida, donde se observa que ningún nodo ejerce de nodo central. A la derecha, el gráfico de una red centralizada, donde existe un nodo central que conecta con todos los otros nodos existentes en la red. Tomado de ¿Qué es la Blockchain?, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/blockchain/blockchain>)

De esta manera, se asegura la seguridad de la información, ya que, como bien explica Daniel Drescher (2017), sería necesario "hackear" una gran parte de la red en lugar de un servidor central único para poder realizar modificaciones, eliminar datos o sustraer información. Sin embargo, es esencial considerar que la seguridad de la blockchain no se basa únicamente en su estructura descentralizada, sino que también se apoya en técnicas criptográficas que aseguran que ninguna modificación o eliminación de datos pueda llevarse a cabo sin que todos los usuarios lo detecten (p. 61).

Tabla 1*Comparativa de tipos de privacidad en Blockchain*

Propiedad	Privada	De Consorcio	Pública
Determinación del consenso	Una sola organización	Nodos seleccionados	Mediante todos los mineros
Permiso de lectura	Pública o restringida	Pública o restringida	Pública
Inmutabilidad	Manipulable	Manipulable	Casi imposible de manipular
Eficiencia	Alta	Alta	Baja
Centralizado	Si	Parcialmente	No
Proceso de consenso	Mediante Permisos	Mediante Permisos	Sin Permisos

Nota. Adaptado de Zheng et al. (2017, p. 559)

2.3.3 Criptografía

“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” (Franca, 2019, p. 7).

¿Qué es un hash?

Un hash es, según Drescher (2017), un código que se obtiene al procesar información a través de una función. Si se modifica, 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 (p. 83).

Como menciona Jonathan Waldman (2018):

Aunque hay muchas variantes de algoritmo de hash criptográfico unidireccional, a menudo se usa SHA-256, una función hash unidireccional que acepta un mensaje de hasta $(2^{64}-1)/8$ bytes y devuelve un valor hash de 32 bytes (64 caracteres hexadecimales) del intervalo de decimales de 0 a, aproximadamente, $1,16 \times 10^{77}$. Al retocar cualquier carácter del mensaje y volver a calcular el valor de hash SHA-256, se genera un valor de hash completamente nuevo. (Sección “Componentes principales de la cadena de bloques”, párr. 1)

De esta manera, y tal como indica Franca (2019):

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, dado que no es posible reconstruir la información original a partir de un hash, se garantiza que no se otorga acceso a personas no autorizadas, incluso si ese hash se encuentra registrado de forma pública en la Blockchain. (p. 8)

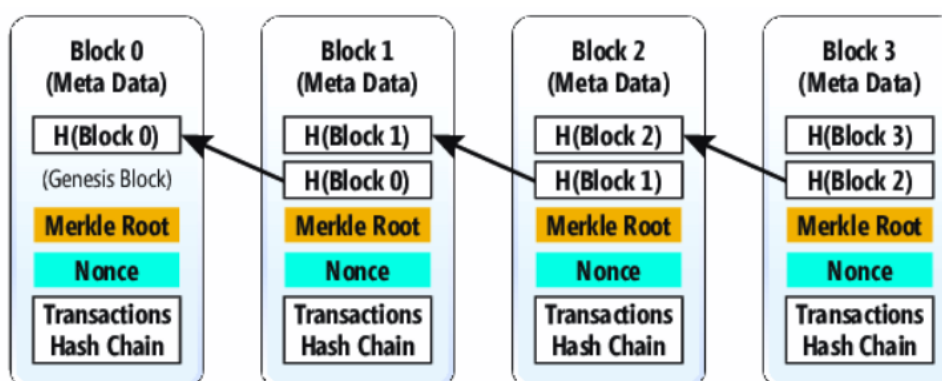
2.3.4 Bloques y Transacciones

Como se comentó anteriormente, el hash también juega un papel elemental en la arquitectura de Blockchain. Franca afirma que “cada bloque de información que se suma al registro posee necesariamente el hash del bloque de información anterior” (p. 9).

Como explica Jonathan Waldman (2018), “para crear una cadena de bloques, el objeto de datos de cadena de hash binario que contiene transacciones se debe enviar de algún modo a un almacén de datos a prueba de manipulación que cualquier usuario pueda utilizar” (Sección “Creación de una cadena de bloques”, párr. 1). Waldman agrega que “la estructura del árbol de Merkle [presentado en la Figura 1] contiene transacciones y está a prueba de manipulación, así que, en principio, podría servir como cadena de bloques” (Sección “Creación de una cadena de bloques”, párr. 1) siempre y cuando se utilicen algoritmos o protocolos de consenso.

Figura 2

Esquema de blockchain basado en el árbol de Merkle.



Nota. La cadena de bloques está formada por bloques que, a su vez, incluyen árboles de hash de transacción; los bloques de la cadena de bloques se vinculan mediante un vínculo de retroceso a los bloques anteriores y se validan mediante un algoritmo de prueba de trabajo. Tomado de Creación de una cadena de bloques, por Jonathan Waldman, 2018, Microsoft Learn (<https://learn.microsoft.com/es-es/archive/msdn-magazine/2018/march/blockchain-blockchain-fundamentals>)

Este mismo modelo es planteado en el whitepaper de Bitcoin, escrito por Satoshi Nakamoto (2008), quien explica que 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 (p. 2).

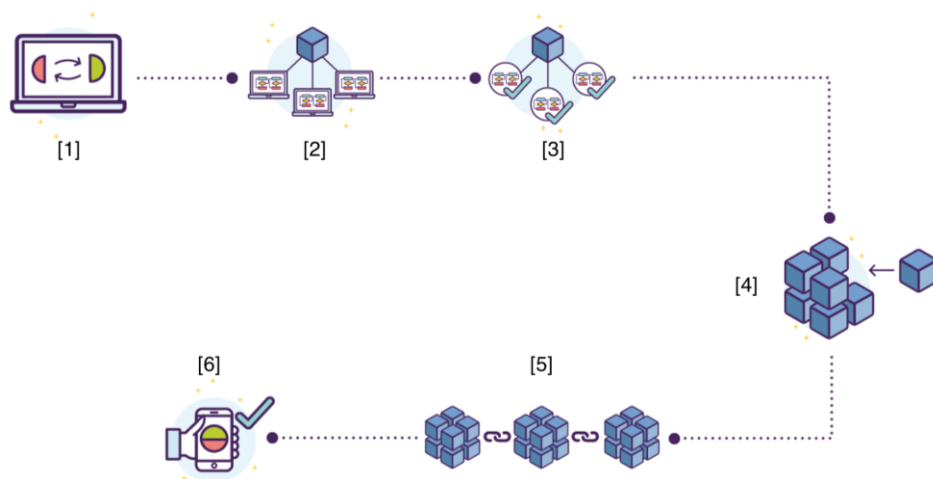
Ahora bien, de acuerdo con lo que indica Franca (2019), estos bloques que van llenando de información la blockchain por medio de distintos tipos de operaciones, denominadas

transacciones. El contenido de estas transacciones puede variar considerablemente, y generalmente depende del tipo de red que se esté utilizando. Por ejemplo, algunas blockchains permiten la carga de archivos digitales en el registro a través de transacciones, mientras que otras se centran en operaciones de compra y venta de activos criptográficos. Una transacción puede ser tan simple como una línea de texto o incluso un hash que hace referencia a un documento almacenado fuera de la cadena de bloques (p. 10).

Como menciona Satoshi Nakamoto (2008), cada transacción se envía a la red mediante un nodo y se agrupa con otras transacciones para formar un bloque. Cuando este bloque se añade a la cadena, la transacción se considera definitivamente incorporada y se marca como "completada" (p. 2).

En simples pasos, la Franca (2019) define el proceso de creación de bloques y transacciones de la siguiente forma:

Alguien realiza una operación en la blockchain, conocida como transacción [Paso 1 en la figura 3]. Esta transacción se envía a una red de pares [Paso 2 en la figura 3] formada varias computadoras (nodos). La red de nodos verifica tanto que la transacción esté firmada cómo que el usuario tenga recursos para enviarla [Paso 3 en la figura 3]. Una vez verificada, se combina con otras transacciones para crear un nuevo bloque de datos [Paso 4 en la figura 3], y el nuevo bloque se agrega a la cadena, quedando esta replicada en todos los nodos de forma permanente e inalterable [Paso 5 en la figura 3]. De este modo, la transacción queda finalizada. (p. 11)

Figura 3*Transacciones*

Nota. Flujo de una transacción. Adaptado de Bloques y Transacciones, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/blockchain/bloques-y-transacciones>)

2.3.5 Protocolos de consenso

En el contexto de Blockchain, de acuerdo con la BFA (s. f.), el proceso anteriormente explicado por el cual un bloque de transacciones se configura y se añade de forma permanente a la cadena se conoce como sellado o minado. Una vez que un bloque ha sido sellado, su contenido se integra a la cadena de manera definitiva, haciéndolo inmutable e inalterable. El Protocolo de Consenso, por su parte, es el mecanismo que establece cómo los nodos encargados del sellado de bloques alcanzan un consenso para efectuar esta acción y así integrar el bloque a la cadena (párr. 1).

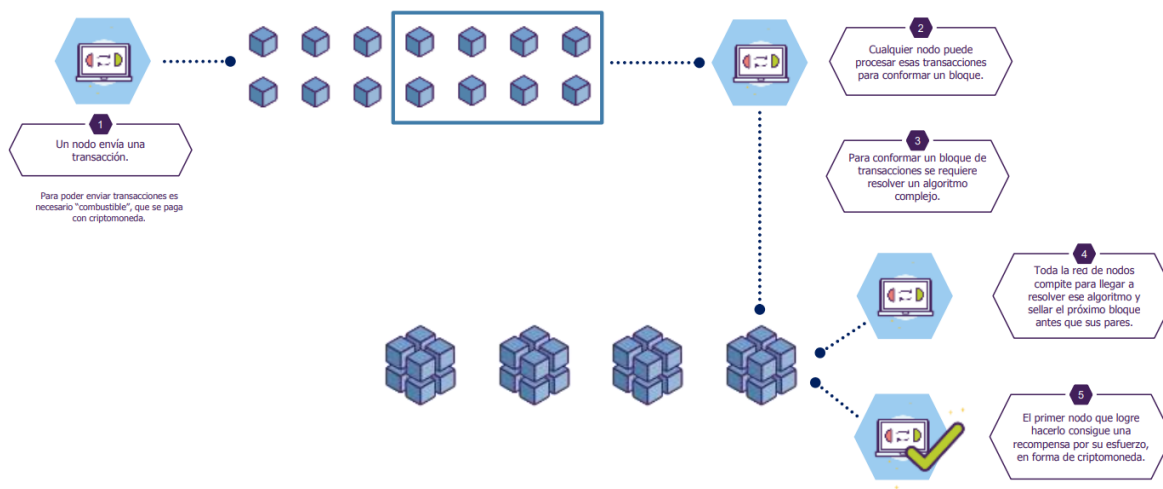
Uno de los protocolos más reconocidos globalmente es el llamado Proof of Work (PoW). Jonathan Waldman (2018) lo explica de la siguiente manera:

PoW se basa en la idea de que un nodo de la red debe demostrar sus buenas intenciones incurriendo en un costo y dedicando el tiempo necesario para resolver un problema complicado desde el punto de vista computacional. Para inducir a un nodo para que

participe en dicho sistema y siga sus reglas, la red ofrece un incentivo (a menudo, dinero); es decir, se paga a los operadores del nodo por agregar un bloque a la cadena de bloques. Para ganar ese dinero, los nodos deben validar todas las transacciones (para asegurarse de que cumplen las reglas específicas de la cadena de bloques) y, a continuación, resolver un enigma criptográfico. (Sección “Creación de una cadena de bloques”, párr. 4)

Figura 4

Funcionamiento del protocolo PoW



Nota. 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. Tomado de Protocolos de Consenso, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/blockchain/protocolos-de-consenso>)

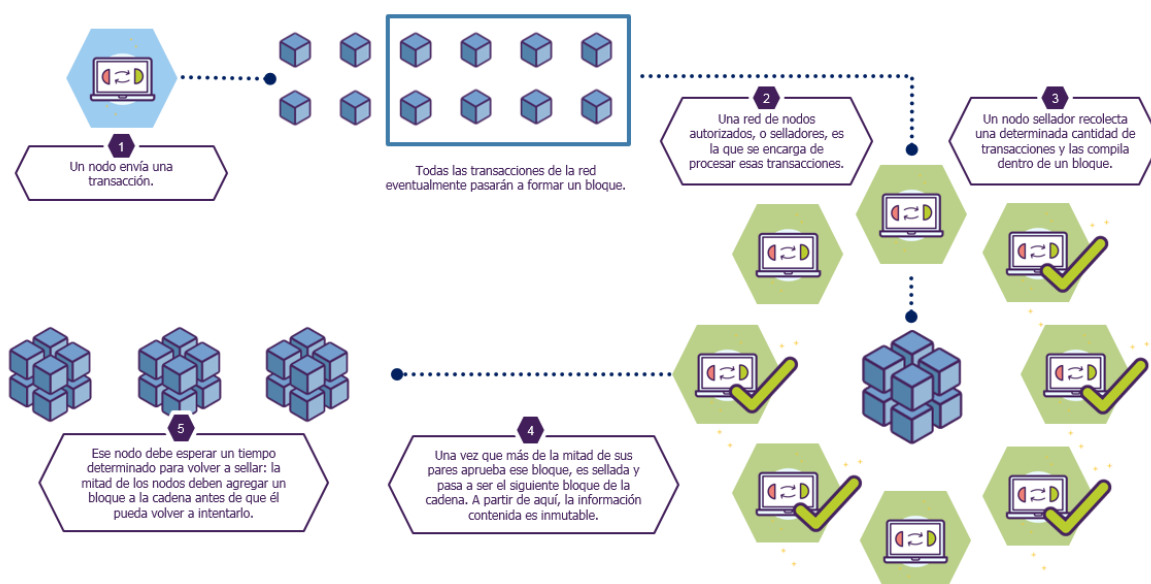
Entonces, observando la Figura 4 se entiende que en este modelo todos los nodos son pares iguales en la red, y todos compiten para sellar un bloque antes que el resto y poder conseguir criptomoneda a cambio. Para realizar esto, deben resolver un algoritmo complejo. El que primero logre hacerlo y pueda 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.

Por otro lado, existe un protocolo llamado Proof of Stake (PoS), el cual según Zheng (2017) es una alternativa al Proof of Work (PoW) que resulta más eficiente en términos de costos. En este sistema, los participantes deben demostrar la posesión de una cantidad específica de moneda para poder minar. A pesar de que se supone que quienes poseen más moneda son menos propensos a atacar la red, este método puede ser percibido como injusto ya que tiende a favorecer la dominación de la red por parte de un solo individuo. Dado estos problemas, se han propuesto diferentes soluciones que buscan una manera más equitativa de determinar qué nodo producirá el siguiente bloque dentro de la cadena de bloques (p. 560).

Otro protocolo disponible en la actualidad es el Proof of Authority (PoA). En este modelo, solo existe una cantidad determinada de nodos que están autorizados a resolver el sellado de bloques.

Figura 5

Funcionamiento del protocolo PoA



Nota. Hay redes de Blockchain que optan por un modelo de Proof of Authority donde solo algunos nodos autorizados pueden crear bloques que contengan transacciones. Tomado de Protocolos de Consenso, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/blockchain/protocolos-de-consenso>).

Según Stefano De Angelis (2018), 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 no existe necesidad de resolver algoritmos complejos, la cantidad de procesamiento es mínima. Es por ello que a estos modelos se los considera 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 (p. 3).

A continuación, se observa en la Tabla 2 una comparación sobre las principales características entre los distintos algoritmos de conceso.

Tabla 2

Comparativa de protocolos de consenso

Protocolo	Velocidad	Consumo de Energía	Seguridad	Madurez	Costo
Proof of Work	Lenta	Ineficiente	No confiable (sin permisos)	Probado	Costoso
Proof of Stake	Promedio	Eficiente	No confiable (sin permisos)	No probado	No tan Costoso
Proof of Authority	Rápida	Eficiente	Confiable (mediante permisos)	Probado	Sin Costo

Nota. Adaptado de Asad et al (2020, p. 37).

2.3.6 Contratos Inteligentes

Hasta este punto hemos explicado que la Blockchain opera como un registro de transacciones, pero cabe destacar que también permite la creación de aplicaciones mediante lo que se denomina "contratos inteligentes" o smart contracts. Franca (2019) indica que “estos desarrollos pueden tanto ejecutarse como consecuencia de transacciones como generar, ellos mismos, transacciones nuevas” (p. 18). Además, agrega Franca (2019) que “es verdad que el término puede ser un poco confuso, porque no son justamente contratos. Son más bien flujos

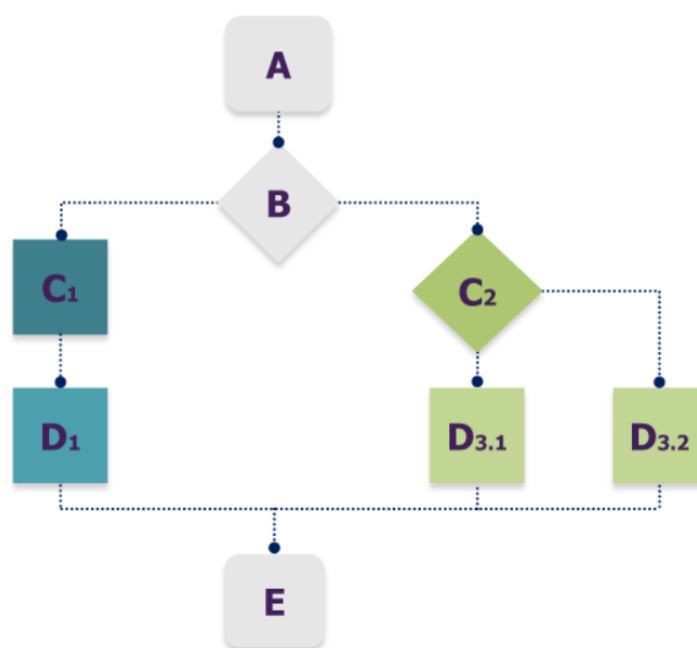
de tareas programables dentro de Blockchain, que abren la posibilidad de desarrollar aplicaciones” (p. 18).

