

UNIVERSIDAD NACIONAL DE TUCUMAN



Facultad de Ciencias Exactas y Tecnología
Departamento de Eléctrica, Electrónica y Computación
INGENIERÍA EN COMPUTACIÓN

TRABAJO DE GRADUACIÓN
“Integración de la Universidad Nacional de Tucumán
(UNT) en la Blockchain Federal Argentina (BFA).”

Autores:
Bardin, Pablo Mauricio.
López Jerez, Maria Mercedes.

Tutores:
Ing. Lutz, Federico Herman.
Ing. Bilbao, Javier Ignacio.

Abril 2025

Agradecimientos

En este momento tan significativo para nosotros, queremos expresar nuestro más profundo agradecimiento a nuestras familias y amigos, cuyo apoyo constante y aliento incondicional fueron clave para superar cada etapa de este camino.

Agradecemos a nuestros docentes, quienes con compromiso y generosidad compartieron su saber, guiando nuestro crecimiento académico y personal. También a nuestros compañeros, por los momentos compartidos, el apoyo mutuo y las risas que hicieron más llevadero todo este recorrido.

Finalmente, queremos destacar y agradecer a la Universidad Nacional de Tucumán, por brindarnos una formación académica sólida y por abrirnos las puertas a nuevas oportunidades de aprendizaje y desarrollo.

A nuestros padres,

Por ser nuestro refugio en los días difíciles y nuestra mayor alegría en los días de logro.

Por enseñarnos con el ejemplo que todo esfuerzo vale la pena, guiarnos con amor y alentarnos a seguir cuando dudábamos de nosotros mismos.

Este trabajo es tan nuestro como suyo, porque cada paso que dimos hasta aquí fue posible gracias a su amor incondicional, su apoyo constante y su fe inquebrantable en nosotros.

Con todo nuestro amor y gratitud, les dedicamos este logro.

Prólogo

Vivimos en una era donde la tecnología avanza a un ritmo vertiginoso y redefine la manera en que interactuamos con la información. En medio de este panorama, la Blockchain se presenta no solo como una innovación técnica, sino como una oportunidad para construir sistemas más transparentes, colaborativos y seguros.

Este trabajo nace de una inquietud genuina: ¿Qué lugar pueden ocupar nuestras universidades en este nuevo paradigma digital? ¿Cómo podemos acercar a las instituciones públicas a tecnologías emergentes que, hasta hace poco, parecían lejanas o complejas?

Así fue como decidimos explorar el potencial de la Blockchain Federal Argentina (BFA) desde una mirada universitaria. La instalación de un nodo de prueba en la Universidad Nacional de Tucumán fue mucho más que un ejercicio técnico, fue un primer paso hacia una transformación posible, donde el conocimiento abierto, la soberanía digital y la innovación pública se dan la mano.

Este informe es el resultado de horas de investigación, pruebas, errores y aprendizajes. Pero también es una invitación a imaginar nuevas formas de construir tecnología desde lo público, desde lo local, desde la universidad. Esperamos que, al recorrer estas páginas, el lector descubra no solo una experiencia técnica, sino una visión del futuro que queremos ayudar a construir.

Índice General

1 - Introducción.....	7
1.1 Introducción.....	7
1.2 Objetivos.....	7
1.2.1 Objetivos Generales.....	7
1.2.2 Objetivos específicos.....	7
1.3 Especificaciones del trabajo.....	8
2 - Marco Teórico - Conceptos Clave.....	9
2.1 Blockchain.....	9
2.1.1 Tipos de Blockchain.....	10
2.1.2 Transacciones.....	10
2.2 Criptografía.....	11
2.2.1 Importancia de los hash en Blockchain.....	12
2.3 Blockchain Federal Argentina (BFA).....	12
2.3.1 Modelo sin criptomoneda.....	13
2.3.2 Modelo liviano.....	13
2.3.3 Transacciones gratuitas.....	13
2.3.4 Almacenamiento Off-Chain.....	13
2.3.5 Software libre.....	14
2.3.6 Tecnología Ethereum.....	14
2.3.7 Monitoreo.....	14
2.3.8 Sello de tiempo.....	14
2.3.9 Destilería de Gas.....	15
2.3.10 Plataforma y Aplicaciones sobre BFA.....	16
2.3.11 Nodos.....	16
2.4 Docker.....	17
2.5 Acceso ssh.....	17
2.6 Amazon Web Services (AWS).....	18
2.7 Testnet.....	19
2.8 Contratos Inteligentes (Smart Contracts).....	19
3 - Especificación de Requisitos:.....	22
3.1 Requisitos Funcionales.....	22
3.2 Requisitos No Funcionales.....	22
3.3 Requisitos Técnicos.....	23
3.4 Requisitos de Documentación.....	23
4 - Documentación.....	24
4.1 Infraestructura del nodo y conexión con la BFA.....	24
4.1.1 Esquema de infraestructura del nodo de la UNT.....	24
4.2 Manual técnico.....	26
4.2.1 Instrucciones para la configuración del nodo en la testnet.....	26
4.2.2 Proceso para ejecutar pruebas de conectividad y transacciones.....	31

4.3 Reportes de Pruebas.....	32
4.3.1 Registro de transacciones realizadas durante las pruebas.....	32
4.3.2 Desempeño del nodo bajo diferentes condiciones.....	35
4.4 Análisis de Factibilidad.....	36
4.4.1 Beneficios de la integración completa de la UNT en la BFA.....	36
4.4.2 Desafíos técnicos, administrativos y operativos identificados durante las pruebas.....	37
4.5 Recomendaciones.....	38
4.5.1 Instrucciones para una futura integración completa.....	38
4.5.2 Recursos adicionales necesarios para garantizar la sostenibilidad del nodo.....	40
5 - Conclusiones.....	41
6 - Bibliografía.....	42

Índice de imágenes

Figura 3.1: proceso simplificado de validación y registro de una transacción en una red blockchain.....	11
Figura 3.2: un mínimo cambio en una foto produce un cambio completo del hash....	12
Figura 3.3: proceso de sellado de archivos en la Blockchain mediante TSA.....	15
Figura 3.4: distribución automatizada de gas para operaciones en la red BFA.....	16
Figura 3.5: quienes pueden instalar los diferentes tipos de nodo de la BFA.....	17
Figura 4.1: infraestructura del nodo BFA en AWS, desplegado en una VM dentro de la VPC de la UNT.....	25
Figura 4.2: flujo de comunicación entre el usuario, el servicio TSA, el nodo BFA y el resto de los nodos de la red.....	25
Figura 4.3: histograma de Tiempos de Confirmación de TimeStamp al sellar un único documento.....	33
Figura 4.4: histograma de Tiempos de Confirmación de TimeStamp al sellar dos documentos.....	34
Figura 4.5: histograma de Tiempos de Confirmación de TimeStamp al sellar cinco documentos.....	34
Figura 4.6: histograma de Tiempos de Confirmación de TimeStamp al sellar diez documentos.....	35
Figura 4.7: tiempo Promedio por Documento vs. Cantidad de Documentos Sellados Simultáneamente.....	36

1 - Introducción

1.1 Introducción

La tecnología Blockchain ha surgido como una herramienta innovadora capaz de transformar diversos sectores mediante la descentralización, la transparencia y la seguridad de los datos. En este contexto, la Blockchain Federal Argentina (BFA) se presenta como una plataforma multiservicios diseñada para integrar aplicaciones y servicios, destacándose por su enfoque en la transparencia, accesibilidad y uso sin criptomonedas.

El presente trabajo tiene como objetivo establecer un nodo de prueba en la Universidad Nacional de Tucumán (UNT) como parte de la red de la BFA. Este nodo permitirá evaluar la factibilidad técnica y los beneficios potenciales de una futura integración completa, explorando aplicaciones prácticas como la digitalización de procesos administrativos y la gestión segura de información académica.

Este informe detalla los pasos seguidos en la investigación, diseño, configuración y pruebas realizadas en un entorno controlado, proporcionando las bases para comprender las posibilidades y desafíos de implementar Blockchain en instituciones académicas. La propuesta incluye una evaluación preliminar de las herramientas utilizadas y los beneficios potenciales que esta tecnología puede aportar a la comunidad universitaria.

1.2 Objetivos

1.2.1 Objetivos Generales

Establecer un nodo de prueba en la Universidad Nacional de Tucumán (UNT) como parte de la Blockchain Federal Argentina (BFA) para evaluar la factibilidad y beneficios de una futura integración completa.

1.2.2 Objetivos específicos

- Diseñar y configurar un nodo de prueba que permita la conexión básica con la Blockchain federal Argentina.
- Realizar pruebas controladas de intercambio de información con otros nodos de la federación en un entorno de prueba.
- Documentar el proceso de implementación y los requerimientos necesarios para una futura implementación completa.
- Proveer un análisis preliminar sobre los beneficios y desafíos de integrar la facultad en la federación.

1.3 Especificaciones del trabajo

- Investigación bibliográfica para definir los requisitos técnicos básicos de un nodo en la Blockchain Federal Argentina.
- Desarrollo de un prototipo funcional de nodo en un entorno controlado, orientado a pruebas de conexión y comunicación básica.
- Realización de pruebas limitadas de conectividad y validación de datos entre el nodo de prueba de la facultad y otros nodos de la red de prueba.
- Generación de documentación técnica sobre el proceso y los requisitos para una futura ampliación del nodo a producción (Sujeto a futura aprobación de la Blockchain Federal Argentina).