Siguiendo esta línea teórica, Andreas Antonopoulos (2018) define los Smart Contract como simples programas de computadora. La palabra “contrato” no tiene ningún significado legal en este contexto. Una vez lanzado el smart contract, su código no puede ser modificado. A diferencia de cualquier otro software tradicional, la única forma de modificar un smart contract es lanzando una nueva versión o instancia (p. 128).

Adicionalmente, Andreas Antonopoulos (2018) indica que el resultado de la ejecución de un smart contract es el mismo para todos aquellos que lo ejecutan, dado el contexto de la transacción que inició su ejecución y el estado de la cadena de bloques en el momento de la ejecución. Además, los smart contracts operan con un contexto de ejecución muy limitado. Pueden acceder a su propio estado, al contexto de la transacción que los llamó y a cierta información sobre los bloques más recientes. (p. 128)

Figura 6

Flujo de trabajo de Smart Contracts



Nota. El flujograma representa una secuencia de transacciones y smart contracts a modo ilustrativo. Tomado de Smart Contracts, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/blockchain/smart-contracts>).

En referencia a los smart contracts, la Franca (2019) considera que, a diferencia de una aplicación tradicional, en la que debemos confiar en las garantías del desarrollador, un contrato inteligente permite programar un flujo de acciones predeterminado entre las partes involucradas, respaldado por las sólidas garantías de confiabilidad y transparencia proporcionadas por una red blockchain (p.19). En la Figura 6 se observa un flujo que representa el funcionamiento de los smart contracts, donde al finalizar la transacción A se ejecuta un contrato inteligente B que a su vez iniciará otros dos contratos C₁ y C₂. Al final de la figura se observa una transacción E que sólo se realizará cuando los contratos D₁, D_{3.1} y D_{3.2} hayan finalizado.

En este sentido, Franca (2019) dice que:

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. (p. 19)

2.3.7 Aplicaciones actuales de la tecnología

A pesar de tratarse de una tecnología emergente, en la Argentina existen diversos procesos a los cuales se les está aplicando Blockchain, entre ellos:

Licitaciones

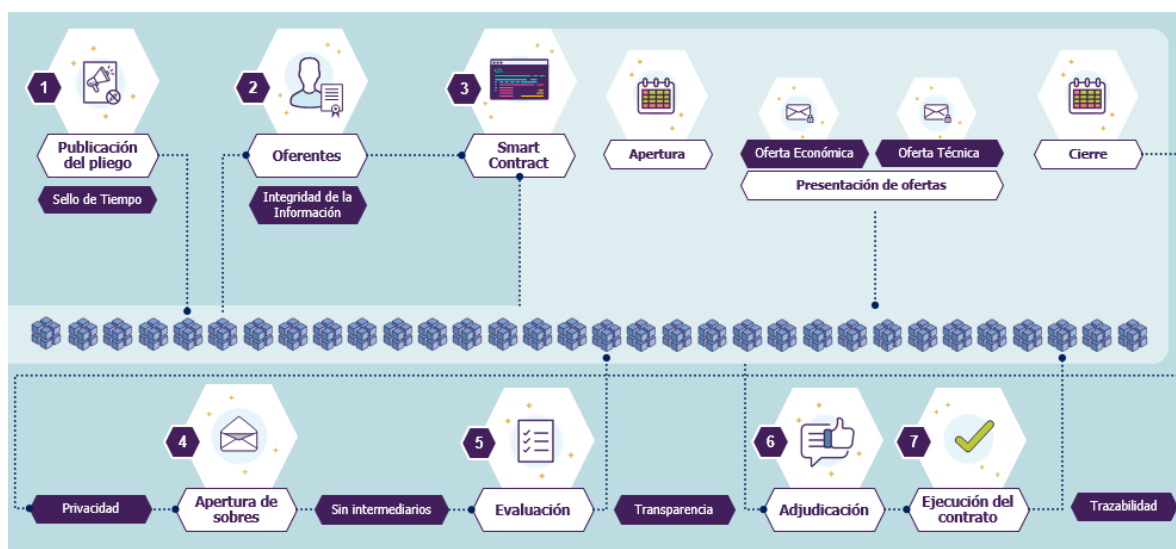
Las compras públicas representan la principal vía de relación directa entre el Estado y el sector privado. También, la Sociedad Civil interviene como parte interesada en los mecanismos de auditoría.

Al incorporar Blockchain a un proceso de licitación, encontramos nuevas formas de facilitar el proceso de auditoría, tanto a los oferentes como a la sociedad en general. Según menciona la BFA (s. f.) “esta tecnología posibilita el desarrollo de una plataforma para la compra de bienes y la contratación de servicios por parte del Estado que garantice transparencia

e impida cualquier tipo de fraude” (Sección “Licitaciones - Aporte de blockchain”, párr. 1), lo cual se logra implementando un sello de tiempo que permite verificar que la licitación no fue modificada luego de su publicación, como se observa en la Figura 7. Además, según indica la BFA (s. f.), la apertura y cierre de licitaciones se encuentra configurada en el smart contract, de modo que sólo los usuarios habilitados como proveedores del estado puedan enviar los hashes de sus ofertas tanto económicas como técnicas dentro del lapso que permanezca abierto el contrato. Así, la apertura y evaluación de ofertas se convierte en un proceso transparente y fácil de fiscalizar.

Figura 7

Caso de uso en licitaciones.



Nota. El gráfico representa el flujo de licitaciones utilizando smart contracts. Tomado de Casos de uso –Licitaciones, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/blockchain/casos-de-uso/licitaciones>)

Esto conlleva ciertas ventajas según la BFA (s. f.):

Al estar públicos en la blockchain, y llevar un sello de tiempo, todos los documentos que deben presentar los interesados acordes a los términos de la convocatoria son públicos e inalterables. De este modo, blockchain ofrece las herramientas para que las ofertas digitales sean efectivamente privadas hasta la apertura de los sobres. Esto

optimiza los tiempos de presentación y a su vez mitiga la desconfianza de los oferentes con relación a irregularidades durante el proceso, lo que muchas veces se traducía en ofertas tardías o falta de estas.

Por otro lado, la utilización de smart contracts permite establecer parámetros facilitando la automatización del proceso, de manera transparente, permitiendo entre otras cosas aceptar propuestas o rechazar aquellas que no cumplan con los requerimientos, notificar automáticamente al ganador o ejecutar los procesos administrativos vinculados.

La evaluación se realiza de forma virtual de acuerdo con las condiciones de la convocatoria, pero es completamente pública y transparente, lo cual permite que se puedan fiscalizar las órdenes de compras y las etapas de cumplimiento hasta el fin del proceso, incluyendo la ejecución del contrato. (Sección “Licitaciones - Ventajas”, párr. 1)

Póliza de caución

Quienes intervienen en la emisión de un Seguro de Caución son la Compañía Aseguradora, el Tomador de la póliza y el Beneficiario o “Asegurado”. Este tipo de seguros sirven para el resarcimiento al Asegurado en caso de que el Tomador no cumpla el compromiso asumido en un contrato.

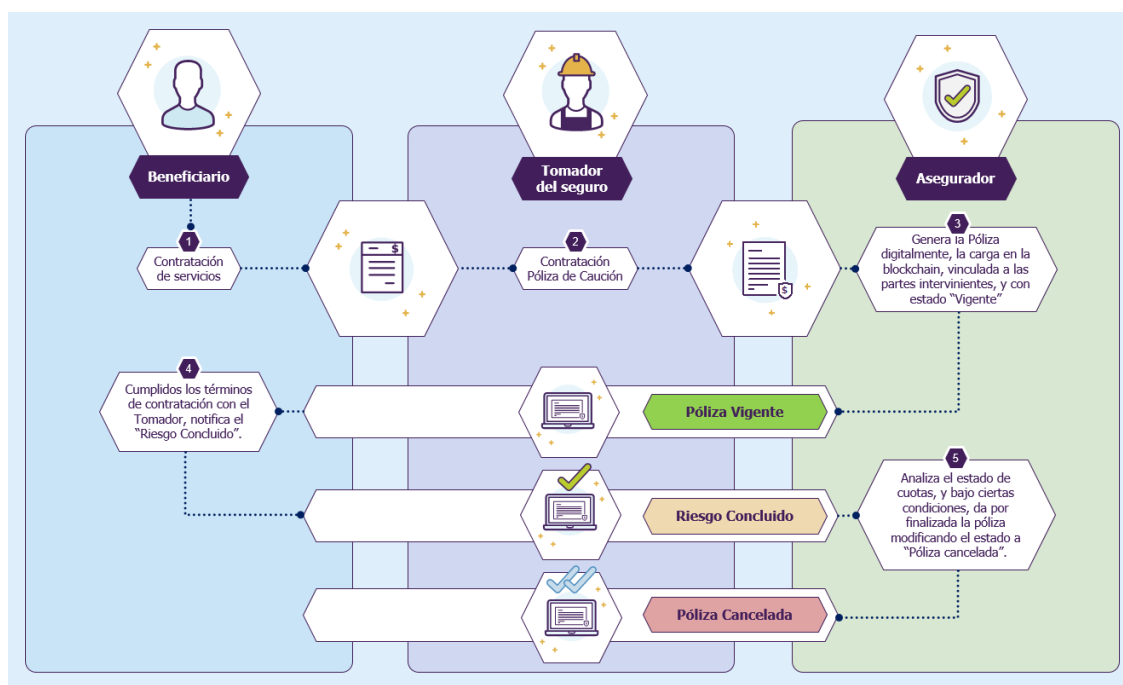
Según indica la BFA (s. f.),

La digitalización del proceso permite emitir una póliza en formato digital y, a su vez, por medio de un Smart Contract, la misma puede ser vinculada a las 3 partes intervinientes. Esto facilita el seguimiento del trámite en base a distintos estados de la póliza, desde la creación del contrato hasta su finalización. Asimismo, es posible monitorear cada instancia y agilizar los sistemas de notificaciones al momento de

realizar cambios en los estados de un seguro en particular. (Sección “Pólizas - Aporte de blockchain”, párr. 1)

Figura 8

Caso de uso en pólizas.



Nota. El gráfico representa el flujo de registración de pólizas en Blockchain. Tomado de Casos de uso – Póliza de Caución, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/blockchain/casos-de-uso/poliza-de-caucion>)

Continuando con las afirmaciones de la BFA (s. f.), el uso de esta tecnología presenta como ventajas que se evitan contratiempos por pérdida de documentación y se agiliza el proceso de notificaciones. Además, permite el monitoreo del estado de la póliza por todas las partes intervinientes como un documento digital “vivo”, de modo que los estados del documento se garantizan de forma fehaciente gracias a Blockchain (Sección “Pólizas - Ventajas”, párr. 1).

Títulos académicos

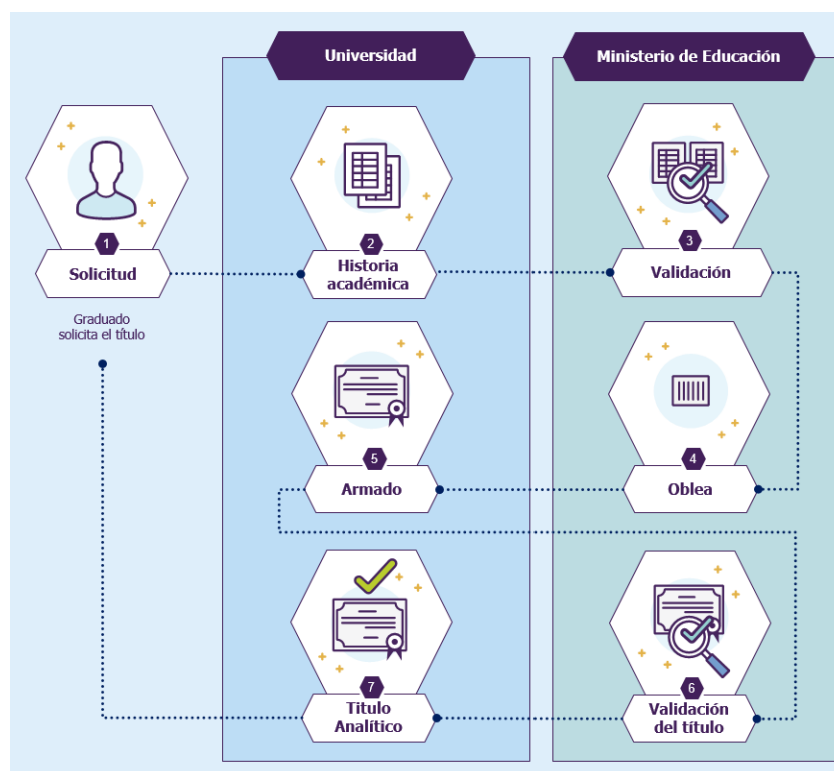
En este proceso intervienen los alumnos que solicitan su título académico, la institución educativa que valida la aprobación de las materias y emite el título dando

constancia de la finalización de la carrera, y el Ministerio de Educación que certifica el título en cuestión.

Gracias a distintos desarrollos que se pueden realizar en blockchain como los “sellos de tiempo”, según la BFA (s. f.) se puede asegurar que los documentos no sean susceptibles a alteraciones. Esto se logra mediante la creación de resúmenes criptográficos (hashes) de historiales académicos o diplomas, que son almacenados en la blockchain, permitiendo así confirmar que no han sufrido modificaciones inapropiadas durante todo el proceso. Al desarrollar más esta solución, sería posible hacer que las copias digitales de los títulos académicos sean fácilmente verificables o incluso incorporarlas en un porta documentos digital. Esto permitiría a los poseedores de los documentos gestionar y modificar los permisos de acceso (Sección “Títulos académicos - Aporte de blockchain”, párr. 1-2).

Figura 9

Caso de uso en títulos.



Nota. El gráfico representa el flujo de certificación de títulos en Blockchain. Tomado de Casos de uso – Títulos Académicos, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/blockchain/casos-de-uso/titulos-academicos>).

De este modo, la BFA (s. f.) indica que se presenta como ventaja el hecho de que se garantiza que no sea posible alterar la información de las actas sin que esa modificación sea detectada y así aumenta la confianza en la autenticidad de los títulos emitidos, así como también la transparencia en el proceso de digitalización, lo cual permite un contexto de confianza entre organismos y partes interesadas. Esto conlleva a que se convierta en un proceso totalmente auditable, ya que permite demostrar que no existen actos de negligencia (títulos falsos) en torno a la emisión de títulos, además de que se podría dar diferentes vigencias a certificado de títulos en trámite, o similares, certificadas en la blockchain (Sección “Ventajas”, párr. 1).

Trazabilidad de alimentos

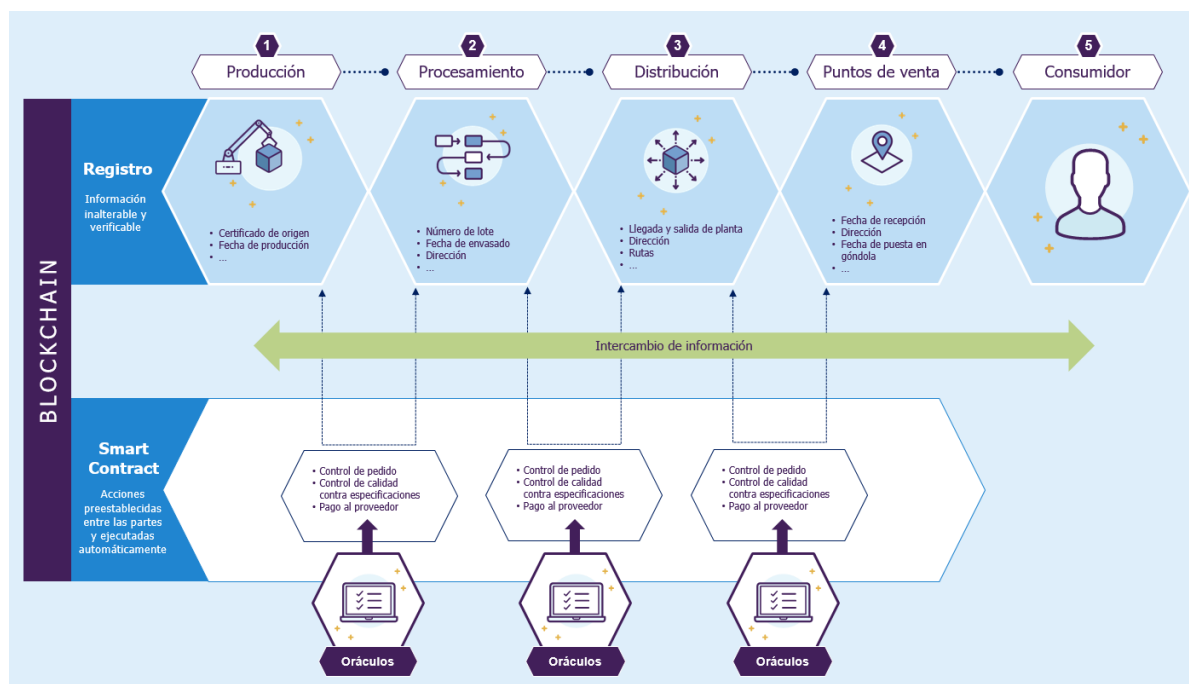
Son múltiples los actores que pueden vincularse dentro del proceso de suministro de alimentos. En este sentido, en un marco general, podemos nombrar, por ejemplo, a agricultores, ganaderos, proveedores, cooperativas, empacadoras, transportistas, exportadores, importadores, mayoristas, minoristas y, por último, al consumidor final.

La BFA (s. f.) manifiesta que:

Blockchain permite rastrear un producto a través de las distintas operaciones industriales, logísticas y administrativas, partiendo desde el inicio del proceso hasta el final, y viceversa. De esta forma, se puede consolidar un registro seguro y distribuido que contiene el historial de todos los actores de la cadena y sus intercambios durante la producción y distribución de cualquier producto. Esto permite gestionar la información de manera transparente, inviolable y a través de datos independientes. (Sección “Trazabilidad de alimentos - Aporte de blockchain”, párr. 1)

Figura 10

Caso de uso en trazabilidad de alimentos.