2 - Marco Teórico - Conceptos Clave

2.1 Blockchain

Blockchain es una tecnología diseñada para administrar un registro de datos online, caracterizada por ser transparente y prácticamente incorruptible.

A grandes rasgos, Blockchain se puede pensar como un libro contable o una base de datos donde solo se puede ingresar entradas nuevas y donde las existentes no se pueden modificar ni eliminar. Esas entradas, llamadas transacciones, se agrupan en bloques que se van agregando, sucesivamente, al registro en forma de cadena secuencial, cada uno de ellos relacionado necesariamente con el anterior.

En ese esquema, si se necesita rectificar algún dato previamente registrado, no se puede hacer modificándolo directamente. En su lugar, debe añadirse una nueva entrada que refleje la corrección, manteniéndose siempre visibles los datos originales, que pueden ser auditados 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, conocidas 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. Así, se garantiza la seguridad de esa información ya que, por ejemplo, habría que “hackear” gran parte de la red y no solamente un servidor central para poder modificarla, borrarla o robarla.

Pero también tenemos que tener en cuenta que la Blockchain no solo está protegida por este modelo de red descentralizada, sino que también está atravesada por métodos criptográficos que garantizan que nada pueda ser borrado o alterado sin que todos los usuarios puedan darse cuenta de ello.

Las principales características de Blockchain incluyen:

- Se puede verificar con seguridad la identidad de quienes participan en cada transacción, ya que todas están respaldadas mediante firmas criptográficas.
- Cada transacción queda registrada con una marca exacta de fecha y hora, funcionando como una certificación temporal.
- La información registrada no puede alterarse ni eliminarse; una vez guardada en la blockchain, permanece inmutable.
- Todos los datos incorporados a la cadena son completamente auditables, ya que quedan registrados de forma pública y accesible para cualquier usuario.
- No necesita intermediarios para validar o certificar la información, ya que la estructura propia de la blockchain garantiza su seguridad e integridad.
- Al igual que en un libro contable, no se permite eliminar ni modificar entradas existentes. Solo se puede sumar nueva información, haciendo que la blockchain crezca de manera continua.

2.1.1 Tipos de Blockchain

La Blockchain se clasifica en dos tipos principales según su nivel de acceso y control:

- **Blockchain Pública:** está abierta a cualquier persona que desee participar. Cualquier usuario puede operar como nodo, enviar transacciones o verificar bloques. Este modelo promueve la descentralización total y asegura altos niveles de transparencia. Ejemplo: Bitcoin, Ethereum.
Usos comunes: criptomonedas, aplicaciones descentralizadas (DApps).
- **Blockchain Privada:** su uso está limitado a un conjunto definido de participantes, normalmente pertenecientes a una empresa o consorcio. El control sobre quién puede acceder, validar o escribir en la cadena está en manos de una autoridad central. Ejemplo: Hyperledger Fabric, Corda.
Usos comunes: gestión de cadenas de suministro, sistemas internos de organizaciones.

2.1.2 Transacciones

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

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

Cada transacción es enviada a la red a través de un nodo, y se combina con otras transacciones para conformar un bloque. Cuando ese bloque se agrega a la cadena, la transacción queda incorporada definitivamente y se considera como “completada” (ver Figura 3.1).

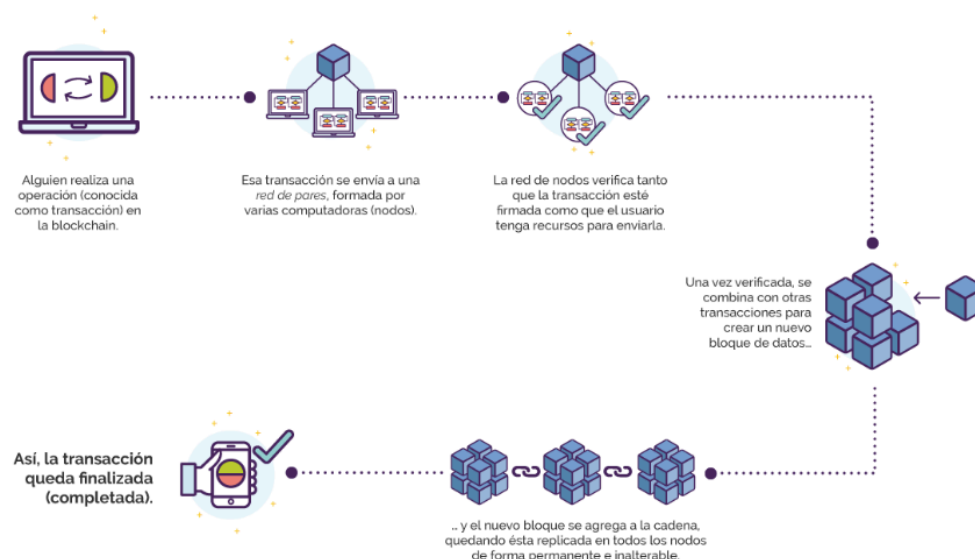


Figura 3.1: proceso simplificado de validación y registro de una transacción en una red blockchain.

2.2 Criptografía

La criptografía es una práctica que consiste en proteger información mediante el uso de algoritmos codificados, hash y firmas. O en otras palabras, se trata de convertir un mensaje de texto plano en un mensaje de texto cifrado.

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

Un hash es un código que se obtiene al procesar información a través de una función. Si modificamos aunque sea algo muy pequeño de esa información, como el color de una foto, o simplemente agregar un acento en un documento de texto, el hash va a cambiar completamente (ver Figura 3.2). Los hash suelen llamarse digestos o resúmenes, porque normalmente tienen un tamaño fijo y de pocos dígitos, por ejemplo 64 caracteres hexadecimales en SHA-256.

Así, al registrar los hash 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, le estamos ofreciendo al público la certeza de que nosotros, responsables de esa foto, no la podremos modificar sin que nadie se entere.

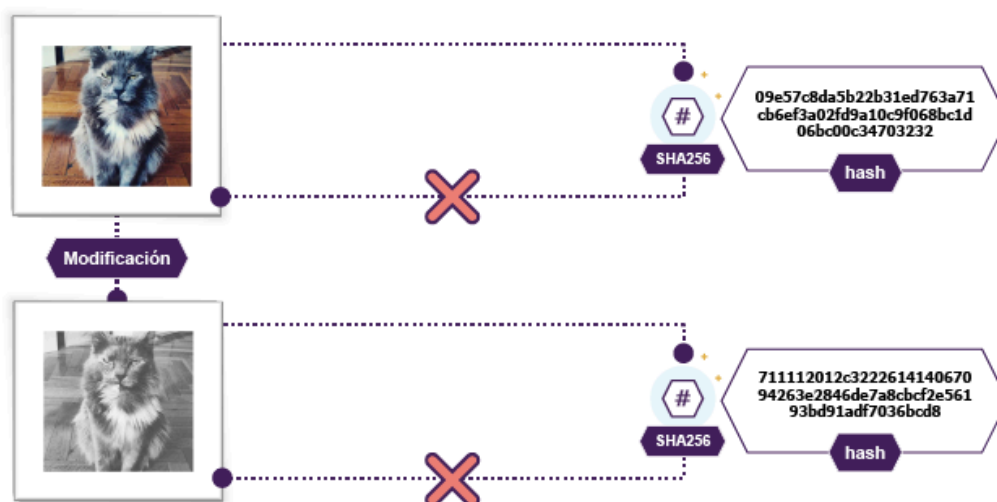


Figura 3.2: un mínimo cambio en una foto produce un cambio completo del hash.

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

2.2.1 Importancia de los hash en Blockchain

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

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

2.3 Blockchain Federal Argentina (BFA)

Es una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre Blockchain.

Una iniciativa confiable y completamente auditable que permita optimizar procesos y funcione como herramienta de empoderamiento para toda la comunidad. Fue concebida dentro de un espacio de trabajo colaborativo, y apunta a reproducir ese patrón como columna vertebral de la plataforma.

Diseñada para potenciarse a través de los aportes de sectores públicos, privados, académicos y de la sociedad civil, BFA opta por una estrategia donde la participación

de toda la comunidad es esencial, desde la ingeniería organizacional hasta el despliegue de la infraestructura.

2.3.1 Modelo sin criptomoneda

Blockchain Federal Argentina está diseñada específicamente para no poseer criptomoneda asociada. El incentivo para participar en BFA es favorecer el desarrollo de servicios e iniciativas basadas en la innovación tecnológica y en un trabajo horizontal entre diversos actores.

Dado esto, no es necesaria la implementación de una moneda virtual para aprovechar las ventajas que proporciona Blockchain. Cuando el objetivo de participar y fortalecer la iniciativa no es la acumulación de criptomonedas, aparece un camino caracterizado por la colaboración en lugar de la competencia.

2.3.2 Modelo liviano

Al no depender del minado de criptomonedas y del esfuerzo por obtener una recompensa, no se hace necesario contar con gran cantidad de computadoras a disposición de la resolución de algoritmos complejos, con el gasto de energía que eso conlleva.

Por ello, se habilita la implementación de mecanismos de consenso eficientes, tanto en lo relativo a cantidad de transacciones por unidad de tiempo como en el consumo eléctrico. En este sentido, BFA necesita de muchos menos recursos que una Blockchain tradicional basada en Prueba de Trabajo.

Todo esto se traduce en una Blockchain que funciona de forma permissionada bajo un consenso basado en Prueba de Autoridad; la red se estructura en base a un conjunto confiable, una determinada cantidad de nodos selladores a partir del consenso de las partes que integran BFA y respaldados por la infraestructura de las instituciones, empresas u organismos responsables de cada uno de ellos. Así, el procesamiento no se basa en un conjunto de mineros anónimos compitiendo por la creación de un bloque, sino en la cooperación entre aquellos que representan a distintos sectores.

2.3.3 Transacciones gratuitas

Las transacciones realizadas sobre Blockchain Federal Argentina no tienen costo. Al no poseer una criptomoneda asociada, y estructurar la red bajo el modelo de Prueba de Autoridad con un costo de infraestructura marginal, las transacciones en BFA son gratuitas. El “combustible” necesario para realizarlas será provisto, sin ningún costo asociado, por Blockchain Federal Argentina.

2.3.4 Almacenamiento Off-Chain

En BFA no se almacenan documentos o archivos dentro de la Blockchain, solo se guardan los hash de esos documentos.

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

2.3.5 Software libre

El software de Blockchain Federal Argentina se basa en una implementación abierta y robusta. Todos los desarrollos y modificaciones que se realicen serán igualmente abiertos, de modo que puedan ser públicamente auditados por cualquier interesado, más allá de los participantes del consorcio. La transparencia inherente en el modelo queda también garantizada desde el código.

2.3.6 Tecnología Ethereum

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

Como el desarrollo está basado en código abierto, toda la comunidad puede participar en las pruebas de concepto existentes para mejorar la plataforma, o tomar todo ese trabajo y adaptarlo a otros contextos y necesidades. Blockchain Federal Argentina toma el software de Ethereum, utilizando Prueba de Autoridad y sin criptomoneda asociada.

2.3.7 Monitoreo

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

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

2.3.8 Sello de tiempo

Existen modos de certificar contenidos a través de Blockchain. Estos mecanismos permiten generar una “prueba de existencia”, algo así como un sello digital que demuestra que un mensaje existió en una fecha y hora determinada. BFA ofrece su propio servicio de TSA (*Time Stamping Authority*), que permite demostrar o evidenciar que un determinado archivo digital se ha mantenido inalterado en el tiempo a partir de una determinada fecha (ver Figura 3.3).

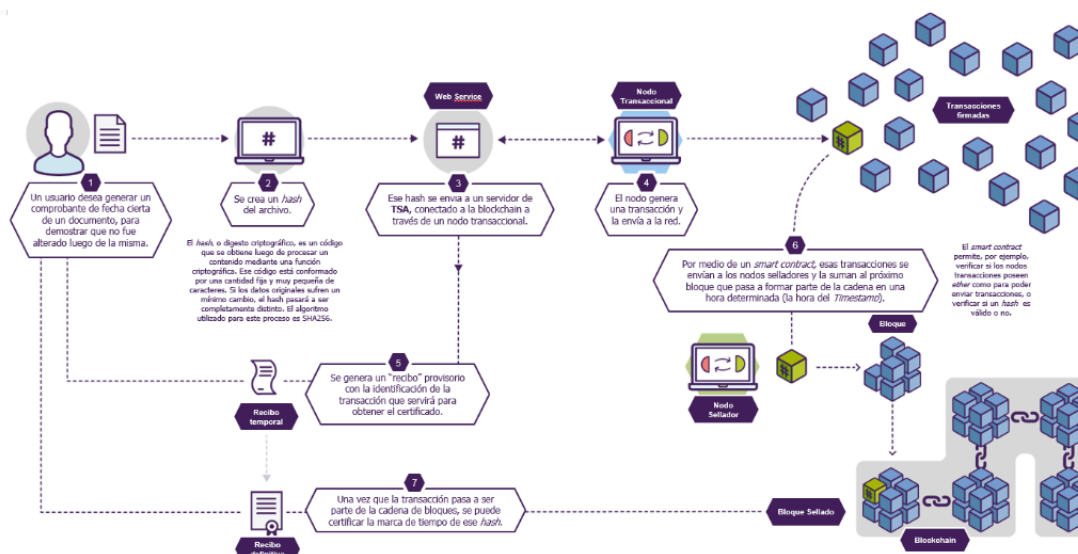


Figura 3.3: proceso de sellado de archivos en la Blockchain mediante TSA.

2.3.9 Destilería de Gas

Para enviar transacciones a la Blockchain se necesita un “combustible” o “gas” llamado Ether, que BFA distribuye a aquellos operadores registrados de nodos transaccionales que desplieguen aplicaciones sobre la plataforma.

El Ether no tiene ningún tipo de valor económico y se envía periódicamente mediante un espacio operado por la organización llamado Destilería. Así, se implementa un modelo donde se evita la especulación y/o el tráfico de gas: 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 (ver Figura 3.4).

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

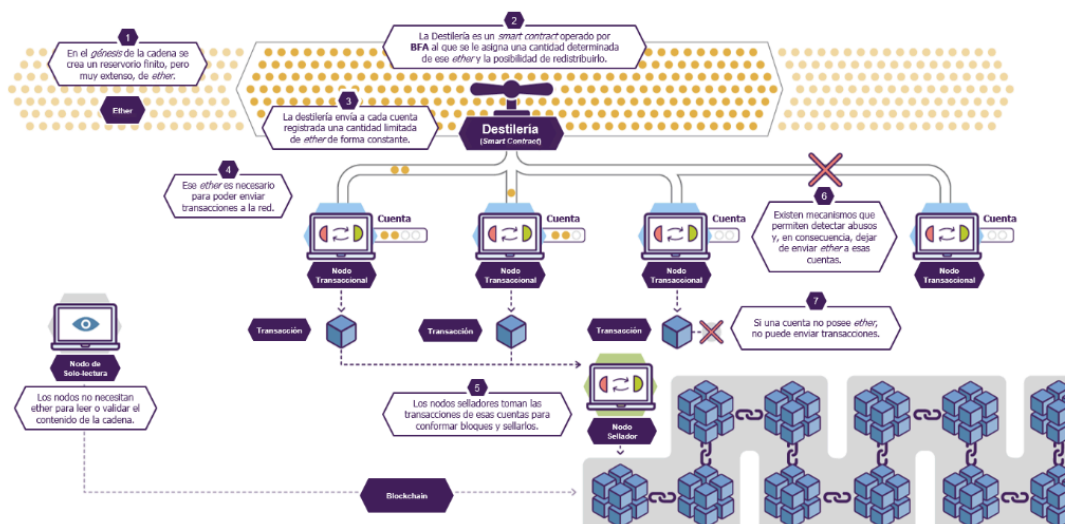


Figura 3.4: distribución automatizada de gas para operaciones en la red BFA.

2.3.10 Plataforma y Aplicaciones sobre BFA

La utilización de la Blockchain Federal Argentina es pública. Las organizaciones que deseen desarrollar servicios y/o aplicaciones sobre la Blockchain sólo deberán aceptar un acuerdo de utilización y buenas prácticas, pero no estarán obligados a desplegar nodos selladores.

BFA se encargará de la infraestructura mientras que los usuarios desarrollarán las aplicaciones.

2.3.11 Nodos

La red está integrada por distintos tipos de nodos:

- Los nodos selladores conforman la estructura central de la red confiable de BFA ya que son los únicos que pueden sellar (agregar) bloques a la cadena. Todos ellos están desplegados por miembros del consorcio. 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 procesadas por los nodos selladores. Usualmente son ejecutados por operadores de servicios que utilizan la Blockchain (los que implementan aplicaciones).
- Existen también nodos verificadores que pueden "ver" la Blockchain, pero no pueden generar ni sellar transacciones. Cualquier usuario puede correr este tipo de nodos, sin necesidad de autorización de BFA.

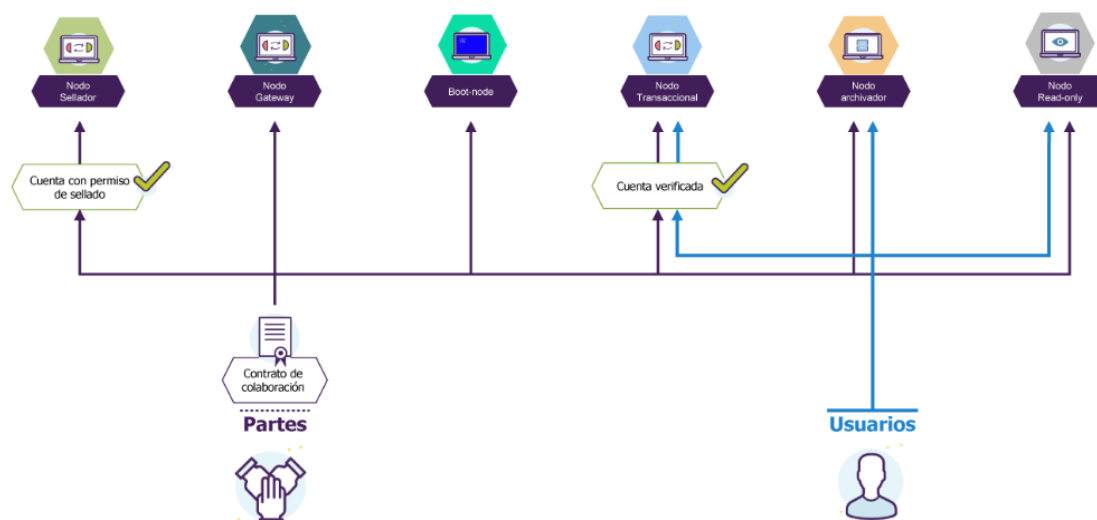


Figura 3.5: quienes pueden instalar los diferentes tipos de nodo de la BFA.