Nota. El gráfico representa la certificación de los datos por medio de Blockchain, para poder ser controlados en cualquier parte del proceso a través del smart contract. Tomado de Casos de uso – Trazabilidad de alimentos, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/blockchain/casos-de-uso/trazabilidad-de-alimentos>)

Usando esta tecnología, la BFA (s. f.) menciona que se logra la ventaja de generar una cadena de confianza entre las partes involucradas, posibilitando la transparencia en el movimiento de un producto a través de todas sus etapas, partiendo desde la producción hasta llegar al consumidor final. Además, contribuye a la prevención de incidencias dado que facilita la ubicación de productos o lotes y, en caso de surgir inconvenientes, facilita la retirada efectiva y selectiva del producto o alimento afectado (Sección “Trazabilidad de alimentos - Ventajas”, párr. 1).

Boletín Oficial de la República Argentina

Como indica la BFA (s. f.), el Boletín Oficial publica diariamente en su web cuatro secciones en formato digital que contienen normas jurídicas y otros actos de naturaleza pública, relacionados con el poder legislativo, ejecutivo y judicial. Por medio de BFA ofrece una

garantía más sobre la integridad de la información, ya que cualquier ciudadano puede verificar que la información publicada no fue alterada luego de su publicación en el sitio oficial.

Cámara de Diputados

La implementación del voto electrónico de diputados utiliza el servicio de la BFA cuando se emite el voto, momento en el que “el sistema genera un archivo en formato PDF que está vinculado a un "Hash", código que queda registrado en la red BFA y no permite la edición ni la manipulación de ese archivo” (BFA, sección “Aplicaciones”, s. f.).

NIC Argentina

NIC posee una sección donde se publican a diario las altas y transferencias de Dominios de Internet Argentinos en formato CSV. Según la propia web de NIC (s. f.) “dichos documentos son certificados por el Sello de Tiempo de Blockchain Federal Argentina que brinda una fecha cierta y la garantía de que no han sido modificados luego de su publicación”.

Inspección General de la Justicia

Toda sociedad por Acciones Simplificadas tiene la obligatoriedad de presentar sus libros en formato digital ante la AFIP. “Con BFA se garantiza la inmutabilidad de los PDF sin necesidad de tener la información publicada en la Red” (BFA, sección “Aplicaciones”, s. f.).

Gobierno de la Ciudad de Buenos Aires

El Gobierno lanzó una solución llamada Carpeta Ciudadana dentro de la aplicación MiBA que funciona como un “repositorio de documentos digitales del vecino que sean emitidos por el Gobierno de CABA u otra Entidad afín, como ser certificados de capacitaciones, títulos secundarios, partidas de nacimiento, actas de matrimonio entre otros” (BFA, sección “Aplicaciones”, s. f.). La integridad de estos certificados es resguardada y verificada gracias a la integración con la BFA.

2.3.8 Resumen

En resumen, y bajo lo expuesto en este capítulo se entiende que, 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.

Permite garantizar en cada transacción la identidad de las partes involucradas, ya que todas las transacciones son firmadas criptográficamente, certificar de la fecha y hora de la transacción, y que la información es inmutable e inalterable, es decir, no es posible modificarla ni borrarla. Además, toda la información almacenada en la cadena es completamente auditable, se incorpora de forma pública y visible para todos los usuarios, y como Blockchain funciona sin intermediarios, no hace falta una persona, empresa o institución que legitime la información guardada en la cadena, ya que es segura por naturaleza.

Capítulo 3

3.1 Propuesta de Intervención

3.1.1 Introducción

En este capítulo presentaremos la propuesta a desarrollar para dar una solución a la problemática planteada en el Capítulo I. Esta solución utilizará la red creada por la Blockchain Federal Argentina, haciendo uso del servicio de “Sello de Tiempo” ofrecido por la BFA.

3.1.2 Estrategias y Recursos

Teniendo como base los conceptos y conocimientos plasmados en el capítulo anterior, la principal estrategia sobre la cual se abordará la solución a la problemática planteada radica en el uso de la Blockchain Federal Argentina como red que dará soporte a la solución que plantearemos en el presente capítulo. La idea radica en utilizar el servicio de Sello de Tiempo para generar un hash sobre los documentos que las entidades necesiten entregar a distintos entes reguladores y otras partes interesadas.

Al generar este sello único, cualquier interesado en el archivo podría verificar la originalidad e inmutabilidad de este simplemente utilizando el servicio de BFA que permite generar el hash en base a un archivo. Si los hashes coinciden, el interesado comprobará que el archivo no fue modificado. Como mencionamos anteriormente en el apartado de Criptografía, el más mínimo cambio en el archivo, su contenido o hasta su nombre, provocaría que el hash generado por el TSA (Time Stamping Authority) cambie.

Pero para utilizar este recurso, primero es necesario conocer a detalle qué es y cómo funciona la Blockchain Federal Argentina. La BFA, como bien indica Franca (2019), representa una innovadora plataforma multiservicios diseñada para integrar y potenciar aplicaciones sobre la tecnología blockchain. Esta iniciativa emerge como un espacio abierto y participativo que no solo busca optimizar procesos administrativos y operativos, sino también actuar como catalizador de empoderamiento para la comunidad en su conjunto. Su infraestructura es confiable y completamente auditable, lo que significa que todas las transacciones y cambios dentro de la plataforma están abiertos a ser revisados por cualquier interesado, garantizando así la transparencia total. Esto es vital para el fortalecimiento de la

confianza entre los usuarios y para promover una adopción más amplia de esta tecnología (pp. 22-23).

Desde su concepción, como bien indica Franca (2019), la BFA fue diseñada para funcionar como un entorno de colaboración colectiva, fomentando la participación de diversas partes interesadas. Su estructura invita a la contribución de representantes de los sectores público y privado, académicos y de la sociedad civil. Este enfoque colaborativo no solo enriquece la plataforma con diversas perspectivas y expertises, sino que también refuerza la idea de que la mejora continua y la innovación son responsabilidades compartidas (p. 22).

Siguiendo el modelo de Múltiples Partes Interesadas, la gobernanza de BFA está diseñada para asegurar que todas las voces sean escuchadas en el proceso de toma de decisiones. Esto es crucial para asegurar que la plataforma no solo sirva los intereses de un grupo específico, sino que sea beneficiosa para todos los usuarios potenciales, incluyendo individuos, instituciones, empresas y organismos públicos. Además, al ser una plataforma pública, BFA está abierta a todos aquellos que deseen contribuir o desarrollar aplicaciones, marcando un hito en el desarrollo tecnológico participativo del país (Franca, 2019, p. 23).

La BFA invita a cualquier interesado en explorar o implementar soluciones basadas en blockchain a participar en la plataforma. Esta política de puertas abiertas no solo amplifica las posibilidades de innovación, sino que también democratiza el acceso a tecnologías de punta. Al facilitar una base donde cualquiera, independientemente de su tamaño o sector, puede desarrollar aplicaciones, BFA potencia el ecosistema de innovación nacional y posiciona a Argentina en la vanguardia de la tecnología blockchain. El diseño técnico y organizativo de la BFA asegura que la plataforma no solo sea escalable, incorporando a nuevos participantes de forma fluida, sino también sostenible a lo largo del tiempo. El enfoque horizontal y colaborativo permite que la plataforma evolucione y se adapte a medida que cambian las necesidades y emergen nuevas tecnologías, garantizando su relevancia y utilidad futura (Franca, 2019, p. 23).

3.1.3 *Funcionamiento del Modelo*

De acuerdo con la descripción dada por Franca (2019), la BFA funciona como 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” (p. 22).

Como toda Blockchain sería lógico esperar algún tipo de criptomoneda asociada, pero este no es el caso, ya que según Franca (2019), la motivación fundamental para formar parte de la Blockchain Federal Argentina trasciende los objetivos financieros inmediatos y se orienta hacia el fomento de un ecosistema colaborativo, enfocado en la innovación tecnológica. Al no depender de una moneda virtual, la BFA se aparta del esquema competitivo que caracteriza a otras iniciativas blockchain, concentrándose en lugar de ello en potenciar el desarrollo de servicios y proyectos que aprovechan las capacidades de esta tecnología para la mejora colectiva. Esto establece un precedente importante para cómo la tecnología blockchain puede ser utilizada con fines más amplios que la mera especulación financiera, subrayando el valor de la cooperación y la innovación como pilares para el avance tecnológico y el beneficio común (p. 22).

Además, la implementación de la BFA mediante un protocolo de Prueba de Autoridad marca una innovación significativa en la gestión de redes blockchain, especialmente en términos de eficiencia operativa y sostenibilidad ambiental. En concordancia con Franca (2019), al eliminar la necesidad de resolver algoritmos complejos para el minado de criptomonedas, esta aproximación permite a la BFA facilitar un mayor volumen de transacciones en menos tiempo y con un consumo eléctrico notablemente menor. Este enfoque no solo posiciona a la BFA como una alternativa más eco-amigable en comparación con las blockchain que operan bajo el esquema de Prueba de Trabajo, sino que también subraya el potencial de los mecanismos de consenso innovadores para mejorar la eficiencia y reducir el impacto ambiental de las tecnologías de contabilidad distribuida (p. 14).

Al funcionamiento de la Blockchain explicado, debemos sumar el servicio de TSA llamado “Sello de tiempo”. Como bien mencionamos anteriormente en la sección “Estrategias y Recursos”, este servicio será vital para el proyecto ya que permite generar un digesto

criptográfico único para cada archivo procesado por el TSA, lo cual implica poder verificar que un archivo no fue modificado desde la fecha que pasó por el Sello de Tiempo.

Para aclarar el funcionamiento de la solución, pongamos de ejemplo un requisito habitual del BCRA a entidades financieras, el Anexo B. Este Anexo es un complemento a los Estados Financieros que presentan los bancos, por ejemplo, que contempla la clasificación de préstamos y otras financiaciones por situación y garantías recibidas, “incluyendo el total de las financiaciones comprendidas (capitales, intereses devengados a cobrar, diferencias de cotización y ajustes) en las normas sobre “clasificación de deudores”, (...) consignando las garantías que las respaldan” (Com. A 7423 BCRA, 2022, p. 2). La información de este anexo no sólo es de interés para el Banco Central, sino también para Auditores y Accionistas del banco en cuestión, y dado que está compuesto por una gran cantidad de datos, es un ejemplo ideal para este proyecto.

Normalmente los bancos presentan el Anexo B al BCRA junto con algún tipo de evidencia que valide cómo se generó la información entregada y que la misma no fue alterada. Posteriormente, el auditor externo solicita la misma información, y llegado el momento de presentaciones a comité o directorio, se debe volver a presentar la información. Todo esto conlleva repetir el mismo proceso de validación de datos en diversas instancias, lo cual consume recursos y genera pérdidas de tiempo. Aquí es donde aplicamos la solución planteada con BFA y el TSA. Si se procesaran los archivos entregados al Banco Central en primera instancia con el servicio de Sellado de Tiempo que ofrece BFA, tendríamos un hash único que identifica al archivo y que contiene una marca de tiempo, con el cual tanto el BCRA, el auditor, y cualquier otra parte interesada podría utilizar para, al volver a procesar el archivo entregado, comparar los hashes y verificar su originalidad. De este modo se evita el proceso de certificación de que los datos no fueron modificados desde su generación. Además, como la BFA no almacena la información de los archivos procesados con el TSA, sino que sólo almacena el hash generado, no se estaría poniendo en riesgo ningún tipo de filtración o divulgación de información confidencial.

Volviendo sobre el funcionamiento de la BFA, más específicamente del Sello de Tiempo, Franca (2019) indica que existen distintas formas de utilizar el servicio de TSA, según las necesidades de cada usuario. Una GUI está disponible en bfa.ar/sello, la cual permite sellar documentos sin ningún tipo de conocimiento sobre Blockchain o programación. También se

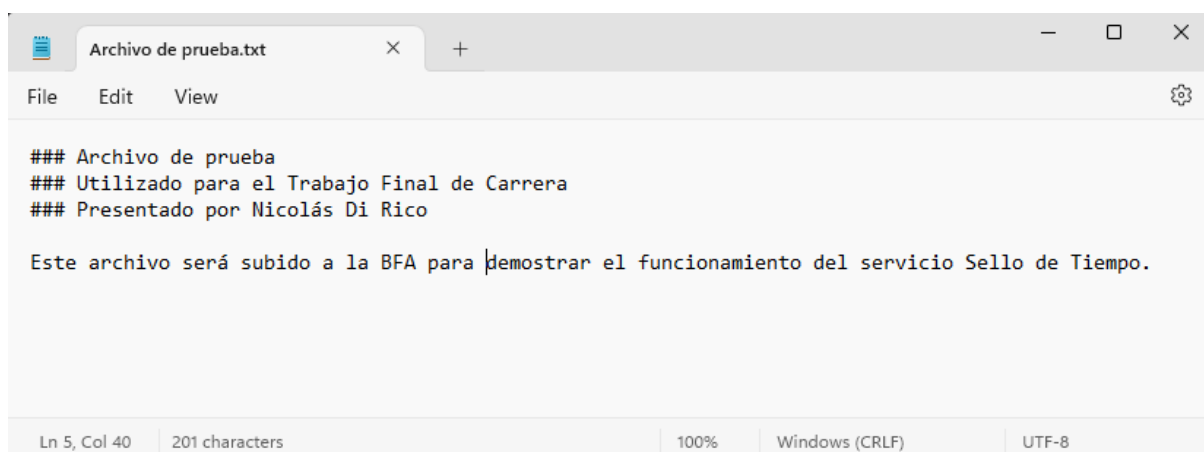
encuentra disponible una API REST para facilitar desarrollos que quieran conectarse con este servicio. Y, por último, de fondo se encuentra funcionando el Smart Contract que posibilita todo esto.

En este sentido, Franca (2019) comenta que “Si alguien desea desarrollar un nuevo smart contract y volcarlo en la blockchain, puede hacerlo perfectamente.” (p. 37), lo cual concuerda con lo anteriormente mencionado “el software de BFA se basa en una implementación abierta y robusta. Todos los desarrollos y modificaciones que se realicen (...) podrán ser públicamente auditados por cualquier interesado, más allá de la organización” (Franca, 2019, p. 29). De modo que queda garantizado desde el código la transparencia inherente en el modelo.

A continuación, ejemplificaremos el funcionamiento del modelo planteado con un caso práctico. Cabe destacar que la explicación del funcionamiento técnico del servicio TSA se encuentra plasmada en el Anexo III. Para esta ejemplificación, tomaremos como ejemplo un archivo de texto (.txt) con los datos observados en la Figura 11.

Figura 11

Archivo de texto de prueba

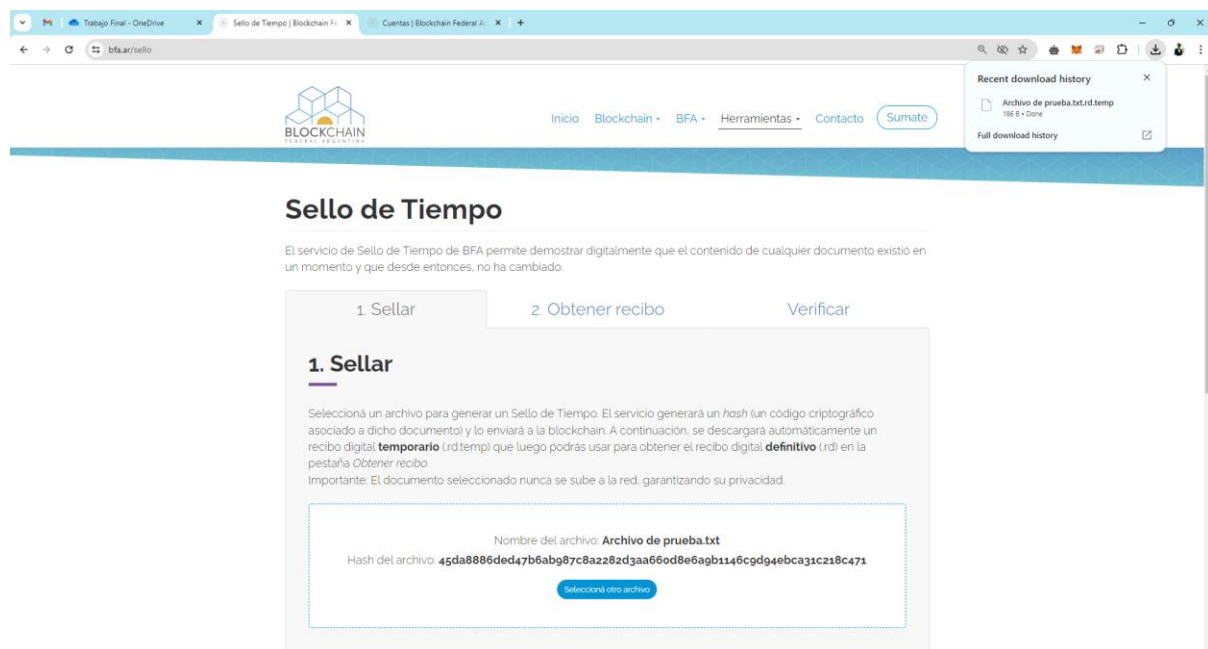


Ya en la web de la BFA, nos dirigimos al servicio de Sello de Tiempo, y utilizamos la función “Sellar”. Al subir el archivo de prueba se genera el hash de este, en este caso es `45da8886ded47b6abg87c8a2282d3aa660d8e6agb1146cgd94ebca31C218C471`, tal como se

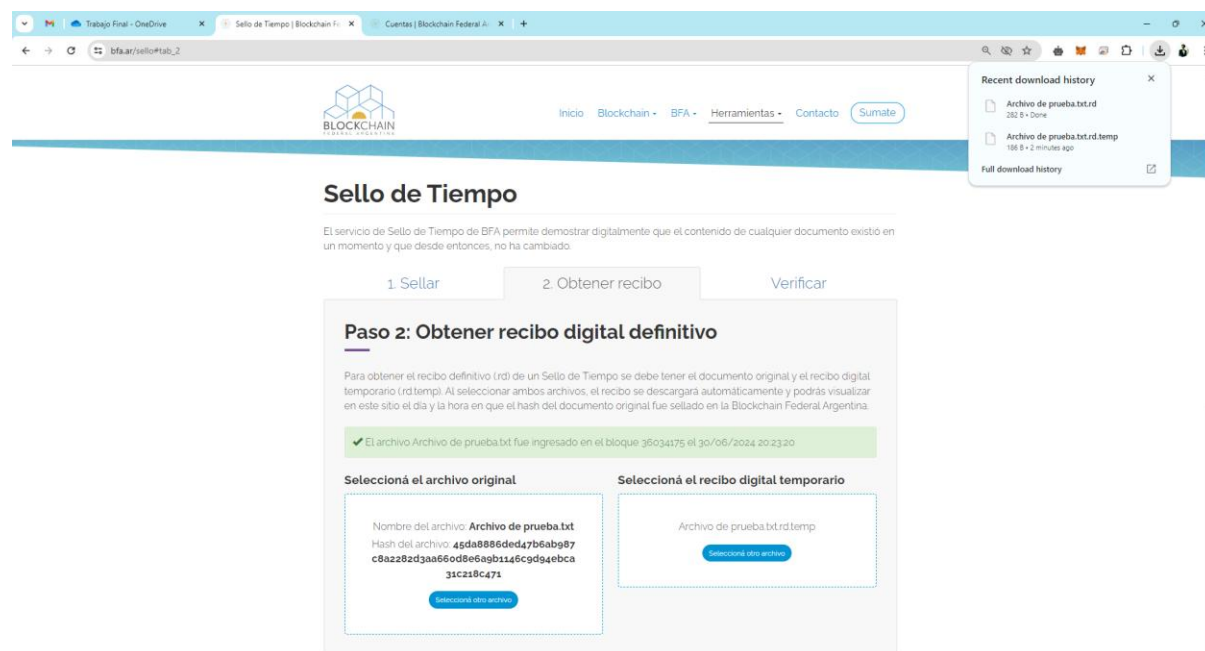
observa en la Figura 12 y se descarga automáticamente el certificado temporal, archivo con extensión `rd.temp`, que utilizaremos más adelante.