2.4 Docker

Es una plataforma de código abierto que permite crear, desplegar y ejecutar aplicaciones dentro de contenedores. Los contenedores son entornos ligeros, portátiles y consistentes que contienen todo lo necesario para ejecutar una aplicación, incluyendo su código, bibliotecas, dependencias y configuraciones. Esto garantiza que las aplicaciones se ejecuten de manera uniforme en cualquier sistema, independientemente de las diferencias en los entornos de desarrollo, prueba o producción.

Principales características de Docker:

- Portabilidad: los contenedores se pueden ejecutar en cualquier sistema operativo que soporte Docker, ya sea localmente o en la nube.
- Eficiencia: los contenedores son más livianos que las máquinas virtuales, ya que comparten el mismo kernel del sistema operativo.
- Aislamiento: cada contenedor opera de forma independiente, lo que garantiza que no haya conflictos entre aplicaciones.
- Rapidez: el despliegue de aplicaciones con Docker es más rápido en comparación con otros métodos tradicionales.

Docker facilita la implementación y administración de nodos Blockchain, ya que simplifica la configuración y el despliegue en diferentes entornos sin preocuparse por incompatibilidades.

2.5 Acceso ssh

Es un protocolo de comunicación seguro que permite la administración remota de servidores y sistemas. SSH utiliza criptografía para cifrar la conexión, asegurando la

confidencialidad e integridad de los datos transmitidos entre el cliente y el servidor remoto.

Características clave:

- Seguridad: utiliza claves criptográficas para autenticar al usuario y establecer una conexión segura.
- Control remoto: permite gestionar servidores y nodos desde cualquier lugar, siempre que se tenga acceso a las credenciales y permisos necesarios.
- Transferencia de archivos: SSH también permite transferir archivos de manera segura mediante herramientas como SCP (Secure Copy Protocol) o SFTP (Secure File Transfer Protocol).
- Túneles seguros: facilita el acceso a recursos de una red privada a través de un túnel encriptado.

El acceso SSH es fundamental para configurar, monitorizar y mantener nodos de Blockchain cuando se implementan en servidores remotos o en la nube.

2.6 Amazon Web Services (AWS)

Es una plataforma de servicios de computación en la nube proporcionada por Amazon. Ofrece una amplia gama de servicios como almacenamiento, bases de datos, redes, herramientas de desarrollo, y soluciones específicas como Amazon Managed Blockchain (AMB) para crear y gestionar redes Blockchain.

Servicios clave de AWS:

- Computación (EC2): servidores virtuales que permiten ejecutar aplicaciones en la nube.
- Almacenamiento (S3): almacenamiento escalable para datos estructurados y no estructurados.
- Redes: servicios como Amazon VPC que permiten crear redes privadas en la nube.
- Gestión de Blockchain (AMB): permite implementar redes Blockchain escalables utilizando frameworks como Hyperledger Fabric o Ethereum.

Ventajas:

- Escalabilidad: los recursos se pueden ajustar según las necesidades del proyecto.
- Almacenamiento dinámico: posibilidad de ampliar el espacio en disco sin interrupciones, ideal para nodos blockchain cuyo tamaño crece constantemente.
- Flexibilidad: compatible con múltiples herramientas y sistemas operativos.
- Costos bajos: pago por uso, evitando inversiones iniciales altas.
- Fiabilidad: infraestructura global y redundante para garantizar alta disponibilidad.

2.7 Testnet

Es una versión alternativa de una Blockchain diseñada específicamente para el desarrollo y prueba de aplicaciones, contratos inteligentes y otras funcionalidades sin afectar la red principal o mainnet. En este entorno, los desarrolladores pueden experimentar, identificar errores y optimizar sus soluciones de manera segura, utilizando criptomonedas sin valor real para simular transacciones y operaciones.

El propósito principal de una testnet es proporcionar un entorno controlado donde se puedan realizar pruebas exhaustivas sin riesgos financieros ni repercusiones en la red principal. Esto permite a los desarrolladores y usuarios:

- Evaluar nuevas funcionalidades: probar actualizaciones o cambios en el protocolo antes de su implementación en la mainnet.
- Desarrollar y depurar contratos inteligentes: asegurar que los contratos funcionen correctamente antes de su despliegue oficial.
- Formación y educación: permitir a los nuevos usuarios y desarrolladores familiarizarse con la tecnología Blockchain sin riesgos.

Dentro de una testnet, los nodos de prueba juegan un papel crucial. Estos nodos son instancias de la Blockchain que participan en la validación y propagación de transacciones y bloques dentro de la red de prueba. Su función principal es:

- Validar transacciones: asegurar que las operaciones realizadas en la testnet sean correctas y sigan las reglas del protocolo.
- Propagar información: distribuir transacciones y bloques a otros nodos de la red para mantener la coherencia y sincronización.
- Simular condiciones de la mainnet: ayudar a replicar el comportamiento de la red principal, permitiendo pruebas más realistas.

En el contexto de la Blockchain Federal Argentina (BFA), la implementación de una testnet permite a las instituciones y desarrolladores locales experimentar con la tecnología Blockchain, adaptándola a sus necesidades específicas y asegurando que las soluciones propuestas sean eficientes y seguras antes de su adopción en entornos de producción.

2.8 Contratos Inteligentes (*Smart Contracts*)

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

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

Gracias a ellos 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.

En resumen, la implementación del nodo de prueba aprovecha la inmutabilidad, descentralización y transparencia de Blockchain. Estas propiedades garantizan que las transacciones realizadas sean seguras, auditables y sin posibilidad de alteraciones, lo que es fundamental para generar confianza en el entorno académico.

La BFA, como red permissionada, utiliza un modelo de consenso basado en Prueba de Autoridad (*Proof of Authority*), que reduce los requisitos de infraestructura y simplifica la participación. Esto facilita la integración del nodo de prueba de la UNT, ya que no se necesita una gran cantidad de recursos, ni se manejan criptomonedas, lo que la hace accesible y eficiente.

Los hash criptográficos juegan un rol esencial en la seguridad del nodo de prueba, permitiendo verificar la integridad de los datos y garantizar su inmutabilidad. Además, el modelo de almacenamiento off-chain de la BFA utiliza hashes para proteger los documentos sin sobrecargar la red, lo que será probado en las transacciones desde el nodo.

La compatibilidad de la BFA con contratos inteligentes abre la posibilidad de implementar aplicaciones futuras en la UNT, como la gestión de títulos académicos o trámites administrativos automatizados. Esto se evaluará en el análisis de factibilidad.

El diseño de la BFA elimina la necesidad de criptomonedas, permitiendo realizar transacciones gratuitas y simplificando la operatividad del nodo. Esto es clave para la evaluación del impacto y sostenibilidad de la integración futura de la UNT.

El nodo de prueba actúa como un nodo transaccional, encargado de enviar información a los nodos selladores para su validación y registro. Esto permite probar la conectividad, integración y funcionamiento dentro de la red de la BFA.

La configuración del nodo se beneficia del uso de Docker, que asegura portabilidad y consistencia en el entorno de prueba, y de AWS, que ofrece una infraestructura flexible para el despliegue, pruebas y ajustes sin depender de recursos físicos adicionales.

La testnet proporciona un entorno controlado donde el nodo de prueba interactúa con otros nodos para simular operaciones reales sin riesgos. Esto permitirá evaluar la viabilidad técnica y operativa del nodo antes de su posible migración a la red principal.

La responsabilidad de monitorear y mantener el nodo recae en la UNT. Este aspecto será clave para evaluar la capacidad técnica de la institución y los recursos necesarios para sostener un nodo activo en la BFA.

En conjunto, estos conceptos permiten diseñar, configurar y probar un nodo de prueba

que se ajuste a los estándares de la BFA, mientras se documenta el proceso y se evalúan los beneficios y desafíos de una integración completa. Este proyecto representa un paso inicial hacia el uso de Blockchain como herramienta innovadora para mejorar los procesos administrativos y académicos en la UNT.

3 - Especificación de Requisitos:

3.1 Requisitos Funcionales

1. Configuración del Nodo de Prueba:
 - El nodo debe conectarse a la testnet de la BFA.
 - El nodo debe estar constantemente sincronizado con el resto de nodos de la red.
 - Debe permitir el envío de transacciones a través de la red.
2. Intercambio de Información:
 - Validar la propagación de transacciones en la red y su registro en los bloques.
3. Almacenamiento Off-Chain:
 - Implementar el almacenamiento de los hash de documentos en la Blockchain.
 - Garantizar que los documentos originales permanezcan fuera de la cadena.
4. Monitoreo:
 - Registrar métricas clave del nodo, como tiempos de respuesta, transacciones procesadas y estado de conectividad.
5. Pruebas y Validaciones:
 - Realizar pruebas controladas de conectividad y rendimiento en el entorno de prueba.