Figura 12

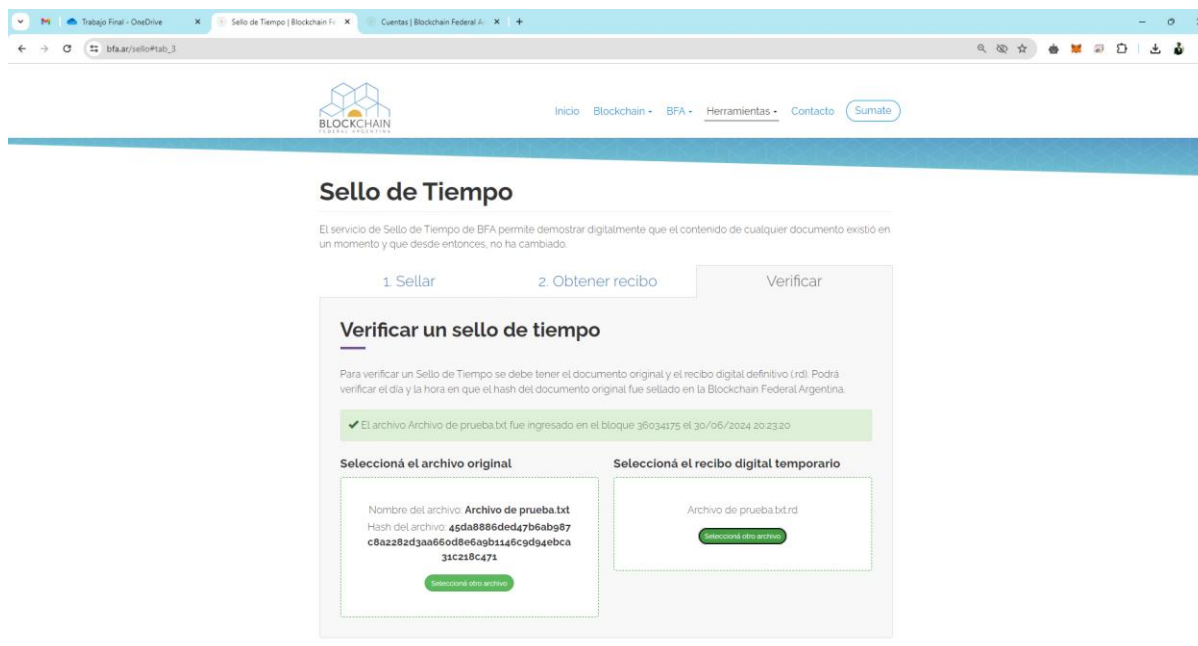
Función Sellar de la TSA de la BFA



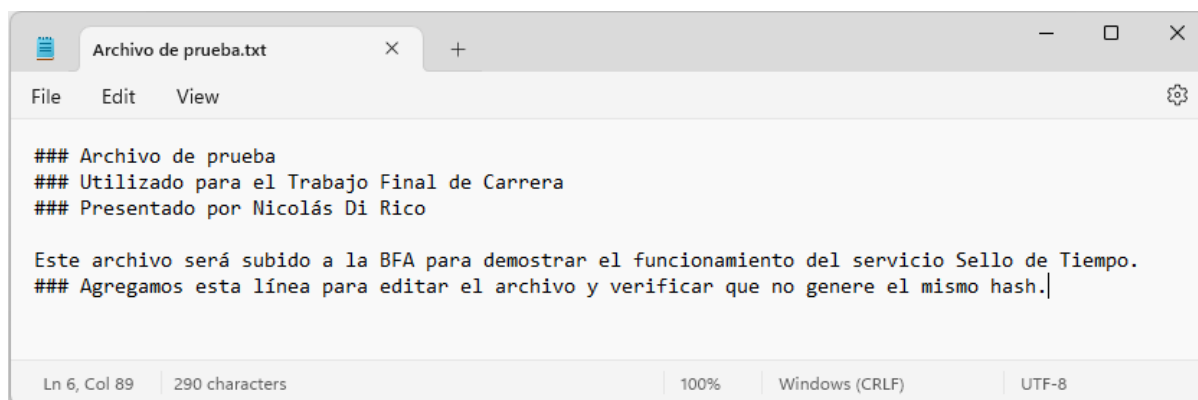
En el siguiente paso, dentro de la sección “Obtener Recibo”, debemos subir el archivo original y el certificado temporal generado. Si para el momento en el que realizamos esta acción la transacción que añade nuestro hash a la cadena de bloques de la BFA ya finalizó, entonces recibiremos el mensaje que se observa en la Figura 13, y se descargará automáticamente el comprobante definitivo. Este es sumamente importante conservarlo para poder validar la originalidad del archivo posteriormente.

Figura 13*Función Obtener Recibo de la TSA de la BFA*

Ahora, ya con el comprobante definitivo, podemos comprobar su originalidad en la sección “Verificar”. Aquí debemos subir nuevamente el archivo original y el comprobante definitivo. Podremos observar en la Figura 14 que el servicio muestra el mismo hash que al principio, y nos indica por medio de un mensaje el número de bloque y fecha en el que fue añadido a la cadena.

Figura 14*Función Verificar de la TSA de la BFA*

Por último, demostraremos que el servicio reconoce cuando un archivo no se corresponde con el comprobante definitivo. Para ello, modificamos el archivo de texto original, como se puede ver en la Figura 15.

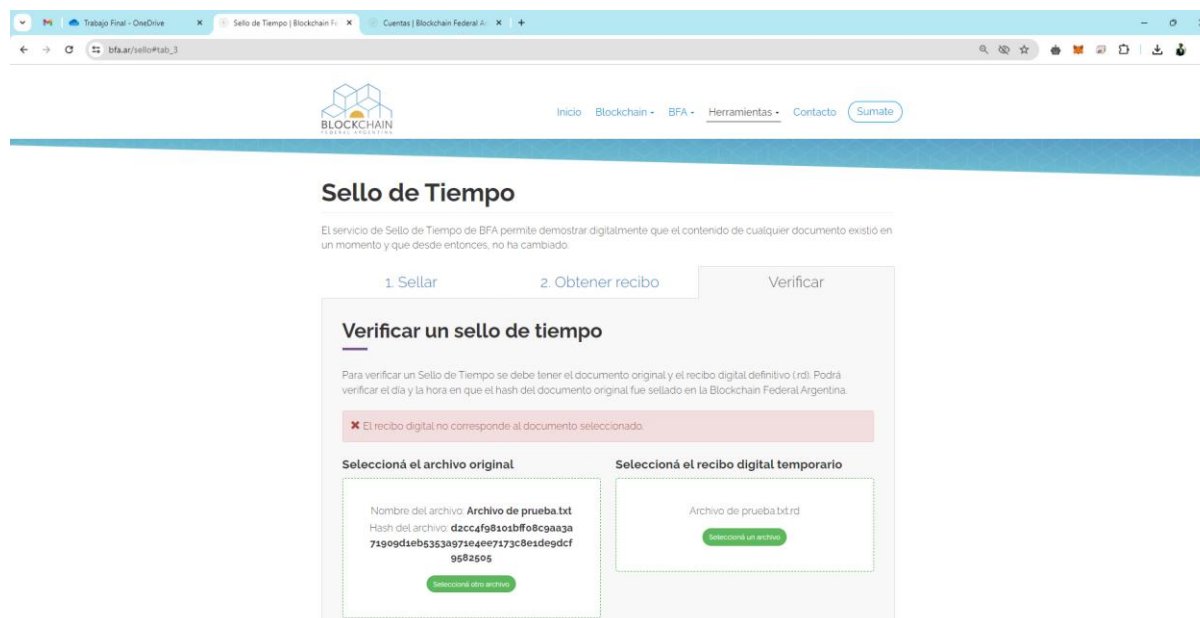
Figura 15*Archivo de prueba modificado*

Al subirlo en la sección “Verificar”, junto con el comprobante definitivo original, vemos que el Sello de Tiempo indica que no hay correspondencia entre el archivo subido y el

comprobante. Esto sucede porque el archivo de texto modificado genera el siguiente hash `d2cc4f98101bffa08cga371909d1eb5353a9714007173C8e1degdcf9582505`, distinto al que observamos en las Figuras anteriores.

Figura 16

Error en la función Verificar de la TSA de la BFA



3.1.4 Infraestructura

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. En este sentido, la BFA se encargará de la infraestructura mientras que los usuarios desarrollarán las aplicaciones.

De acuerdo con Franca (2019), la red está integrada por distintos tipos de nodos tal como se observan en la figura 17:

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 del consorcio. Los selladores están conectados solamente

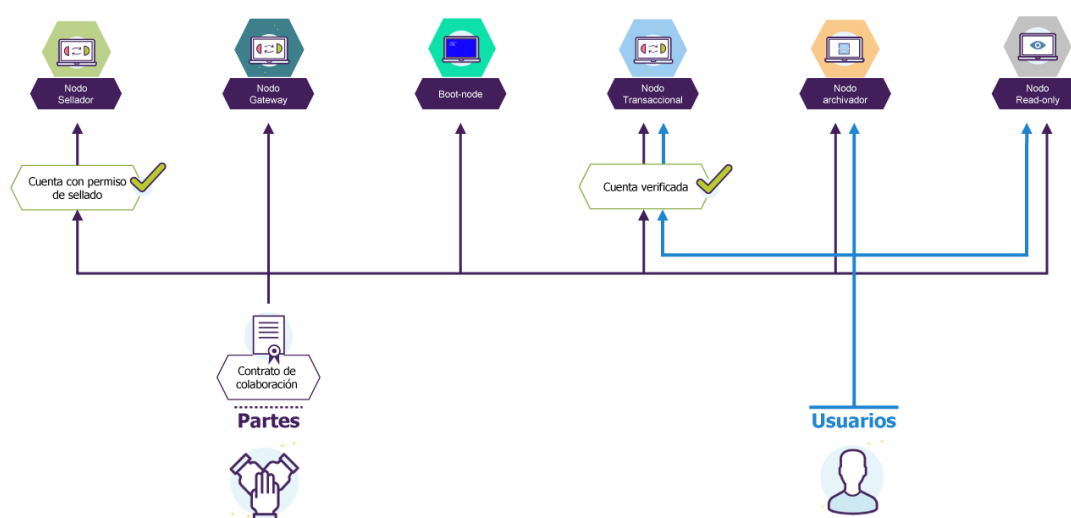
entre sí, y a los nodos tipo Gateway, que actúan como buffer entre ellos y el resto de la red.

Los nodos transaccionales 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. 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. 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 ni contar con autorización de BFA. También podrían servir para acceder a la información por parte de una aplicación o servicio. (p. 32)

Figura 17

Participantes por tipo de nodo.



Nota. Tomado de Infraestructura, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/bfa/infraestructura>)

Actualmente existen 23 nodos selladores funcionando, entre ellos los correspondientes a las organizaciones listadas en la Figura 18

Figura 18

Organizaciones con nodos selladores



Nota. Tomado del Brief BFA (p. 33), por la Blockchain Federal Argentina (2019).

El proceso asociado a la creación de un nodo, de cualquier tipo que sea, se encuentra plasmado en el Anexo I, en este apartado nos limitaremos a comentar los requerimientos técnicos presentados en la Tabla 3.

Tabla 3

Requerimientos técnicos mínimos para la instalación de un nodo.

Especificaciones	Sellador	Gateway	Bootnode	Testnet
Tipo Maquina	Virtual/Dedicada	Virtual/Dedicada	Virtual/Dedicada	Virtual
CPU	2	2	2	1-2
RAM	6 GB	4 GB	4 GB	2 GB
Disk Space	1 TB	300 GB	300 GB	40 Gbps
Placa de Red	100 Mbps	1 Gbps	1 Gbps	100 Mbps

SO	Debian/Ubuntu Server	Debian/Ubuntu Server	Debian/Ubuntu Server	Debian/Ubu ntu Server
IPv4/IPv6	fija, pública, sin NAT	fija, pública, sin NAT	fija, pública, sin NAT	fija, pública

Nota. Los nodos selladores deben tener los puertos tcp abiertos a y desde los selladores a todos los gateways, y los udp a y desde el mundo.

3.1.5 *Tecnología Utilizada*

Continuando con las afirmaciones de Franca (2019), BFA utiliza la tecnología de Ethereum, una de las blockchains públicas más conocidas a nivel internacional. Ethereum ofrece una plataforma descentralizada operando mediante Prueba de Trabajo (PoW), y habilita a los desarrolladores para crear y desplegar aplicaciones distribuidas que ejecutan contratos inteligentes apoyados en la cadena de bloques, con una infraestructura de nodos distribuida globalmente. Dado que BFA es de código abierto, permite que la comunidad participe en las pruebas de concepto para optimizar la plataforma o adaptar el trabajo a diferentes contextos y necesidades. Específicamente, la Blockchain Federal Argentina adapta este software al emplear Prueba de Autoridad (PoA) y no incorpora una criptomoneda propia (p. 31).

Respecto al monitoreo de la red, la responsabilidad del mantenimiento y la vigilancia de cada nodo de la BFA recae sobre las entidades que los operan, no existiendo una instancia central que maneje dichas operaciones en la red. Para respaldar esta estructura, la Blockchain Federal Argentina implementó un plan de monitoreo por medio del NOC (Centro de Operaciones de Red), dedicado a mantener el buen funcionamiento de los nodos selladores y de pasarela. Este centro no operará desde una única ubicación, sino que está repartido de manera geográfica y entre distintas áreas de la organización (Franca, 2019, p. 35)

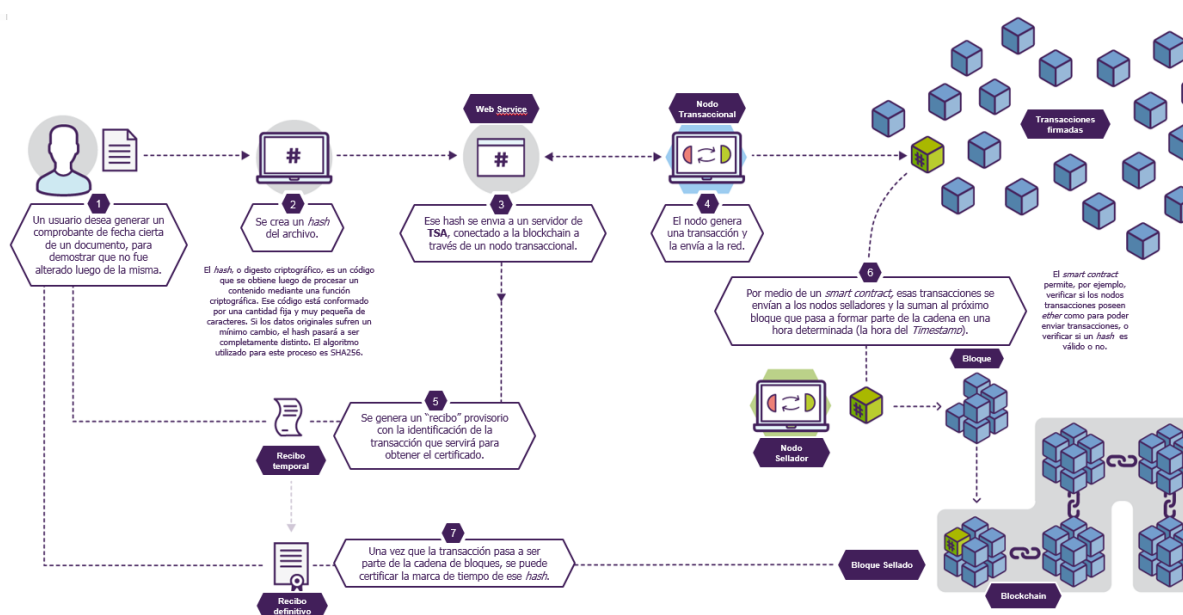
En cuanto a los usos de esta tecnología, la blockchain puede utilizarse para autenticar distintos tipos de contenidos. Dentro de sus capacidades, Franca (2019) destaca la creación de una “prueba de existencia”, similar a un sello digital que confirma la presencia previa de un mensaje a una fecha y hora específicas. La BFA ofrece un servicio de TSA (Time Stamping Authority) que certifica que cierto archivo digital no ha sido alterado después de una fecha determinada (p. 36). Este será el servicio que utilizaremos para certificar los documentos que

las entidades financieras deban presentar a los entes reguladores. De este modo, la información no tendrá que ser validada cada vez que se quiera presentar a una nueva parte interesada, sino que será directamente el interesado quien corrobore la autenticidad de la documentación por medio del servicio de la BFA.