3.2 Requisitos No Funcionales

1. Seguridad:
 - Garantizar el acceso seguro al nodo mediante SSH con autenticación basada en claves.
2. Escalabilidad:
 - Asegurar que el diseño del nodo permita futuras ampliaciones para una integración completa en la red principal.
 - Configurar Docker para garantizar la portabilidad y replicación del nodo en diferentes entornos.
3. Fiabilidad:
 - Implementar redundancia básica para evitar interrupciones de la comunicación con la red de bloques.
 - Asegurar que las pruebas realizadas en la testnet simulen condiciones reales de operación.
4. Usabilidad:
 - Proveer documentación detallada sobre la configuración y operación del nodo.
 - Diseñar el nodo para que sea fácilmente administrable por personal técnico de la UNT.
5. Eficiencia:

- Optimizar el consumo de recursos del nodo para operar de forma eficiente en una máquina virtual o infraestructura en la nube (AWS).
- Configurar el entorno Docker para minimizar el tiempo de despliegue y reinicio del nodo.

3.3 Requisitos Técnicos

1. Hardware y Recursos Computacionales:

- Procesador: 2 vCPU.
- RAM: 4 GB.
- Almacenamiento: 50 GB.
- Máquina virtual en AWS.

2. Software:

- Sistema Operativo: linux.
- Git para clonar repositorios.
- Docker y Docker Compose para el despliegue del nodo.

3. Red:

- Conexión estable a Internet con al menos 10 Mbps.
- Acceso a puertos específicos para comunicación con la red BFA, para acceso ssh y para el servicio de API:
 - Puerto 30303: permite la comunicación entre nodos
 - Puerto 8545: para las consultas JSON-RPC a través del protocolo HTTP, útil para interacciones puntuales.
 - Puerto 8546: para consultas JSON-RPC mediante WebSocket, permitiendo una conexión persistente con el nodo
 - Puerto 3000: para el servicio de *Time Stamping Authority* (TSA)
 - Puerto 22: para el acceso ssh

3.4 Requisitos de Documentación

1. Manual Técnico:

- Instrucciones para la configuración del nodo.
- Detalles sobre las dependencias y software necesarios.
- Proceso para ejecutar pruebas de conectividad y transacciones.

2. Reportes de Pruebas:

- Registro de transacciones realizadas durante las pruebas.
- Desempeño del nodo bajo diferentes condiciones.

3. Análisis de Factibilidad:

- Beneficios de la integración completa de la UNT en la BFA.
- Desafíos técnicos, administrativos y operativos identificados durante las pruebas.

4. Recomendaciones:

- Instrucciones para una futura integración completa.
- Recursos adicionales necesarios para garantizar la sostenibilidad del nodo.

4 - Documentación

Este capítulo tiene como objetivo documentar en detalle el proceso técnico de instalación, configuración y pruebas realizadas sobre el nodo de prueba implementado en la red de testnet de la Blockchain Federal Argentina (BFA). Se presentan tanto los pasos para su despliegue en un entorno de infraestructura virtualizado con AWS y Docker, como las pruebas funcionales llevadas a cabo para validar su correcto funcionamiento. La documentación incluye guías prácticas, análisis de desempeño, factibilidad y recomendaciones orientadas a una futura integración completa de la universidad a la red BFA, buscando facilitar la replicabilidad de esta experiencia en otros entornos académicos o institucionales.

4.1 Infraestructura del nodo y conexión con la BFA

4.1.1 Esquema de infraestructura del nodo de la UNT

La siguiente figura (ver Figura 4.1) muestra la arquitectura general del nodo de prueba desplegado en la nube de Amazon Web Services (AWS). Dentro de una instancia virtual (VM) ubicada en la VPC (*Virtual Private Cloud*) de la UNT, se ejecuta un sistema operativo Amazon Linux sobre el cual corre el motor de contenedores Docker. Dentro de este entorno se alojan los servicios necesarios para operar el nodo de prueba, incluyendo el nodo de la BFA y el servicio de sellado temporal TSA.

Este diagrama permite visualizar claramente la disposición de los componentes técnicos, su encapsulamiento dentro de contenedores, y la forma en que la infraestructura está organizada para garantizar estabilidad, portabilidad y escalabilidad.

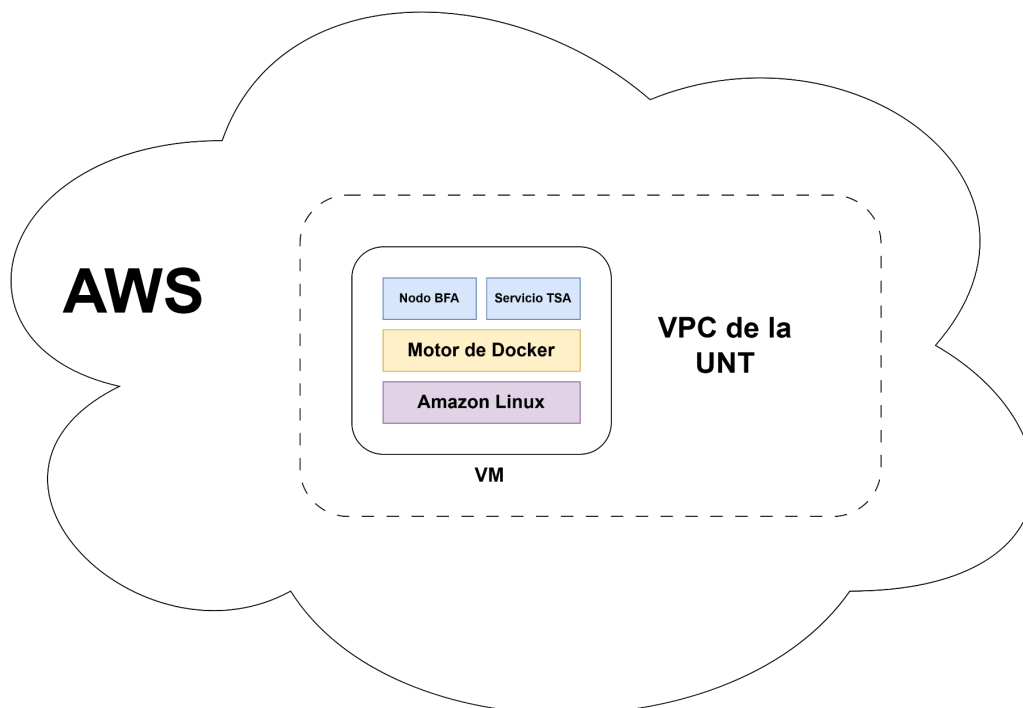


Figura 4.1: infraestructura del nodo BFA en AWS, desplegado en una VM dentro de la VPC de la UNT.

La siguiente figura (ver Figura 4.2) ilustra cómo se establece la comunicación entre los distintos componentes del sistema: el usuario accede al servicio TSA, que a su vez interactúa con el nodo BFA para operar sobre la red. Este nodo se comunica con el resto de los nodos de la blockchain a través del puerto correspondiente, garantizando la sincronización y participación en la red distribuida.

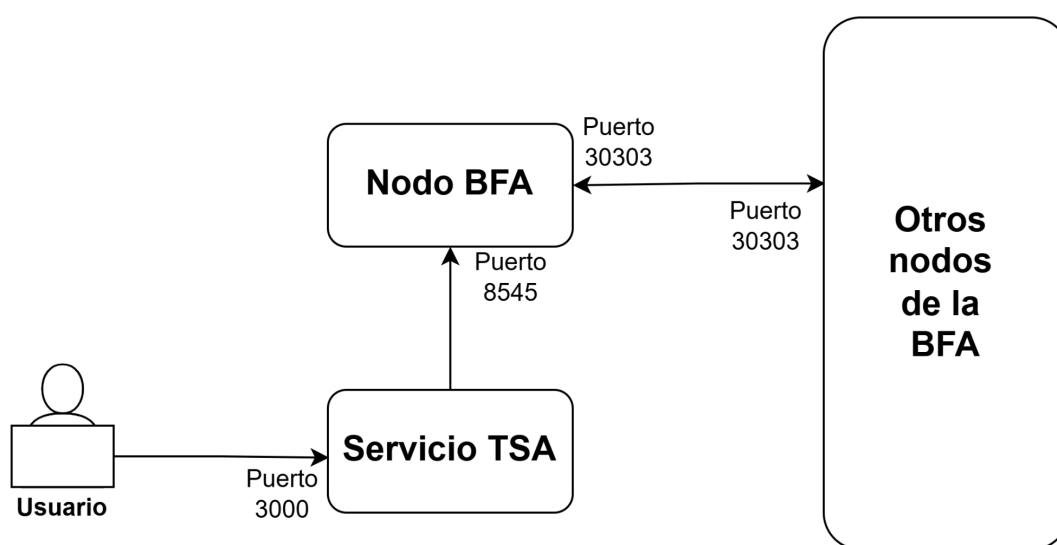


Figura 4.2: flujo de comunicación entre el usuario, el servicio TSA, el nodo BFA y el resto de los nodos de la red.

Esta arquitectura está diseñada para separar claramente tres capas fundamentales:

- Capa de exposición (puerto 3000): donde el usuario final interactúa a través de una interfaz que se comunica con el servicio TSA.
- Capa de acceso a la blockchain (puerto 8545): donde el servicio TSA se conecta con el nodo BFA mediante el protocolo JSON-RPC, utilizado para enviar transacciones o consultar información.
- Capa de red entre nodos (puerto 30303): que permite al nodo BFA sincronizarse y comunicarse de manera distribuida con el resto de los nodos de la red BFA, utilizando conexiones peer-to-peer (P2P).