El funcionamiento de este Sello de Tiempo, ilustrado en la Figura 19, comienza con un request de un usuario que desea generar un comprobante de fecha cierta de un documento, para demostrar que no fue alterado luego de la misma. Al procesarlo con el servicio de la BFA, se genera un hash del archivo, que es enviado a un servidor de TSA, conectado a la blockchain a través de un nodo transaccional. En este momento se genera un recibo temporal para el usuario, al mismo tiempo que el nodo transaccional está generando una transacción y enviándola a la red. Por medio de un Smart Contract la transacción pasará a un nodo sellador y se sumará al próximo bloque que formará parte de la cadena con un horario determinado (el timestamp que tendrá el hash). Finalmente, cuando el bloque es sellado a la cadena, se completa el contrato y se certifica la marca de tiempo del hash inicial, lo cual queda plasmado en el recibo definitivo que recibe el usuario.

Figura 19

Sello de tiempo.



Nota. El gráfico representa el sello de tiempo que se le aplica a los documentos. Tomado de Tecnología, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/bfa/tecnologia>)

A continuación, se presentan las especificaciones técnicas del funcionamiento de la TSA de la BFA en sus distintas presentaciones, tanto como Smart contract, API REST y en su versión interfaz web para usuarios finales, de acuerdo con el manual provisto por la BFA en su repositorio de Github. Para comenzar, como se indicó en el Capítulo 3, el servicio de TSA funciona gracias a smart contracts que corren en la blockchain. En el caso de la BFA, se trata de dos contratos inteligentes, uno llamado Stamp y otro llamado Verify.

Stamp es un smart contract que debe recibir una lista de digesto criptográfico e insertarla en la blockchain como una transacción, es decir, es el contrato encargado de tomar el hash del archivo que el usuario haya subido e iniciar el proceso de sellado en la cadena de bloques (Especificación de TSA, s. f., p. 1).

Verify es el smart contract que debe recibir un hash e informar en qué bloque apareció por la primera vez. El resultado “bloque cero” significa que ese hash todavía no ha sido guardado en la blockchain (Especificación de TSA, s. f., p. 1).

Los comprobantes y certificados son generados por las interfaces en formato texto de Unix. La extensión sugerida es “.tsabfa”. Una línea no puede tener más que 2000 caracteres UTF8 (según las normas EBNF) y el archivo no más de 1000 líneas. Cada comprobante incluye el hash, una identificación del algoritmo que se utilizó para generar el hash y la dirección del contrato de procedencia de la validación. Los certificados contienen lo mismo que los comprobantes, sumado a el número de bloque en la blockchain donde quedó insertado el hash y el timestamp del bloque correspondiente (Especificación de TSA, s. f., pp. 1-2).

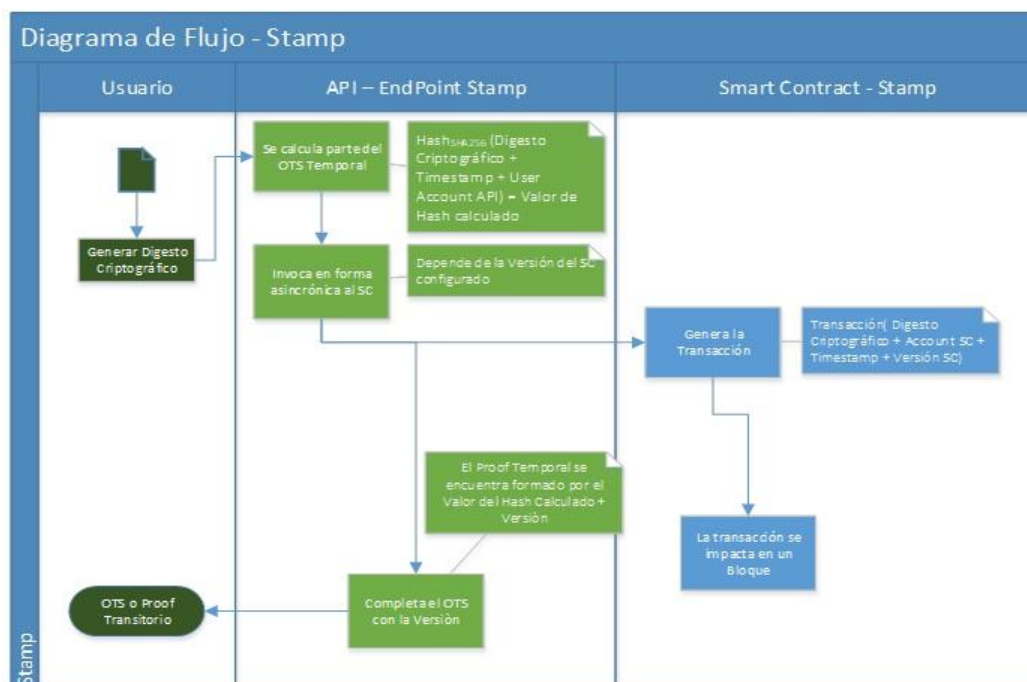
Por otro lado, también se dispone de la API REST, la cual cuenta con tres endpoints, Stamp, Certify y Verify, aunque realmente los últimos dos comparten algunas funciones, como veremos a continuación.

Stamp es el endpoint que recibe un hash y, si todavía no existe, lo envía a insertar en la blockchain. Es configurable para permitir acumular una serie de hashes e insertarlos como una única transacción. Además, permite configurar un límite (*threshold*) para hacer el *flush* de todos los hashes pendientes hacia la blockchain, tanto en base al tiempo transcurrido desde que se recibió el primero como en base a la cantidad de hashes recibidos. Al finalizar su operación, el

Stamp devuelve un recibo temporario de la transacción, demostrando la intención de incorporar el hash a la blockchain (Especificación de TSA, s. f., p. 2).

Figura 20

Diagrama de flujo de Stamp

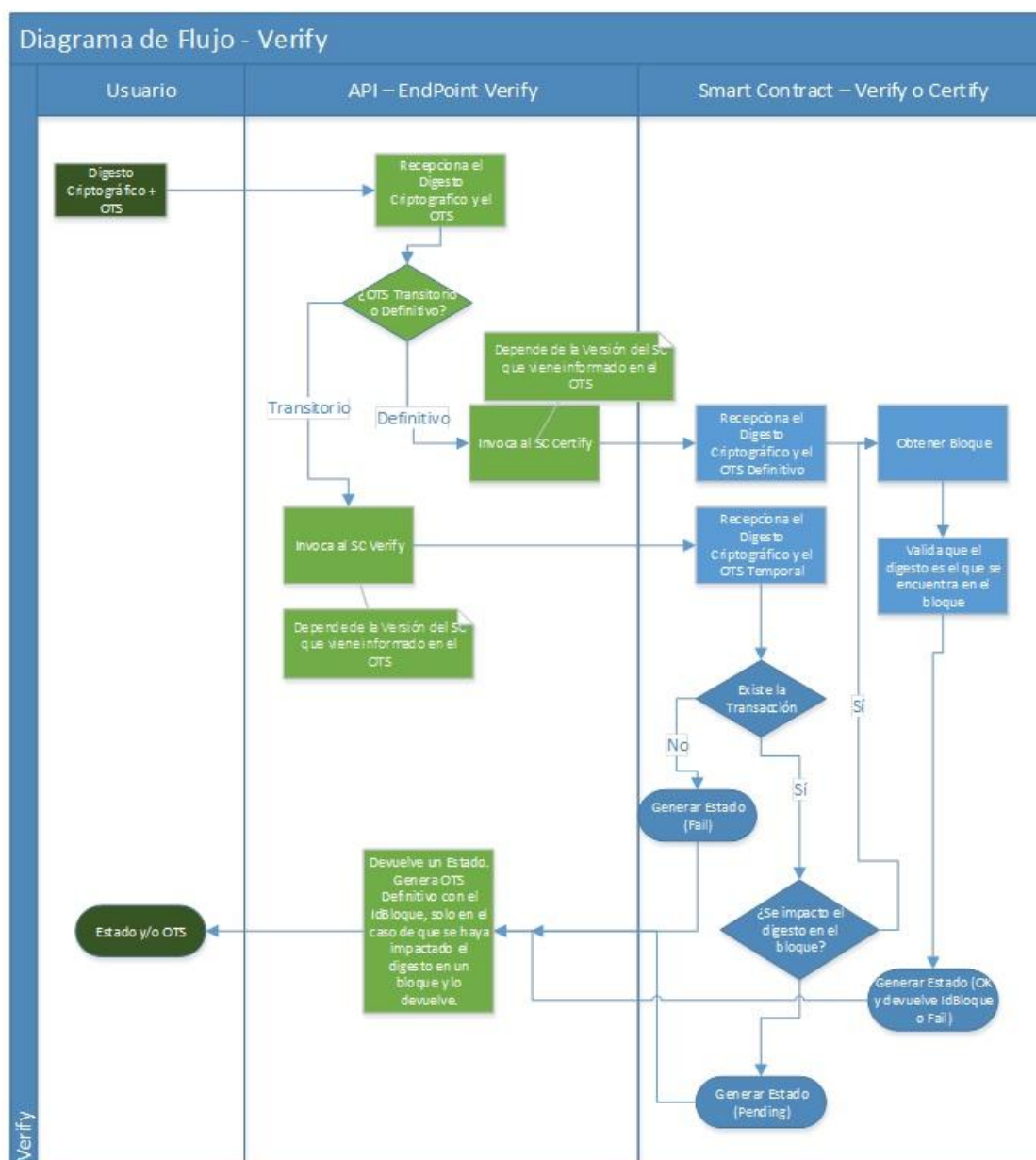


Nota. Tomado del repositorio de Github de la BFA (s. f.).

(<https://docs.google.com/document/d/19PYSiAkInGXLEbSDqWQh-1zSrY4rr20Palr1H8MjaEQ>)

Certify es el endpoint que recibe un hash previamente enviado a la blockchain y obtiene el comprobante digital (el .ots o equivalente). Los resultados posibles son Pending (pendiente), si todavía no fue insertado en la blockchain, Unknown (desconocido), si no fue recibido previamente para insertar, u OK, caso en el cual es acompañado del certificado (Especificación de TSA, s. f., p. 3).

Verify es el endpoint que recibe un comprobante digital (el .ots o equivalente) y verifica que es válido, es decir, que el hash contenido en el comprobante está efectivamente en el bloque indicado en el comprobante (Especificación de TSA, s. f., p. 3).

Figura 21*Diagrama de flujo de Verify - Certify*

Nota. Tomado del repositorio de Github de la BFA (s. f.).

(<https://docs.google.com/document/d/19PYSiAkInGXLEbSDqWQh-1zSrY4rr20Palr1H8MjaEQ>)

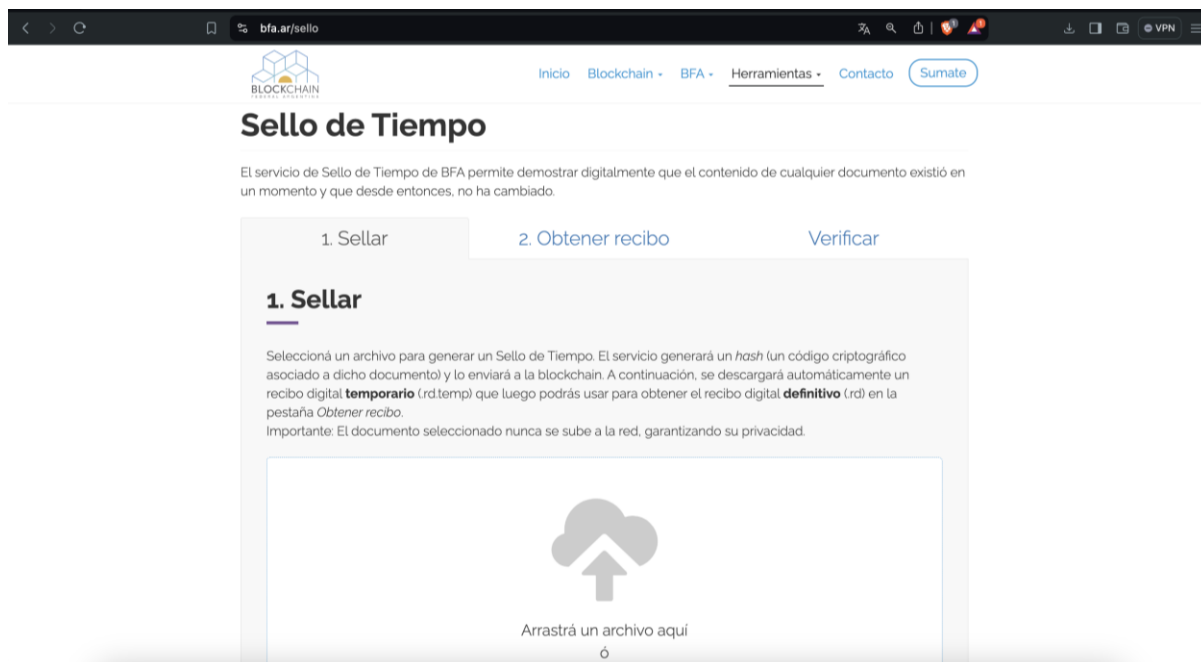
La interfaz web para usuarios finales, a la cual se accede desde <https://bfa.ar/sello>, enmascara la API y brinda las siguientes funcionalidades.

Insertar Hash. Esta función permite cargar un hash y lo envía a insertar en la blockchain. Tiene una opción inmediata, asíncrona, que devuelve el control en cuanto la API

procesó el Stamp, y una sincrónica, que espera a que la API obtenga el comprobante vía Certify y se lo devuelve al usuario (Especificación de TSA, s. f., p. 3).

Figura 22

Función Sellar del TSA



Nota. Captura de pantalla de la interfaz web que permite subir un archivo para generar el hash y enviarlo a la Blockchain. (https://bfa.ar/sello#tab_1/)

Obtener comprobante. Permite cargar un hash previamente enviado y obtiene el comprobante digital (el .ots o equivalente). Invoca directamente el Certify de la API y, si ya está insertado en la blockchain, devuelve el comprobante digital (.ots o equivalente), en caso contrario, indica si todavía está pendiente de inserción (permitiendo volver a invocarlo con solo apretar un botón) o si el hash es desconocido porque no había sido enviado previamente (Especificación de TSA, s. f., p. 3).

Figura 23*Función Obtener Recibo del TSA*

Nota. Captura de pantalla de la interfaz web que permite obtener el comprobante definitivo. (https://bfa.ar/sello#tab_2/)

Verificar hash. Permite subir un comprobante digital (el .ots o equivalente) y verifica que es válido, es decir, que el hash contenido en el comprobante está efectivamente en el bloque indicado en el comprobante (Especificación de TSA, s. f., p. 3).

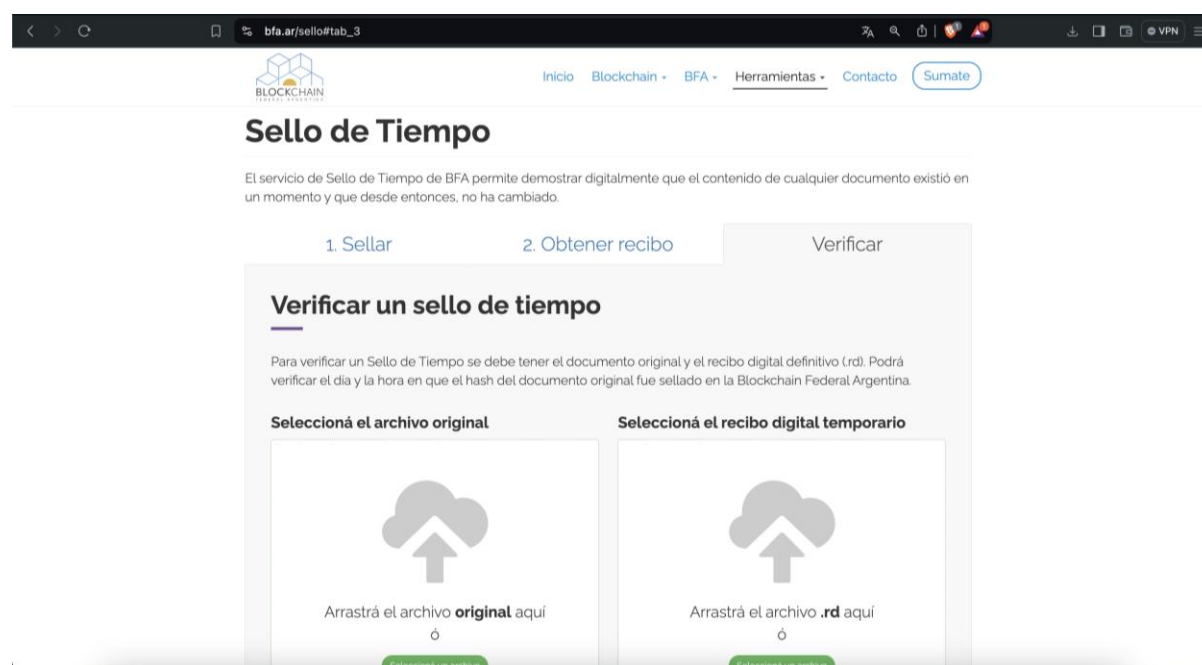
Figura 24*Función Verificar Hash del TSA*

Nota. Captura de pantalla de la interfaz web que permite verificar un hash. (<https://bfa.ar/sello2#/>)

Verificar documento. Permite subir un documento y un comprobante digital (el .ots o equivalente) y realiza dos tareas, genera el hash del documento utilizando el algoritmo de hash indicado en el comprobante digital. Esto lo hace vía javascript sin ofuscar, enteramente en el browser; el documento no se transmite nunca. Si el hash es igual al del comprobante, sigue adelante, si el hash no coincide con el del comprobante, informa que el comprobante no corresponde al documento o el documento ha sido modificado y se detiene. En la segunda tarea, si el hash era correcto, procede a verificar el comprobante digital, es decir, que el hash está efectivamente en el bloque indicado en el comprobante. Si el hash se encuentra en ese bloque informa que el documento corresponde al comprobante y que fue insertado en la blockchain tal cual indica el comprobante. Informa también fecha y hora del bloque. Si el hash no se encuentra en ese bloque, informa que el comprobante digital es inválido en la blockchain (Especificación de TSA, s. f., p. 4).