Los servicios están encapsulados en contenedores y cada uno expone los puertos necesarios para su funcionamiento, garantizando un diseño modular y seguro. Esta organización permite una interacción controlada y eficiente con la red blockchain, facilitando tanto el acceso del usuario como la integración con la red descentralizada.

4.2 Manual técnico

4.2.1 Instrucciones para la configuración del nodo en la testnet

1 - Acceso a una máquina virtual con los recursos de hardware especificados anteriormente.

Acceder a una máquina virtual previamente configurada con los recursos de hardware recomendados para el funcionamiento del nodo, incluyendo CPU, memoria RAM y almacenamiento adecuado para su ejecución continua.

2 - Instalación de Git.

Instalar la herramienta Git, necesaria para clonar los repositorios necesarios.

3 - Instalación de Docker y Docker compose.

Para facilitar el despliegue del nodo, se utilizaron tecnologías de virtualización ligera como Docker y Docker Compose. Docker permite encapsular aplicaciones y sus dependencias en contenedores, asegurando un entorno controlado y reproducible, mientras que Docker Compose facilita la orquestación de múltiples contenedores a través de un único archivo de configuración.

La instalación se realiza siguiendo la documentación oficial de Docker, asegurando la compatibilidad con el sistema operativo de la máquina virtual. Una vez instaladas ambas herramientas, se verifica su correcto funcionamiento mediante los comandos:

```
docker --version  
docker-compose --version
```

Estas herramientas resultan esenciales para levantar el nodo de forma rápida y estandarizada, tal como lo propone la arquitectura de la Blockchain Federal Argentina en su red de testnet.

4 - Creación del archivo docker-compose.yml.

El mismo define los servicios, redes y volúmenes requeridos para la ejecución del nodo. Tiene como contenido lo siguiente:

```
version: "3.8"

services:
  bfanodo:
    image: bfaar/nodo:test
    container_name: container-bfanodo-testnet
    restart: always
    ports:
      - 8545:8545
      - 8546:8546
      - 30303:30303

    volumes:
      - lvm_device_test01:/home/bfa/bfa/network/node/
      - bfa_vol_test:/home/bfa

volumes:
  bfa_vol_test:
  lvm_device_test01:
```

5 - Despliegue del contenedor del nodo.

Con el archivo docker-compose.yml ya creado, y las herramientas necesarias instaladas, se procede a levantar el contenedor del nodo de la BFA.

Se ejecuta el siguiente comando:

```
docker-compose up -d
```

Este comando descarga las imágenes necesarias, crea los contenedores y los ejecuta en segundo plano. Una vez levantado el nodo, se verifica su estado mediante:

```
docker ps
```

Este paso marca el inicio de la ejecución efectiva del nodo en la red de prueba de la BFA, permitiendo su conexión con otros nodos y la participación en la validación de transacciones dentro del entorno.

6 - Sincronización de la red.

Una vez levantado el contenedor del nodo, el siguiente paso consiste en la sincronización con la red de prueba de la Blockchain Federal Argentina (BFA). Durante este proceso, el nodo comienza a descargar todos los bloques existentes en la testnet, actualizando su estado hasta alcanzar el último bloque válido.

Este proceso es automático, pero demora varias horas dependiendo de la velocidad de conexión y el rendimiento de la máquina virtual utilizada. En el entorno de prueba de este proyecto, la sincronización inicial tomó aproximadamente seis horas.

Durante este tiempo, se monitorean los logs del contenedor con el siguiente comando para asegurar que el proceso se esté desarrollando correctamente:

```
docker logs -f nodo_bfa
```

Solo una vez completada esta sincronización, el nodo queda plenamente operativo dentro de la red, permitiendo la ejecución de pruebas y la interacción con otros nodos.

7 - Creación de una cuenta (dirección) en la Blockchain.

Para interactuar con la red y realizar operaciones como el sellado de archivos o pruebas de otros contratos inteligentes, es necesario contar con una cuenta válida dentro de la Blockchain. Esta cuenta o dirección actúa como una identidad digital dentro de la red.

Ingresar a la terminal del contenedor con el comando:

```
sudo docker exec -it --user root id_del_contenedor bash
```

Luego acceder a la consola del nodo y ejecutar el comando:

```
attach.sh
```

Dentro de la consola, crear una cuenta nueva ejecutando:

```
personal.newAccount()
```

Este comando genera un nuevo par de claves (pública y privada) y crea una dirección asociada. Durante el proceso, se solicita establecer una contraseña para proteger la clave privada. Es fundamental conservar esta contraseña y realizar una copia segura del archivo keystore generado, ya que serán necesarios para firmar transacciones y acceder a la cuenta en el futuro.

Una vez creada, la dirección puede ser utilizada para recibir fondos de prueba y participar en actividades dentro de la testnet de la BFA.

8 - Solicitud de ether necesario para realizar transacciones (gas).

Para que una cuenta pueda ejecutar transacciones dentro de la red de prueba, es necesario contar con un saldo mínimo en ether (ETH) de testnet, que se utiliza como gas para cubrir los costos computacionales de las operaciones.

En el caso de la testnet de la Blockchain Federal Argentina, la forma de obtener estos fondos de prueba es a través de un canal oficial en Telegram, donde los desarrolladores pueden solicitar ETH de manera gratuita.

El proceso consiste en enviar la dirección generada en el paso anterior al grupo designado de la BFA en Telegram. Una vez aprobada la solicitud, se recibe una transferencia con la cantidad necesaria para ejecutar pruebas dentro del nodo.

Esta recarga permite realizar acciones como el sellado de archivos, el despliegue o interacción con contratos inteligentes, y otras pruebas dentro del entorno de la red.

9 - Desbloqueo de la cuenta.

Para firmar transacciones desde la cuenta creada, es necesario desbloquear la cuenta ya que por defecto no se permite el gasto de ETH. La configuración inicial del nodo no permite realizar dicho desbloqueo.

Para lograr el desbloqueo, es necesario modificar el script de inicio del contenedor. Este script se llama `singlestart.sh` y está ubicado en la ruta `/home/bfa/bfa/bin` (dentro del contenedor). Se debe editar con un editor de texto y realizar el cambio correspondiente en la línea 75, que originalmente contiene:

```
geth --config ${BFATOML} $* &
```

Y reemplazarse por:

```
geth --config ${BFATOML} --allow-insecure-unlock $* &
```

Finalmente, se debe reiniciar el contenedor para que los cambios tengan efecto.

Una vez configurado el nodo se realizan los siguientes pasos:

1 - Clonación del repositorio del servicio de la API TSA 2.

Para realizar pruebas de sellado de archivos en la red de prueba de la BFA, se utiliza el servicio TSA (*Time Stamping Authority*) versión 2, que expone una API REST sobre la infraestructura de Blockchain.

El primer paso consiste en clonar el repositorio correspondiente al servicio TSA 2, el cual se encuentra disponible públicamente y fue citado en la bibliografía del presente trabajo. Este repositorio contiene el código fuente del servicio y ejemplos de cómo utilizarlo para emitir sellos de tiempo basados en Blockchain.

Desde la terminal, se ejecuta el siguiente comando para obtener el código:

```
git clone https://github.com/mauriciobardin/API-TSA-2.git
```

Una vez clonado, se accede al directorio del proyecto para revisar la documentación incluida y configurar el entorno necesario para ejecutar la API localmente o interactuar con una instancia ya desplegada.

2 - Despliegue del servicio de la API TSA 2.

Con el repositorio clonado localmente, el siguiente paso es levantar el servicio TSA 2 para realizar pruebas de interacción con la Blockchain. Este servicio se encuentra preparado para ejecutarse mediante Docker, lo cual simplifica el proceso de configuración y despliegue.

Desde la raíz del proyecto, se ejecuta el siguiente comando para construir y levantar los contenedores definidos en el archivo docker-compose.yml:

```
docker-compose up -d
```

Este comando inicializa los servicios necesarios para que la API funcione correctamente.

3 - Búsqueda del archivo de keystore.

Acceder al contenedor del nodo e ir al directorio:

```
/home/bfa/bfa/test2network/node/keystore
```

En este directorio se encuentra el archivo correspondiente a la cuenta creada. El nombre del archivo sigue el siguiente formato:

UTC--{fecha creación}--{dirección de cuenta}

Por ejemplo:

```
UTC--2025-02-27T18-24-45.734065152Z--6368e4d952a80115e2a4d07c0cb8dea34ef  
f02f6
```

4 - Almacenamiento del archivo de keystore dentro de la carpeta “api” de la TSA 2.

Este archivo es necesario para que el servicio de la API pueda desbloquear la cuenta y realizar correctamente las operaciones de sellado de tiempo. El archivo contiene la clave privada cifrada asociada a la dirección utilizada para firmar las transacciones.