Figura 25

Función Verificar Documento del TSA



Nota. Captura de pantalla de la interfaz web que permite verificar el sello de tiempo de un documento. (https://bfa.ar/sello#tab_3/)

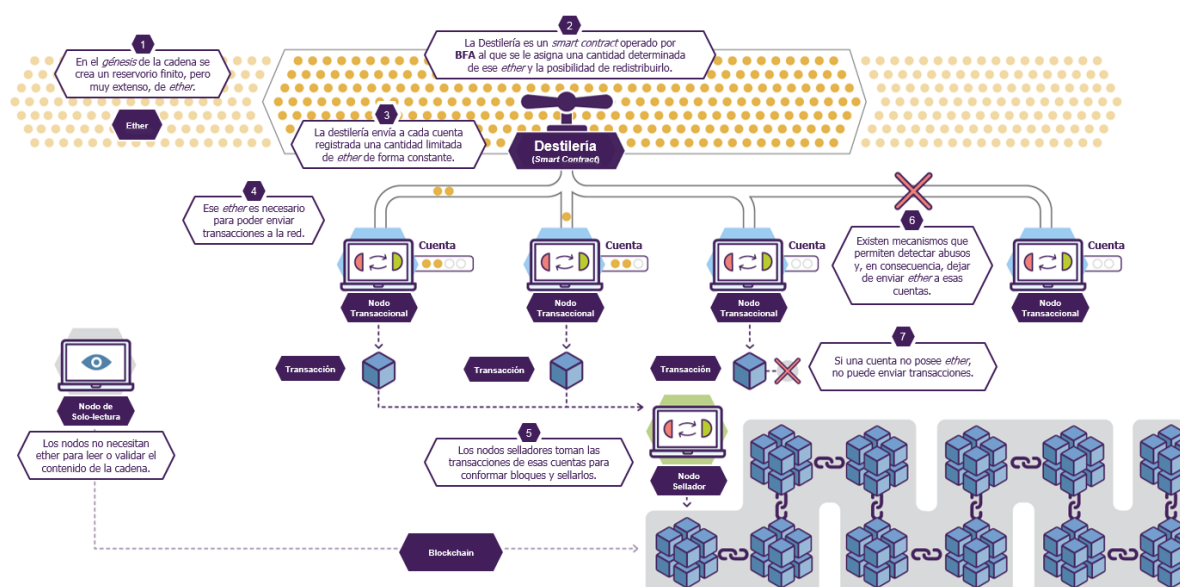
Cabe destacar que, como en cualquier blockchain basada en Ethereum, para enviar transacciones a la cadena de bloques se necesita un “combustible” o “gas” llamado Ether. En

este caso particular, “la BFA distribuye [el Ether] a aquellos operadores registrados de nodos transaccionales que desplieguen aplicaciones sobre la plataforma” (Franca, 2019, p. 34).

De acuerdo con Franca (2019), dentro del ecosistema de la BFA, el Ether no tiene ningún tipo de valor económico, además de que es distribuido a diario mediante un espacio operado por la organización llamado Destilería (p. 34), tal como se observa en la figura 20. Así, se evita la especulación y/o tráfico de gas, ya que “no hay ninguna necesidad de comprar o vender Ether, ya que se distribuye a todos los usuarios sin costo alguno. Además, la Destilería posibilita métodos para detectar abusos y proteger la red” (Franca, 2019, p. 34). Cabe destacar que cualquier nodo de solo lectura puede verificar la fidelidad de la información, por más que no posea Ether.

Figura 26

Destilería de Gas.



Nota. El gráfico representa la “destilería”, un sistema centralizado de distribución de ether utilizado por la BFA para el sellado de tiempo. Tomado de Tecnología, por la Blockchain Federal Argentina, 2019, BFA (<https://bfa.ar/bfa/tecnologia>)

3.1.6 Administración de la Red

La administración de una blockchain, en particular la gestionada por BFA, muestra un modelo inclusivo y multipartito diseñado para asegurar una operación transparente, eficiente y colaborativa. Este modelo de administración cobra relevancia al considerar que la tecnología blockchain se basa en sistemas distribuidos que requieren una gestión cuidadosa para mantener su integridad, seguridad y alineación con los intereses de numerosos stakeholders.

El CdA (Consejo de Administración) es el eje central de la administración de la BFA, “compuesto por cinco miembros titulares y cinco suplentes, cada uno representando sectores fundamentales: Industria y Comercio, Academia, Gobierno Nacional, Gobiernos Provinciales y CABA, y Sociedad Civil” (BFA, sección “Administración”, s. f., párr. 1). Esta estructura proporciona un balance articulado de perspectivas, asegurando que cada sector tenga una voz en la toma de decisiones crucial sobre la gestión y la dirección estratégica de la blockchain.

La selección de los miembros de este consejo se realiza durante la Reunión de Partes, un evento anual que convoca a todos los integrantes y stakeholders de la BFA, y que no solo sirve para la elección del CdA, sino también para revisar y, de ser necesario, modificar el Contrato de Colaboración que marca las pautas de funcionamiento y cooperación entre las partes. Además, este encuentro sirve como plataforma para evaluar el desarrollo y desempeño de la blockchain, debatir sobre estrategias futuras y realizar cambios estructurales o adoptar nuevas políticas a través del voto (BFA, sección “Administración”, s. f., párr. 2).

Aunque no posee facultades ejecutivas o legislativas directas, el comité técnico (CT) juega un papel crucial. Compuesto por expertos en tecnología blockchain y otros campos relevantes, asesora al CdA en cuestiones técnicas y estratégicas, asegurando que las decisiones tomadas estén bien informadas y sean técnicamente viables (BFA, sección “Administración”, s. f., párr. 3). Este comité actúa como un puente entre el desarrollo tecnológico y la aplicación práctica y estratégica de la blockchain.

Con el objetivo de mantener y supervisar la infraestructura de la blockchain, BFA establece al menos tres centros de control independientes (NOC distribuido), operados por organismos partes de BFA. Estos centros desempeñan funciones críticas en el monitoreo constante de la red, garantizando su operación sin interrupciones y la integridad de los datos compartidos (Franca, 2019, p.43). En el Anexo II presentaremos el proceso de monitoreo.

Según Franca (2019), se han establecido diversos grupos de trabajo para abordar áreas específicas como Tecnología, Casos de uso, Legal, Comunicación y Monitoreo. Estos grupos, abiertos a la participación de cualquier interesado, fomentan el debate y la colaboración. Actúan como incubadoras de ideas y soluciones, y su labor facilita la evolución constante de la BFA, adaptándose a nuevos retos y explorando oportunidades emergentes (p.43)

La estructura de gobernanza de BFA ilustra un compromiso con la inclusividad y la eficiencia, manteniendo la transparencia y el control efectivo sobre una tecnología que es por naturaleza descentralizada y distribuida. La colaboración y la representación equitativa de intereses diversos son fundamentales en este esquema, asegurando que la blockchain no solo sea tecnológicamente robusta, sino también socialmente beneficiosa y justa.

La gestión de accesos a la BFA está dividida en dos segmentos, el acceso para usuarios individuales, y el acceso para organizaciones. Para los usuarios persona, la solicitud de acceso es sencilla, ya que se autogestiona a través de la web de la BFA registrándose con un correo electrónico. Con ello obtiene acceso a desplegar sus propios servicios, desarrollar sus propias aplicaciones y generar transacciones sin costo. En cuanto a las organizaciones, su acceso requiere en principio realizar un primer contacto a través de la web. Luego se solicita a los representantes de la organización interesada que completen el formulario de solicitud de incorporación, y aceptar las Políticas de uso de la BFA, así como su Reglamento Interno. Una vez realizado todo esto, la organización deberá desplegar los nodos que requiera siguiendo los instructivos publicados en la wiki interna del Gitlab BFA.

3.1.7 *Impacto de la Intervención*

La estructura de gobernanza de BFA ilustra un compromiso con la inclusividad y la eficiencia, manteniendo la transparencia y el control efectivo sobre una tecnología que es por naturaleza descentralizada y distribuida. La colaboración y la representación equitativa de intereses diversos son fundamentales en este esquema, asegurando que la blockchain no solo sea tecnológicamente robusta, sino también socialmente beneficiosa y justa.

La Blockchain Federal Argentina es una iniciativa pionera que está diseñada para transformar el panorama tecnológico, económico y social del país. Al integrar a distintos sectores en una única plataforma blockchain, BFA no solo impulsa la innovación tecnológica,

sino que también crea una base para profundos efectos económicos y mejores prácticas en la colaboración entre terceras partes. A continuación, exploramos estos impactos en detalle:

3.1.7.1 Impacto Económico.

Gran parte del impacto recae en la mejora en eficiencia y reducción de costos, ya que la BFA permite la automatización de procesos que tradicionalmente requieren extensos recursos humanos y temporales. La digitalización de registros y la implementación de contratos inteligentes reducen significativamente los costos asociados con la administración y ejecución de procesos, desde transacciones comerciales hasta cumplimientos regulatorios.

Otro factor importante es la transparencia y reducción del fraude. La irrevocabilidad y la transparencia de la blockchain disminuyen considerablemente las posibilidades de corrupción y fraude, lo cual es especialmente importante en un contexto argentino, donde tales desafíos han sido persistentes en varios niveles de la administración y gestión.

Además, se genera una innovación en servicios financieros, ya que, con la implementación de la BFA, el sector financiero puede ofrecer nuevos productos y servicios como microcréditos gestionados de manera eficiente y segura, o sistemas de ahorro más accesibles y fiables, lo que podría mejorar la inclusión financiera.

3.1.7.2 Impacto Tecnológico.

En cuanto al impacto tecnológico, la BFA incentiva la modernización de la infraestructura tecnológica al requerir sistemas capaces de implementar y mantener soluciones blockchain. Este impulso puede acelerar la adopción de tecnologías avanzadas en varios sectores, no solo en IT. Además, ante la necesidad de profesionales cualificados en blockchain y tecnologías relacionadas, la BFA puede actuar como catalizador para la formación de expertos en estas áreas, potenciando el capital humano del país. Por otra parte, la implementación de BFA puede fomentar la investigación y el desarrollo en áreas de criptografía, seguridad informática y gestión de datos, entre otros, promoviendo un ecosistema de innovación y un entorno favorable para startups tecnológicas.

3.1.7.3 Impacto en Terceras Partes.

La BFA fomenta la cooperación intersectorial, permitiendo que entidades públicas, empresas privadas, instituciones académicas y ONGs colaboren en un terreno neutral y seguro. Esta colaboración puede llevar a soluciones innovadoras a problemas comunes. En este sentido, plataformas abiertas como BFA pueden ser el terreno fértil para emprendimientos conjuntos y proyectos de innovación colectiva, donde diferentes entidades combinan recursos y conocimientos para explorar nuevas oportunidades de negocio o impacto social.

Así, al servir como modelo para operaciones transparentes y eficientes, BFA puede establecer nuevos estándares para la gestión de datos y las prácticas empresariales en Argentina, desafiando a terceras partes a adoptar medidas más robustas y transparentes en sus operaciones.

En resumen, la Blockchain Federal Argentina tiene el potencial de ser una fuerza cambiante en múltiples frentes, promoviendo una economía más eficiente, un paisaje tecnológico avanzado y una sociedad más colaborativa y justa. Su implementación podría ser la piedra angular de la transformación digital y económica del país.

Capítulo 4

4.1 Plan de Implementación

4.1.1 Introducción

En el presente capítulo describiremos las acciones y recursos necesarios para llevar a cabo la implementación de la propuesta planteada en el presente trabajo. Cabe destacar que la red blockchain sobre la cual se implementará la solución ya existe, dado que se planifica utilizar los servicios brindados por la BFA, lo cual genera un gran ahorro a la hora de estimar recursos. Si bien esto es así, como parte del contrato de utilización de la BFA, cada nueva entidad o parte interesada deberá tener con sus propios nodos dentro de la red, para lo cual tendrá que contar con los recursos necesarios para implementar los mismos y mantenerlos.

4.1.2 Cronograma

En este apartado presentamos el cronograma de actividades a realizar para la implementación del proyecto. Este cronograma, representado en la Figura 27, está estimado en una duración de seis meses, dividido en dos trimestres (Q). Cada mes está formado por cuatro cuadros que representan las cuatro semanas. Cabe destacar que esto representa una estimación, y como toda estimación, está sujeta a un margen de error que hemos estimado podría ser del 20% sobre cada actividad.

Figura 27

Cronograma de Actividades

Task number	Task name	Duration	Start date	Finish date	Dependency	Q1				Q2	
						M1	M2	M3	M4	M5	M6
1	Presentación del proyecto a organizaciones interesadas	2w	W1-M1	W2-M1							
2	Envío del formulario de incorporación	1w	W2-M1	W2-M1							
3	Presentación del formulario	1w	W3-M1	W3-M1	2						
4	Aceptación de Políticas de Uso y Reglamento Interno	1w	W4-M1	W4-M1	3						
5	Análisis de viabilidad y uso del sistema	2w	W4-M1	W1-M2							
6	Asignación de equipo al proyecto	1w	W2-M2	W2-M2	5						
7	Asignación de hardware para la implementación	1w	W2-M2	W2-M2	5						
8	Instalación y configuración de Servidores	1s	W3-M2	W3-M2	6, 7						
9	Implementación de nodos	4w	W4-M2	W3-M3	8						
10	Pruebas unitarias	3w	W4-M3	W1-M4	9						
11	Pruebas Integrales	3w	W2-M4	W3-M4	10						
12	Documentación del proyecto	cross	W3-M2	W1-M6							
13	Capacitación de usuarios finales	2w	W2-M5	W3-M5	11						
14	Monitoreo y mantenimiento de la implementación	5w	W3-M5	W3-M6							

4.1.3 Recursos Necesarios

En este apartado se detallarán los recursos humanos y materiales, a nivel hardware y software, que serán necesarios para ejecutar el cronograma de actividades planteado. Cabe destacar que estos recursos son necesarios en cada organización que quiera implementar el proyecto. Para esta estimación de recursos tomamos como objetivo la implementación de un nodo sellador, un nodo transaccional y un nodo de solo lectura.

Líder de Proyecto. Será requerido para dar seguimiento a la implementación del proyecto y garantizar el cumplimiento de los tiempos estimados.

Administradores de infraestructura. Para la instalación y configuración inicial de los servidores y sistemas operativos necesarios para la implementación de los nodos. Deben contar con experiencia en gestión de SO Unix, más específicamente Ubuntu Server o Debian. Lo recomendado es contar con un administrador senior, de no ser posible, recomendamos dos semi-senior.

Programadores. Se requerirán desarrolladores con conocimientos en Solidity y smart contracts en Ethereum. Serán los encargados de implementar los nodos en los servidores preparados por los administradores de infraestructura, y realizar las pruebas antes de quedar en productivo. Se recomienda contar con tres Ssr, con experiencia como full stack developers.

Soporte Técnico. Se deberá establecer un equipo que brinde soporte durante la implementación final como también luego de tener los nodos productivos. Este equipo puede estar formado por miembros que hayan participado en la implementación, o bien podrían ser consultores Ssr.

Servidor Unix. Cada nodo por implementar deberá estar montado sobre un servidor Linux de arquitectura x64. Los servidores recomendados son Debian 12.6 o Ubuntu Server 24.04, o versiones superiores. La memoria RAM y número de CPU de cada servidor depende del tipo de nodo, lo cual se encuentra detallado en la Tabla 3 presentada anteriormente.

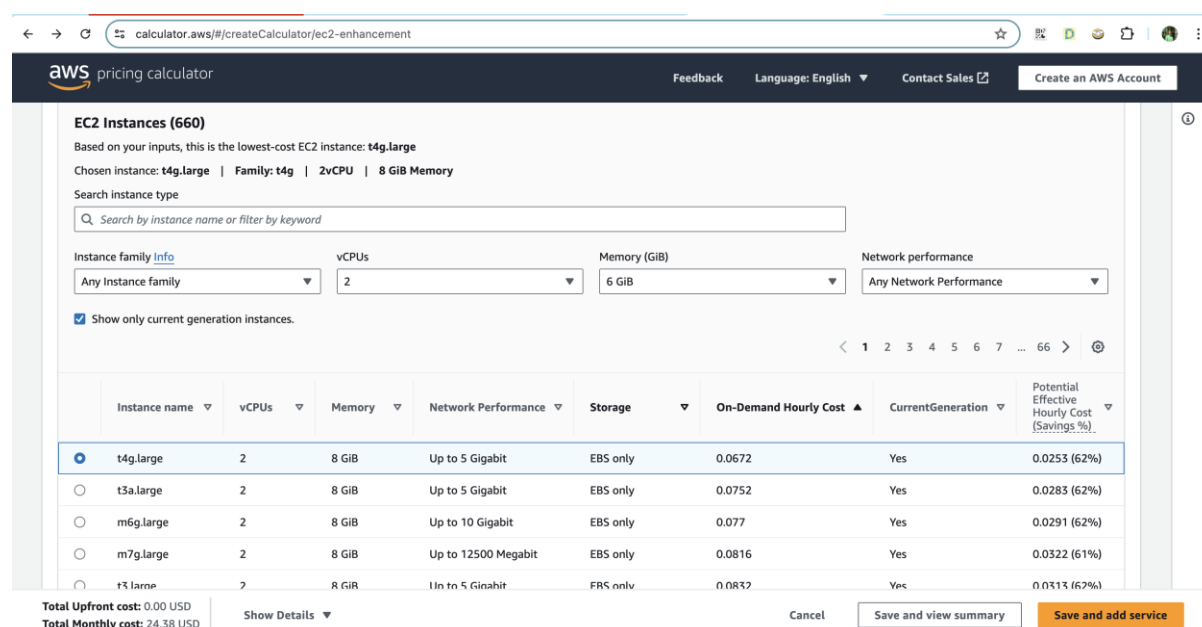
Almacenamiento. Se requiere un mínimo de 300GB para cualquier nodo. De igual modo, en la Tabla 3 se pueden observar las especificaciones recomendadas para cada tipo de nodo. En lo posible utilizar almacenamiento SSD (Solid State Disk) para aprovechar la tasa de I/O (Input/Outputs) de los discos sólidos y evitar problemas de performance.

4.1.4 Estimación de Costos

Para la estimación de costos materiales se tomará como ejemplo la cotización ofrecida por Amazon Web Services (AWS), utilizando la calculadora de precios que dispone la web. Los precios se encuentran expresados en USD (dólar americano).

Figura 28

Costo de servidor AWS para nodo sellador o transaccional



En la figura 28 se observa que un servidor en AWS EC2, correspondiente a la instancia **t4g.large**, con 2 vCPU y 8GB de RAM, cumpliendo de este modo con los requisitos mínimos de un nodo Sellador, tiene un costo de 0.0672 USD por hora activa (on-demand). A este valor, resulta en un total mensual de 24.38 USD.

Con respecto a los otros tipos de nodos, los precios, como se observa en la Figura 29, van desde los 0.0336 USD por hora para un servidor con 2 vCPU y 4GB de RAM, dando un total de 12.19 USD mensual.

Figura 29

Costo de servidor AWS para nodo Gateway, Bootnode, Test o Read-only

EC2 Instances (682)
Based on your inputs, this is the lowest-cost EC2 instance: **t4g.medium**
Chosen instance: **t4g.medium** | Family: **t4g** | 2vCPU | 4 GiB Memory

Search instance type
Search by instance name or filter by keyword

Instance family: Any Instance family | vCPUs: 2 | Memory (GiB): 4 GiB | Network performance: Any Network Performance

☒ Show only current generation instances.

Instance name	vCPUs	Memory	Network Performance	Storage	On-Demand Hourly Cost	CurrentGeneration	Potential Effective Hourly Cost (Savings %)
☒ t4g.medium	2	4 GiB	Up to 5 Gigabit	EBS only	0.0336	Yes	0.0126 (62%)
☐ t3a.medium	2	4 GiB	Up to 5 Gigabit	EBS only	0.0376	Yes	0.0142 (62%)
☐ t3.medium	2	4 GiB	Up to 5 Gigabit	EBS only	0.0416	Yes	0.0156 (62%)
☐ t2.medium	2	4 GiB	Low to Moderate	EBS only	0.0464	Yes	0.0174 (62%)
☐ t4n.large	2	8 GiB	Up to 5 Gigabit	FRS only	0.0672	Yes	0.0253 (62%)

Total Upfront cost: 0.00 USD
Total Monthly cost: 12.19 USD

Show Details | Cancel | Save and view summary | Save and add service

Con respecto al licenciamiento de los sistemas operativos, se utilizará Debian o Ubuntu Server, que, al ser gratuitos no implican el agregado de costos adicionales.

Sobre el capital humano necesario para llevar a cabo el proyecto, en la Tabla 4 se listaron las posiciones requeridas, se estimaron los precios por hora y se calculó la cantidad de horas necesarias para cada puesto. Todo esto sumado a los valores de los servidores da un costo total de 15220,95 USD hasta la fecha de puesta en producción (al finalizar los seis meses).

Tabla 4

Estimación de costos de recursos humanos y materiales

Recursos Materiales			
Descripción	Cantidad necesaria	Precio Mensual	Total (6 meses)
Servidor Nodo			
Sellador/Transaccional	2	\$24,38	\$48,76
Servidor Nodo Solo-Lectura	1	\$12,19	\$12,19
Capital Humano			
Descripción	Horas requeridas	Precio por hora	Total (6 meses)
Líder de Proyecto	960	\$9	\$8640
Administrador de infraestructura	200	\$7	\$1400

Programadores	560	\$7	\$3920
Soporte Técnico	240	\$5	\$1200
Total			\$15220,95

4.1.5 Factores Externos Condicionantes

Existen factores externos que podrían condicionar implementación y durabilidad de este proyecto en el tiempo. En esta sección se analizarán algunos de los más importantes a tener en cuenta:

Regulaciones y Políticas Gubernamentales. Las decisiones legislativas y políticas pueden impactar directamente en la operación y expansión de la BFA. Cambios en la ley de protección de datos, regulaciones de ciberseguridad, o nuevas normas específicas sobre el uso de la blockchain pueden restringir o facilitar sus operaciones.

Tecnología y Avances Competitivos. Las innovaciones en tecnologías blockchain por parte de otras entidades o países podrían desafiar la eficiencia y viabilidad de la BFA si esta no se actualiza o adapta a tiempo. Los avances en criptografía, por ejemplo, podrían hacer que ciertas partes de la infraestructura actual de la BFA se vuelvan obsoletas o vulnerables.

Cooperación Internacional. Dado que la blockchain tiene implicancias que trascienden fronteras (como las transacciones internacionales), la cooperación o las fricciones internacionales podrían influir en la implementación y utilidad efectiva de la BFA.

Adopción del Sector Privado. La efectividad y expansión de la BFA también dependen de su adopción por parte de empresas y organizaciones privadas. La resistencia o la lenta adopción en el sector bancario podría limitar el impacto o la utilidad de la solución planteada.

Condiciones Económicas Generales. Situaciones como inflación, recesión o estabilidad financiera pueden influir en la priorización de proyectos gubernamentales. Factores macroeconómicos adversos podrían llevar a recortes de financiamiento o a una disminución de la inversión en tecnología e innovación.

La caída de los Nodos Selladores. Es poco probable que todos los nodos selladores no se encuentren disponibles o sufran un ataque en simultaneo, pero en caso de suceder, el sistema no se encontraría habilitado para canalizar las actualizaciones que podría sufrir la cadena de bloques. Por lo mencionado anteriormente, es que es necesario determinar la cantidad de nodos selladores necesarios, para garantizar el consenso y la alta disponibilidad del servicio.

Aspectos de Ciberseguridad. La BFA, al estar basada en tecnología digital, está expuesta a riesgos cibernéticos, incluyendo hacks y ataques informáticos. La seguridad de la plataforma debe ser constantemente actualizada y robustecida para prevenir brechas que podrían comprometer datos sensibles.

Cambios Políticos. Las alternancias de poder y los cambios en las administraciones gubernamentales pueden afectar el soporte y la continuidad de proyectos como la BFA, especialmente si la nueva administración tiene una visión tecnológica o de política pública diferente.

4.2 Factibilidad del Proyecto

En esta sección se realizará un análisis de factibilidad del proyecto mencionado en la propuesta de intervención, segmentando el análisis en 5 tópicos, Operativo, Técnico, Económico, Legal y de Duración.

4.2.1 *Análisis de Factibilidad Operativa*

A nivel operativo, la factibilidad del proyecto no debería ser un problema ya que actualmente la propuesta utiliza recursos ya desarrollados por la BFA. Como bien se expuso en la sección “Recursos Necesarios”, para aquellas organizaciones que quieran adoptar este sistema, pero sin incurrir en grandes desarrollos, pueden optar por utilizar nodos de sólo lectura, los cuales requieren de pocos recursos, o directamente utilizar el servicio como usuario final a través de la interfaz web, esta última no requiere instalación de ningún tipo de nodo.

4.2.2 *Análisis de Factibilidad Técnica*

El escenario técnico es quizás el más complejo de la propuesta planteada. Si bien aquellas organizaciones que opten por utilizar sólo la interfaz web no tendrán mayores complicaciones, las que se adentren en la utilización de nodos propios requerirán de recursos más especializados. Como comentamos en la sección “Recursos Necesarios”, para estos casos será necesario contar con personal idóneo con conocimientos en administración de sistemas Unix para la gestión del nodo, conocimientos en Solidity y Web3 para el desarrollo de Smart contracts e integración con los nodos, sumado a los costos de recursos a nivel hardware para implementar y mantener los nodos necesarios activos.

4.2.3 *Análisis de Factibilidad Económica*

El factor económico dependerá completamente del tipo de uso que se le dé al servicio. Tal como comentamos anteriormente, el uso del servicio TSA de la BFA es totalmente gratuito. Si la organización desea unirse al consorcio, en tal caso deberá afrontar los costos de implementación de un nodo sellador. Si además desea realizar desarrollos que integren el servicio Sello de Tiempo o nuevos contratos inteligentes, los costos obviamente se elevarán. En síntesis, a mayor involucramiento con el ecosistema de la BFA, mayores serán los costos, como bien se detalla en la sección “Estimación de costos”.

4.2.4 *Análisis de Factibilidad Legal*

El ámbito legal puede parecer una traba en principio, pero realmente no presenta mayores dificultades. Esto se debe a que, como comentamos en capítulos anteriores, el servicio de la BFA no almacena los archivos que se hashean con el Sello de Tiempo, por lo cual no hay posibilidad de filtración de datos y sus complicaciones legales. Además, la Blockchain Federal Argentina es una iniciativa impulsada por la Administración Pública Nacional, con el apoyo y utilización de Gobiernos provinciales y CABA, siendo una plataforma de multiservicios abierta, participativa y, lo más importante, completamente auditable. Por otro lado, actualmente no existen regulaciones en la Argentina que impidan su uso para la problemática planteada en este proyecto, otro motivo por el cual no debería ser un inconveniente el aspecto legal.

4.2.5 Análisis de Factibilidad de Duración

Respecto a la duración del proyecto, en la sección “Cronograma” hemos realizado una estimación que abarca un total de seis meses. Esta estimación incluye tiempos de entendimiento inicial, concientización, capacitaciones de funcionamiento y utilización, así como también una estimación de tiempos que demoraría la implementación de nodos, conexión a la BFA y su mantenimiento. En comparación con otros proyectos de TI, que normalmente se estiman por trimestre o cuartil (Q), la estimación de este proyecto abarcaría dos Q, lo cual debería ser más que suficiente para cumplir con los tiempos y tareas asignadas.

Capítulo 5

Conclusiones

La presentación de documentación ha sido históricamente un proceso engorroso para los organismos auditados. Las entidades deben entregar la misma información a diferentes organismos en múltiples ocasiones, mientras que estos deben verificar datos que, en muchos casos, ya han sido enviados a otra entidad. Generalmente, la primera entrega incluye un nivel detallado de información y una explicación exhaustiva del proceso de generación de los datos. Sin embargo, a medida que más interesados solicitan la misma información, para el auditado se vuelve tedioso repetir las explicaciones. En este sentido, la propuesta de utilizar el servicio de TSA de la Blockchain Federal Argentina permite que los usuarios puedan certificar la información generada que deben presentar, de modo que esta pueda ser validada directamente por el regulador o auditor sin necesidad de que el auditado participe en el proceso.

Si bien el servicio del Sello de Tiempo es una función ya existente y aplicada en diversos ámbitos, la implementación del servicio como parte del proceso de verificación de documentación para auditorías permite a la parte auditada generar una mejora notable en la administración de tiempos, ya que se evita la repetición de tareas ajenas a su operatoria habitual que debería ejecutar solo para demostrar a los distintos reguladores cómo se genera la misma información. El hecho de que esta solución ya esté siendo utilizada en distintos entes con diversas finalidades demuestra que la solución realmente funciona y es de gran utilidad, como lo son NIC y la validación de dominios generados o transferidos diariamente, el Gobierno Nacional en la publicación de boletines informativos o la cámara de diputados con el proceso de voto electrónico, ambos para certificar que no existieron cambios posteriores a sus publicaciones, entre otros ejemplos de los mencionados a lo largo del trabajo, lo que nos lleva a reafirmar la creencia de que nuestra propuesta es factible de ser implementada y utilizada en el ámbito financiero local.

Además, debemos tener en cuenta que, si bien el costo económico final del proyecto no debería representar un problema al compararlo con otros proyectos de tecnología y desarrollo que habitualmente llevan adelante los bancos, existe también la posibilidad de probar el servicio TSA de la Blockchain Federal Argentina como un usuario final, accediendo de modo totalmente gratuito. De esta forma, cualquier usuario perteneciente a un banco, por ejemplo,

podría probar el sello de tiempo de la BFA sin necesidad de desplegar nodos y los esfuerzos que esto conlleva. Cuando los usuarios hayan probado y verificado que el servicio les es útil, la entidad podrá sumarse como parte de la organización y comenzar a desplegar sus nodos, pero ya con la certeza de su funcionamiento.

Por otro lado, el hecho de contar con sus propios nodos permite a las entidades financieras mitigar el riesgo de caída del servicio, ya que podrían sellar sus propias transacciones y mantener una réplica constante de la red en sus nodos operativos. Un aspecto de suma importancia ya que de este modo se descarta una posible indisponibilidad del servicio.

En conclusión, la propuesta de utilizar la BFA como sistema para certificar documentación regulatoria es una iniciativa innovadora que ofrece numerosos beneficios y representa un gran avance en el manejo y seguridad de documentos críticos. El uso de la BFA no solo incrementa la transparencia y la trazabilidad, sino que también fortalece la integridad de los documentos, garantizando que sean inalterables y permanentes.

A través de este sistema de certificación basado en blockchain, se puede asegurar la autenticidad de la documentación regulatoria, lo cual es esencial para cumplir con las normativas vigentes y minimizar los riesgos de fraude y manipulación. Además, la descentralización del sistema ayuda a eliminar la necesidad de intermediarios, lo que simplifica los procesos y reduce los tiempos de gestión.

Otro aspecto destacable de la propuesta es la mejora en la eficiencia operacional. La automatización de la verificación de documentos a través de la BFA reduce la carga administrativa y permite que las instituciones se enfoquen en tareas de mayor valor estratégico. Esto no solo optimiza los recursos, sino que también mejora el servicio al cliente, ofreciendo respuestas más rápidas y fiables.

Finalmente, cabe resaltar que la implementación de esta tecnología no solo beneficia a las entidades reguladoras y a las empresas sujetas a regulación, sino que también fomenta la confianza pública en los sistemas de control y vigilancia.

Futuras Líneas de Trabajo

En esta sección se presentarán algunas ideas de implementación que podrían enriquecer el proyecto propuesto, o que podrían surgir a partir de posibles extensiones de la solución.

Una de las mejoras sugeridas para el modelo existente sería la creación de una API o la robotización del proceso de conexión con el servicio de TSA. Esto permitiría que los usuarios de las organizaciones participantes puedan generar comprobantes de manera automatizada, sin la necesidad de acceder a la interfaz web de la BFA.

Además, existe la posibilidad de aplicar el modelo a otros ámbitos que no estén relacionados con el sector financiero. En concordancia con los antecedentes expuestos anteriormente, se podría utilizar el sistema de validación para certificaciones y títulos obtenidos por los alumnos de la Universidad Abierta Interamericana. Aunque esta funcionalidad ya está presente en otras instituciones, la UAI aún no la ha implementado, lo que ofrece la oportunidad de desarrollar una solución propia que permita la emisión de certificados directamente desde los servicios de la Universidad.

Estas son solo algunas de las ideas que pueden surgir a partir de la implementación de la solución propuesta. Con un enfoque creativo y una mente abierta a nuevas posibilidades, se pueden encontrar múltiples oportunidades para expandir y mejorar el proyecto inicial.

Referencias

Absatz Mariano (2019), *Monitoreo Procedimiento*. Gitlab BFA.

<https://gitlab.bfa.ar/blockchain/docs/-/wikis/Monitoreo-Procedimiento>

Al Asad Nafiz, Elahi Tausif, Al Hasan Abdullah, Yousuf Mohammad (2020). *Permission-Based Blockchain with Proof of Authority for Secured Healthcare Data Sharing* [Blockchain basada en permisos con Prueba de Autoridad para Publicación de Datos Seguros de Salud]. IEEE Xplore. <https://ieeexplore.ieee.org/document/9333488>

Antonopoulos Andrea (2018), *Mastering Ethereum* [Dominando Ethereum]. Editorial O'Reilly. [https://dl.ebooksworld.ir/motoman/Mastering_Ethereum_Andreas.M.Antonopoulos.w
ww.EBooksWorld.ir.pdf](https://dl.ebooksworld.ir/motoman/Mastering_Ethereum_Andreas.M.Antonopoulos.www.EBooksWorld.ir.pdf)

Argañaraz Ángel Agustín, Mazzuchelli Agostina, Albanese Diana, López María de los Ángeles (2019). *Blockchain: un nuevo desafío para la contabilidad y auditoría*. Facultad de Ciencias Económicas, Universidad de La Plata. <https://epositoriodigital.uns.edu.ar/handle/123456789/5135>

AWS Pricing Calculator [Calculadora de Precio]. Recuperado el 30 de junio de 2024 de <https://calculator.aws/#/createCalculator/ec2-enhancement>

Badiss, K., Essaf, F., Jianbiao, Z., & Sakho, S. (2019). *Improving banking transactions using blockchain technology*. IEEE. <https://ieeexplore.ieee.org/document/9064344>

Banco Central de la República Argentina (s. f.). *Ley 24.144 - Carta Orgánica del BCRA*. Recuperado el 7 de julio de 2024 de https://www.bcr.gov.ar/Institucional/Carta_Organica.asp#a

BCRA (2022). Comunicación “A” 7423.

<https://www.bcra.gob.ar/Pdfs/comytexord/A7493.pdf>

BCRA (2023a). Comunicación “A” 7724.

<https://www.bcra.gob.ar/pdfs/comytexord/A7724.pdf>

BCRA (2023b). Comunicación “A” 7783.