5 - Configuración del archivo.env con las variables de entorno.

```
GETH_ACCOUNT_JSON=  
#Es la direccion del archivo keystore, por ejemplo:  
#GETH_ACCOUNT_JSON=./UTC--2025-03-18T19-23-28.858636054Z--c948546  
2223c0a916465772d112c46603b64c790  
  
GETH_ACCOUNT_PASSWORD=  
GETH_HOST=  
# Es la direccion de ip del nodo, por ejemplo  
# GETH_HOST=http://localhost:8545  
CONTRACT_ABI_PATH=./abi.json  
CONTRACT_ADDRESS=0xFc0f01A88bD08b988173A2354952087C9492d947  
node dist/index.js
```

Desde este punto, el servicio queda disponible para realizar pruebas de sellado de archivos utilizando herramientas como Postman o scripts personalizados.

4.2.2 Proceso para ejecutar pruebas de conectividad y transacciones

Para verificar la conectividad y funcionalidad del servicio de sellado de tiempo, se pueden utilizar herramientas como Postman o cURL para realizar consultas HTTP a la API.

La prueba consiste en enviar una solicitud con uno o más hash de archivos que se desean sellar. Este hash puede generarse utilizando cualquier herramienta o procedimiento confiable, pero es fundamental que el mismo método sea utilizado posteriormente para su verificación. Se recomienda emplear el algoritmo SHA-256 para garantizar integridad y compatibilidad.

La estructura de la solicitud es la siguiente:

```
POST /stamp/ HTTP/1.1
Host: {IP DE LA TSA 2}:3030
Content-Type: application/json

{
  "hashes": ["e2b700c1cb98b7d1506133eeb6d159908c131784880c7ecb1edfe8005c4af5ad"]
}
```

El servidor responde con un objeto JSON con la siguiente estructura:

```
{
  "status": "ok",
  "txHash":
  [
    {
      "hash": "e2b700c1cb98b7d1506133eeb6d159908c131784880c7ecb1edfe8005c4af5ad",
      "block_number": "2540508",
      "status": "stamped"
    }
  ]
}
```

Para verificar si un documento fue sellado y conocer la fecha en la que se realizó el mismo, es necesario generar el hash del archivo utilizando el mismo algoritmo que se usó al momento del registro.

```
GET
/verify/e2b700c1cb98b7d1506133eeb6d159908c131784880c7ecb1edfe8005c4af5ad/
HTTP/1.1
Host: {IP DE LA TSA 2}:3000
```

El servidor responde con un objeto JSON con la siguiente estructura:

```
{
```

```
"stamped": true,  
"stamps":  
[  
  {  
    "whostamped": "0xC9485462223c0a916465772D112c46603b64C790",  
    "blocknumber": "31426381",  
    "block timestamp": 1743714955,  
    "stampdate": "2025-04-03T21:15:55.000Z"  
  }  
]  
}
```

Los campos más interesantes incluidos en la respuesta son los siguientes:

- **block timestamp:** marca temporal del bloque, expresada en segundos desde la época Unix (1 de enero de 1970).
- **stampdate:** fecha y hora del sellado, convertida a formato legible en zona horaria UTC+0.

4.3 Reportes de Pruebas

4.3.1 Registro de transacciones realizadas durante las pruebas

Durante la fase de prueba del nodo de la UNT en la testnet de la Blockchain Federal Argentina (BFA), se llevaron a cabo pruebas funcionales del servicio TSA 2, encargado del sellado de tiempo de archivos. El objetivo fue verificar su correcto funcionamiento, estabilidad y capacidad de respuesta ante solicitudes de sellado y verificación.

Se utilizaron archivos en los cuales se generó el hash correspondiente utilizando el algoritmo SHA-256, y se envió una solicitud HTTP al endpoint de la API TSA 2. Las solicitudes se ejecutaron mediante la herramienta Postman.

El tiempo de respuesta de las solicitudes de sellado varió entre 3,047 y 8,110 segundos, con un promedio general de 5,577 segundos y una mediana de 5,288 segundos, lo cual se considera aceptable para un entorno de prueba (ver Figura 5.1).

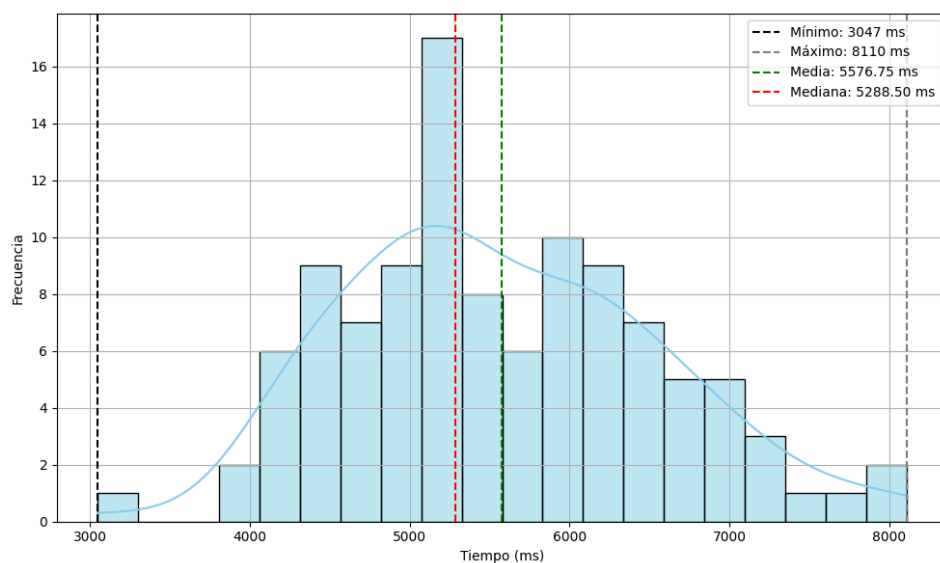


Figura 4.3: histograma de Tiempos de Confirmación de TimeStamp al sellar un único documento

También realizamos el sellado de múltiples hash de forma simultánea. Se observó que las transacciones generadas forman parte de un mismo bloque, y los tiempos de respuesta fueron los siguientes en cada caso:

1- Sellado de 2 hashes de forma simultánea:

El tiempo de respuesta de las solicitudes de sellado varió entre 3,220 y 6,261 segundos, con un promedio general de 5,164 segundos y una mediana de 5,247 segundos, lo cual se considera aceptable para un entorno de prueba (ver Figura 5.2).

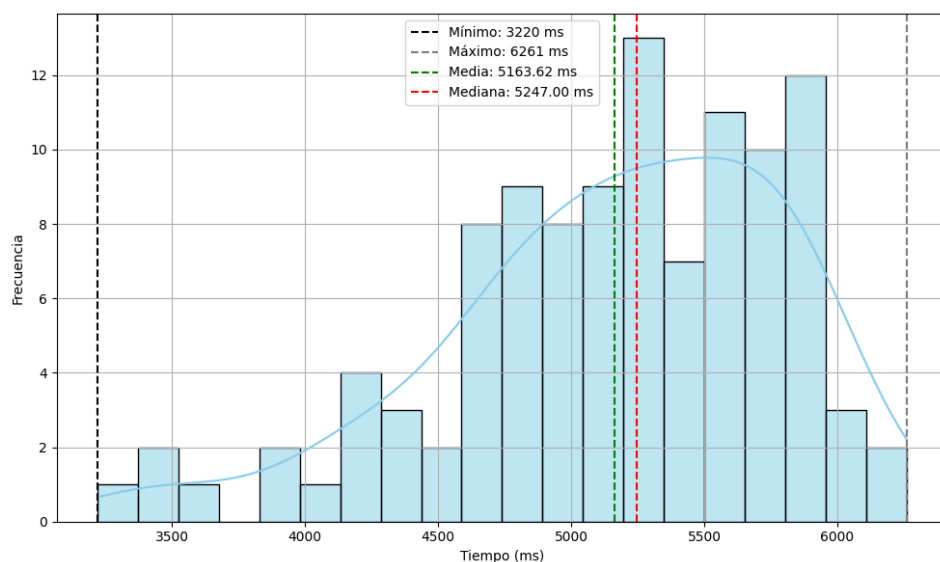


Figura 4.4: histograma de Tiempos de Confirmación de TimeStamp al sellar dos documentos

2- Sellado de 5 hashes de forma simultánea:

El tiempo de respuesta de las solicitudes de sellado varió entre 7,123 y 11,152 segundos, con un promedio general de 9,574 segundos y una mediana de 9,864 segundos, lo cual se considera aceptable para un entorno de prueba (ver Figura 5.3).

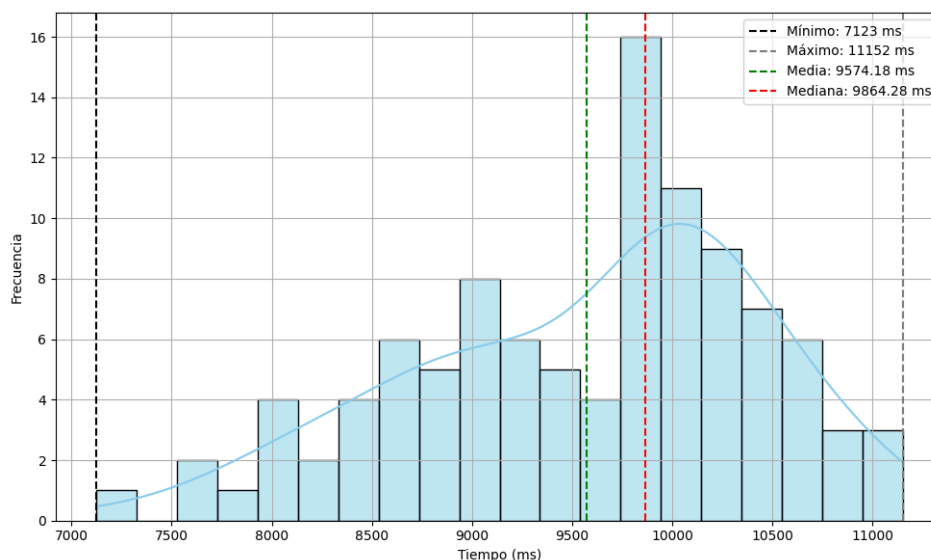


Figura 4.5: histograma de Tiempos de Confirmación de TimeStamp al sellar cinco documentos

3-Sellado de 10 hashes de forma simultánea:

El tiempo de respuesta de las solicitudes de sellado varió entre 6,714 y 12,001 segundos, con un promedio general de 9,533 segundos y una mediana de 9,614 segundos, lo cual se considera aceptable para un entorno de prueba (ver Figura 5.4).