<https://www.bcra.gob.ar/pdfs/comytexord/A7783.pdf>

Blockchain Federal Argentina (s. f). *¿Qué es blockchain?* Recuperado el 30 de junio de 2024

de <https://bfa.ar/blockchain/blockchain>

Blockchain Federal Argentina (s. f). *Aplicaciones*. Recuperado el 8 de julio de 2024 de

<https://bfa.ar/bfa/aplicaciones>

Blockchain Federal Argentina (s. f). *Bloques y Transacciones*. Recuperado el 30 de junio de

2024 de <https://bfa.ar/blockchain/bloques-y-transacciones>

Blockchain Federal Argentina (s. f). *Cómo funciona*. Recuperado el 30 de junio de 2024 de

<https://bfa.ar/bfa/como-funciona>

Blockchain Federal Argentina (s. f). *Especificación de TSA (TimeStamp Authority)* Recuperado

el 30 de junio de 2024 de

<https://docs.google.com/document/d/19PYSiAkInGXLEbSDqWQh->

[1zSrY4rr20Palr1H8MjaEQ/edit?usp=sharing](https://docs.google.com/document/d/19PYSiAkInGXLEbSDqWQh-1zSrY4rr20Palr1H8MjaEQ/edit?usp=sharing)

Blockchain Federal Argentina (s. f). *Licitaciones*. Recuperado el 30 de junio de 2024 de

<https://bfa.ar/blockchain/casos-de-uso/licitaciones>

Blockchain Federal Argentina (s. f). *Pólizas de Caución*. Recuperado el 30 de junio de 2024 de <https://bfa.ar/blockchain/casos-de-uso/poliza-de-caucion>

Blockchain Federal Argentina (s. f). *Protocolos de Consenso*. Recuperado el 30 de junio de 2024 de <https://bfa.ar/blockchain/protocolos-de-consenso>

Blockchain Federal Argentina (s. f). *Títulos Académicos*. Recuperado el 30 de junio de 2024 de <https://bfa.ar/blockchain/casos-de-uso/titulos-academicos>

Blockchain Federal Argentina (s. f). *Trazabilidad de Alimentos*. Recuperado el 30 de junio de 2024 de <https://bfa.ar/blockchain/casos-de-uso/trazabilidad-de-alimentos>

Blockchain Federal Argentina (s. f). *Smart Contracts*. Recuperado el 30 de junio de 2024 de <https://bfa.ar/blockchain/smart-contracts>

Boletín Oficial (2018). *Ley 27444 Simplificación y Desburocratización para el Desarrollo Productivo de la Nación*. <https://www.argentina.gob.ar/normativa/nacional/ley-27444-311587/texto>

Broomé, L. (2019). *Banking on Blockchain*. North Carolina Journal Of Law & Technology. <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1392&context=ncjolt>

CoinDesk (2023). *First Mover Americas: JPMorgan Goes Live With First Blockchain-Based Collateral Settlement*. CoinDesk. <https://www.coindesk.com/markets/2023/10/11/first-mover-americas-jpmorgan-goes-live-with-first-blockchain-based-collateral-settlement/>

Comisión Nacional de Valores (s. f.). *Quienes Somos*. CNV. <https://www.argentina.gob.ar/cnv/institucional/quienes-somos>

Crosby, M., Kalyanaraman, V., Nachiappan, Pattanayak, P., & Vérma, S. (2016). *BlockChain Technology: Beyond Bitcoin. Applied Innovation Review*. <https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf>

De Angelis Stefano, Aniello Leonardo, Baldoni Roberto, Lombardi Federico, Margheri Andrea, Sassone Vladimiro (2018). *PBFT vs proof-of-authority* [BFT contra Pruebas de Autoridad]. Universidad de Southampton. <https://eprints.soton.ac.uk/415083/>

Drescher Daniel (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps* [Blockchain Básico: Una introducción no técnica en 25 pasos]. Apress. https://app.scnu.edu.cn/iscnu/learning/block_chain/Blockchain%20basic.pdf

Franca Daniel (2019). *Brief BFA*. Blockchain Federal Argentina. <https://gitlab.bfa.ar/blockchain/docs/-/wikis/presentacion-bfa>

Glaros Michael (2019). *The Marco Polo Network uses Azure and Corda blockchain to modernize trade finance* [La red Marco Polo usa Azure y la Blockchain Corda para modernizar la financiación del comercio]. Microsoft Azure Blog. <https://azure.microsoft.com/en-us/blog/the-marco-polo-network-uses-azure-and-corda-blockchain-to-modernize-trade-finance/>

Gómez Santiago, Pava Roberto, Hernández Cesar (2023). *Plataforma para preservar y verificar documentos aplicando identidad auto-soberana soportada en blockchain*. Universidad Central Las Villas. https://www.researchgate.net/profile/Roberto-Pava-2/publication/379219253_ConvencionUCLV/links/65fee006f3b56b5b2d25b16a/ConvencionUCLV.pdf

- Howcroft, E. (2023). *Goldman Sachs digital assets chief sees 'huge appetite' for blockchain assets*. Reuters. <https://www.reuters.com/business/finance/goldman-sachs-digital-assets-chief-sees-huge-appetite-blockchain-assets-2023-12-13/>
- HSBC (2019). *A step closer to paperless trade* [Un paso más cerca del comercio sin papeles]. <https://www.hsbc.com/news-and-views/views/hsbc-views/a-step-closer-to-paperless-trade>
- HSBC (2021). *Blockchain en el comercio internacional*. <https://www.business.hsbc.com.ar/es-ar/insights/innovation-and-transformation/blockchain-en-el-comercio-internacional>
- Jiménez Marta (2019). *Utilización de Blockchain para la validación de documentos*. Universidad de las Palmas de Gran Canaria. <https://accedacris.ulpgc.es/bitstream/10553/101063/1/TFG%20Marta%20Jim%C3%A9nez%20Rodr%C3%ADguez.pdf>
- Kinexys by JP Morgan. (2024). *About Kinexys*. <https://www.jpmorgan.com/kinexys/about>
- JP Morgan (s. f.). *JPM Coin Systems*. <https://www.jpmorgan.com/onyx/coin-system>
- Martínez Ian (2023). *Certificados académicos digitales con blockchain*. Escuela Colombiana de Ingeniería Julio Garavito. <https://dspace-escuelaing.metacatalogo.com/handle/001/3035>
- Muneeza, A., & Mustapha, Z. (2020). *Application of Blockchain Technology in Crowdfunding to Fuel the Rise of the Rest Globally*. Sahulat. <https://acortar.link/Y773zc>
- NIC Argentina (s.f.). *Altas y Transferencias Diarias*. Recuperado el 7 de julio de 2024 de https://rdlist.nic.ar/rd_list/

R3 (2023). *Corda Overview* [Descripción General de Corda]. <https://r3.com/factsheets/corda-overview/>

Rizzo, P. (2016). *Goldman Sachs: Blockchain Tech Could Save Capital Markets \$6 Billion a Year*. <https://ccma-acmc.ca/en/wp-content/uploads/Goldman-Sachs-Blockchain-Tech-Could-Save-Capital-Markets-6-Billion-a-Year-May-25-2016.pdf>

Safi Ali (2020). *DLT de cadena de bloques de varias nubes*. Microsoft Learn. <https://learn.microsoft.com/es-es/azure/architecture/example-scenario/blockchain/multi-cloud-blockchain>

Santander (2018). *Lanzamiento One Pay FX*. [https://www.santander.com/content/dam/santander-com/es/documentos/historico-notas-de-prensa/2018/04/NP-2018-04-12-Santander lanza en cuatro países el primer servicio de transferencias internacionales con -es.pdf](https://www.santander.com/content/dam/santander-com/es/documentos/historico-notas-de-prensa/2018/04/NP-2018-04-12-Santander%20lanza%20en%20cuatro%20pa%C3%ADses%20el%20primer%20servicio%20de%20transferencias%20internacionales%20con%20-%20es.pdf)

Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System* [Bitcoin: Un Sistema de dinero electrónico par a par]. <https://bitcoin.org/bitcoin.pdf>

Superintendencia de Entidades Financieras y Cambiarias (s. f.). *Autoridades*. SEFyC. https://www.bcra.gob.ar/institucional/Autoridades_Detalle.asp?Nombre=Superinten

Superintendencia de Seguros de la Nación (s. f.). *¿Quiénes somos?*. SSN. <https://www.argentina.gob.ar/superintendencia-de-seguros/institucional>

Unidad de Información Financiera (s. f.). *¿Quiénes somos?*. UIF. <https://www.argentina.gob.ar/uif/institucional>

Waldman Jonathan (2018). *Cadena de bloques: aspectos básicos de la cadena de bloques*.

Microsoft Learn.

<https://learn.microsoft.com/es-es/archive/msdn-magazine/2018/march/blockchain-blockchain-fundamentals>

Zheng Zibin, Xie Shaoan, Dai Honging, Chen Xiangping, Wang Huaimin (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends* [Un Resumen de la Tecnología Blockchain: Arquitectura, Consenso y Futuras Tendencias]. IEEE Xplore. <https://ieeexplore.ieee.org/document/8029379>

Acrónimos

API: Application Programming Interface, se refiere a la interfaz de programación de aplicación software que actúa de intermediario para poder establecer una comunicación e intercambiar datos.

API REST: (del inglés Representational State Transfer) es un tipo de servicio web que utiliza solicitudes HTTP para manipular y recuperar datos. Es una forma ligera y flexible de integrar aplicaciones y conectar componentes en arquitecturas de microservicios.

BCRA: Banco Central de la República Argentina

BFA: Blockchain Federal Argentina

PBFT: La tolerancia a faltas bizantinas (del inglés Practical Byzantine Fault Tolerance) es la resistencia de un sistema informático tolerante a faltas, en particular los sistemas informáticos distribuidos, a fallas de componentes electrónicos donde hay información imperfecta sobre si un componente falla.

CA: Certificate Authority, o autoridad certificante, corresponde al componente dentro de una red blockchain para la emisión de certificados pertenecientes a cierta organización.

CNV: Comisión Nacional de Valores

UIF: Unidad de Información Financiera

EBNF: La Notación de Backus-Naur, también llamado BNF extendido (del inglés Extended Backus–Naur Form) es un metalenguaje usado para expresar gramáticas libres de contexto.

GUI: Graphical User Interface. La interfaz gráfica de usuario es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.

NOC: Centro de Operaciones de Red

PoW: Proof of Work

PoA: Proof of Authority

SHA: Secure Hash Algorithm. Son un conjunto de funciones hash utilizadas durante el proceso de encriptación.

SO: Sistema Operativo. Hace referencia al conjunto de instrucciones, programas y servicios para controlar el hardware de la computadora.

SR: Senior, se refiere al grado de seniority de un recurso que forma parte de un equipo de trabajo. En este caso, se refiere a un recurso con un nivel avanzado de conocimientos en el campo.

SSr: Semi Senior, se refiere al grado de seniority de un recurso con conocimientos y experiencia intermedios dentro un campo de aplicación en particular.

TSA: Una Autoridad de Sellado de Tiempo (del inglés Time Stamping Authority) es una entidad que proporciona una forma segura y confiable de sellar documentos, datos o transacciones digitales.

Anexo I

A continuación, se describen una serie de pasos a seguir para la correcta instalación de un nodo BFA (nodo sellador, nodo gateway, nodo transaccional). Esta guía está pensada para ejecutarse en sistemas operativos Debian o Ubuntu Server sin GUI instalada.

Para comenzar se debe instalar en el servidor el servicio *git*. Utilizando un usuario con permisos de superusuario (*root*) se debe ejecutar el comando `apt install git`

Luego, se debe clonar el repositorio oficial de la BFA. Para ello se ejecuta el comando `git clone https://gitlab.bfa.ar/blockchain/nucleo.git bfa`. Luego se inicia la instalación del nodo, lo cual cambiará algunas configuraciones del sistema. Para ello, se ejecuta con permisos *root* el comando `bfa/bin/installbfa.sh`. Esta acción consultará si se desea conectar a la red de *producción* o de *prueba (test2)*.

Es probable que durante la instalación de Web3 aparezcan en pantalla varios *warnings* (advertencias), lo cual es normal y no limita el proceso de instalación.

Una vez finalizado este proceso, se debe cambiar al usuario *bfa* para ejecutar la sincronización con la red de la BFA. Para ello, con permisos *root*, se debe ejecutar el comando `su - bfa`, y desde este usuario se inicia la sincronización con el comando `start.sh`. Este proceso puede llevar algo de tiempo, ya que debe sincronizar toda la blockchain de la BFA con el nodo creado. Cabe destacar que este script se ejecuta automáticamente cada vez que se reinicia el sistema.

Finalmente, para administrar la configuración del nodo se utiliza `admin.sh syncmode`, aunque se recomienda esperar a que el nodo termine de sincronizar para hacer cualquier cambio. Puede tardarse alrededor de una hora conectarse la primera vez, es normal que en el log no se observe nada.

En la Tabla 5 se presentan otros comandos que pueden ser de utilidad para la administración de un nodo.

Tabla 5

Comandos útiles para el manejo del nodo.

Comando	Función
explorer.sh	Sigue el bloque más nuevo " <i>latest</i> " por default, pero es posible especificar un número de bloque cualquiera como argumento, por ejemplo " <i>explorer.sh 0</i> " permite ver el génesis (bloque 0).
walker.pl	Toma un número de bloque para iniciar. Sigue esperando nuevos bloques.
sealerwatch.pl	Muestra cuando los selladores firman.
net.getVersion	Permite consultar el ID de la red Red de producción (nombre: network): 47525974938 (0xb10c4d39a) Red de pruebas (nombre: test2network): 55555000000 (0xcef5606c0)
eth.chainId	Permite consultar el chainId Red de producción (network): 200941592 (0xbfa2018) Red de pruebas (test2network): 99118822 (0x5e86ee6)
attach.sh	Conecta a la línea de comandos (CLI) del geth que está corriendo en la máquina local (falla si no hay un geth corriendo).
rewind.sh	Si el nodo local parece estancado y sigue conectado, esta herramienta va a retroceder algunos bloques en la cadena y tratar de retomar desde allí.
bfalog.sh	Permite monitorear los logs del nodo.
monitor.js	Esto se corre desde cron.sh. Cada minuto actualizará el archivo network/status que muestra información del estado del nodo muy básica.
compile.and.deploy.contract	Compila y despliega un <i>smart contract</i> a la blockchain. Debe haber una cuenta local que tenga suficiente Ether para pagar por la transacción.
localstate.pl	Muestra el estado actual del nodo y varios detalles del entorno local.

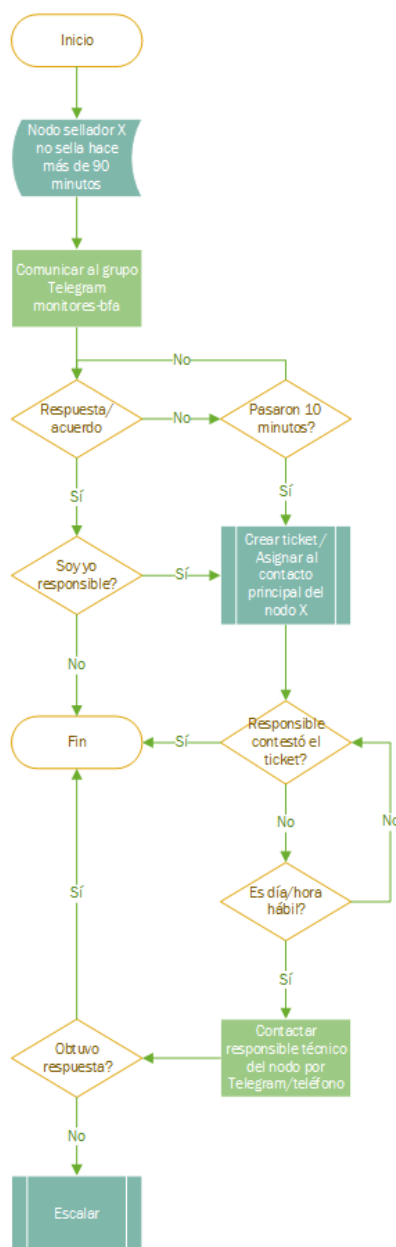
Anexo II

En este anexo se detalla el procedimiento indicado para el tratamiento de eventos alertados por el proceso de monitoreo. Para explicar mejor el proceso, tomaremos como ejemplo el caso de que un nodo sellador no selle transacciones en un periodo mayor a 90 minutos, tal como se observa en la Figura 30.

Ante la detección de un evento de este estilo, lo primero que realiza el equipo de monitoreo es comunicar el caso vía Telegram al grupo @monitores-bfa (donde sólo están los que monitorean, no los selladores). Esto es para evitar tickets duplicados cuando un inconveniente es detectado por más de un NOC. Se acuerda cuál de los NOC levantará el ticket (si no hay respuesta en el grupo Telegram en 10 minutos, el que detectó el inconveniente levanta el ticket); si se llegan a crear múltiples tickets, a medida que se detecta que es el mismo caso, se cierran los tickets duplicados con referencia al ticket que se defina como principal.

El NOC seleccionado crea un ticket en el proyecto del gitlab que se defina (debe ser un proyecto al que sólo tienen acceso los responsables de los nodos selladores, el equipo de monitoreo, el CdA y el comité técnico). El ticket se debe asignar al contacto técnico principal del nodo afectado. Una vez que el responsable del nodo toma conocimiento, debe o bien solucionar el problema (y que esto se refleje en las consolas de monitoreo) o solicitar la suspensión temporal de su permiso de sellado.

Si el sellador solucionó el problema, debe informarlo en el ticket. Al menos dos NOCs de monitoreo deben confirmar que ven al nodo sellar correctamente y marcar el ticket como resuelto. El responsable del nodo sellador deberá cerrar el ticket, y si este solicita la suspensión temporal de su permiso de sellado, debe marcar el ticket como “*wontfix*”, iniciar el proceso de suspensión de su nodo y cerrar el ticket

Figura 30*Flujo de tratamiento de un evento por parte del NOC*

Nota. Si se producen discusiones o acuerdos telefónicamente o vía Telegram, los mismos deben transcribirse al ticket. Tomado de Procedimiento de Monitoreo, por la Blockchain Federal Argentina. (<https://gitlab.bfa.ar/blockchain/docs/-/wikis/Monitoreo-Procedimiento>)