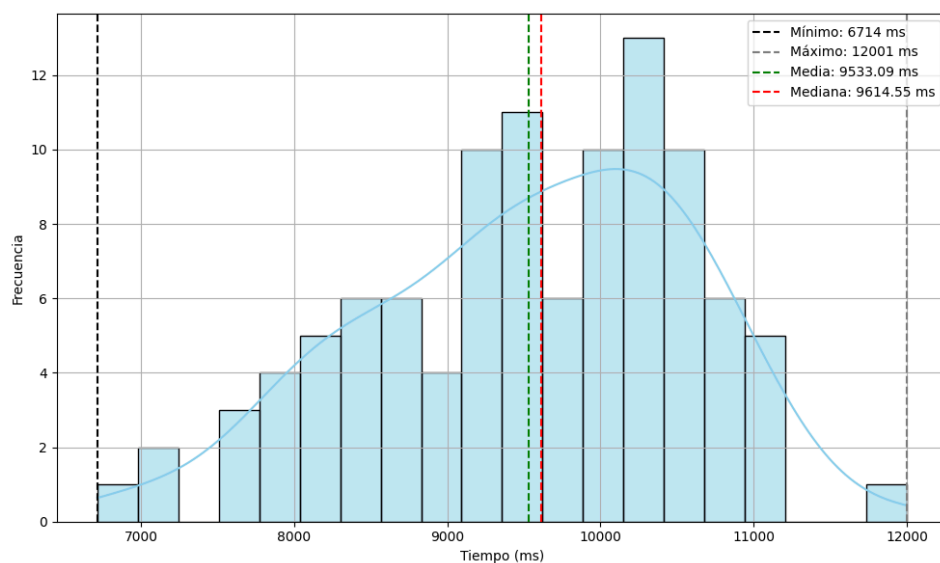


Figura 4.6: histograma de Tiempos de Confirmación de TimeStamp al sellar diez documentos

También se realizaron pruebas de verificación de documentos.

El tiempo de respuesta de las solicitudes de verificación varió entre 0,704 y 0,751 segundos, con un promedio general de 0,715 segundos y una mediana de 0,710 segundos, lo cual se considera aceptable para un entorno de prueba.

4.3.2 Desempeño del nodo bajo diferentes condiciones

Los resultados muestran que el sellado simultáneo de hasta 2 documentos mantiene un desempeño muy similar al sellado individual. Sin embargo, a partir de 5 documentos se incrementa el tiempo de respuesta de forma notable. No obstante, si se considera el tiempo promedio por documento (es decir, el tiempo total dividido por la cantidad de documentos), este resulta más eficiente que realizar sellados individuales (ver Figura 5.5). Este comportamiento resulta alentador para contextos en los que se necesite sellar múltiples documentos a la vez.

A pesar del aumento en el tiempo total, el nodo se mantuvo operativo y respondió correctamente a todas las solicitudes, incluso bajo una carga mayor, lo cual demuestra una buena tolerancia del sistema en escenarios de uso más intensivo.

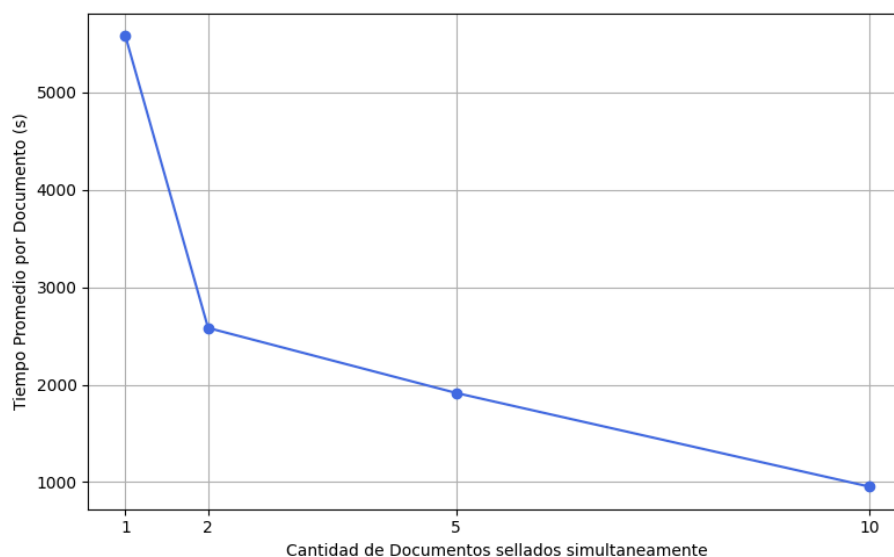


Figura 4.7: tiempo Promedio por Documento vs. Cantidad de Documentos Sellados Simultáneamente

Los resultados de las pruebas de verificación de archivos demostraron que esta operación presenta una latencia baja y estable.

Estas pruebas permitieron validar que el servicio TSA 2 opera de forma estable y segura en el entorno del nodo de prueba, siendo capaz de registrar y verificar sellos de tiempo con rapidez y precisión.

Observaciones:

- El sistema respondió de forma estable y rápida en todos los casos.
- Las pruebas demostraron que el servicio valida correctamente la existencia previa de un hash ya sellado.
- El uso de SHA-256 como algoritmo estándar resultó adecuado para garantizar la integridad de los archivos.

4.4 Análisis de Factibilidad

4.4.1 Beneficios de la integración completa de la UNT en la BFA

La integración completa de la Universidad Nacional de Tucumán (UNT) en la Blockchain Federal Argentina (BFA) presenta una serie de beneficios que pueden transformar positivamente los procesos administrativos, académicos y tecnológicos de la institución. Algunos de los beneficios más relevantes incluyen:

- **Innovación y posicionamiento tecnológico:** ser pionera en la integración con una Blockchain pública federal posiciona a la UNT como una institución innovadora, comprometida con la mejora continua y abierta a nuevas tecnologías que potencien su gestión y sus servicios.
- **Transparencia y trazabilidad:** la adopción de Blockchain permitiría registrar y auditar operaciones en tiempo real, brindando mayor transparencia en la gestión de documentos, contratos, resoluciones y procesos académicos. Cada transacción registrada en la BFA es inmutable y verificable por cualquier nodo autorizado, lo que refuerza la confianza institucional.
- **Seguridad de la información:** el uso de algoritmos criptográficos garantiza la integridad y autenticidad de los datos almacenados. Esto es especialmente importante para la gestión de títulos, actas, certificados académicos y documentos administrativos sensibles.
- **Digitalización y eficiencia operativa:** la integración con la BFA permite automatizar procesos a través de contratos inteligentes, lo que se traduce en mayor eficiencia, reducción de tiempos administrativos y menor uso de papel.
- **Reducción de intermediarios:** al eliminar la necesidad de validaciones manuales o duplicadas entre diferentes áreas de la universidad, se agilizan los procesos y se reduce la posibilidad de errores humanos.

4.4.2 Desafíos técnicos, administrativos y operativos identificados durante las pruebas

Durante el desarrollo e implementación del nodo de prueba en la Universidad Nacional de Tucumán (UNT), se identificaron diversos desafíos que reflejan tanto las complejidades técnicas propias de la tecnología Blockchain como las particularidades del entorno institucional. Estos obstáculos representan áreas clave a considerar para una futura integración completa en la Blockchain Federal Argentina (BFA).

- **Desafíos técnicos:** la configuración inicial del nodo y su conexión con la red de prueba de la BFA implican la adaptación a herramientas y entornos poco conocidos dentro del ámbito universitario. La falta de documentación detallada o casos de uso específicos para instituciones académicas generó una curva de aprendizaje considerable. Asimismo, aspectos como la sincronización de bloques, gestión de claves criptográficas y monitoreo de logs requieren conocimientos específicos en redes distribuidas y seguridad informática que no siempre están disponibles en el personal técnico local.
- **Desafíos administrativos:** la introducción de una tecnología disruptiva como Blockchain en un entorno tradicional presenta resistencias naturales al cambio. La falta de conocimiento general sobre sus beneficios, sumada a la ausencia de normativas internas que contemplen su uso, dificulta la toma de decisiones institucionales. La descentralización, aunque beneficiosa en muchos sentidos, choca con estructuras administrativas centralizadas que aún funcionan bajo

modelos analógicos.

- **Desafíos operativos:** si bien se logró una integración funcional en el entorno de pruebas, todavía se requiere una mayor capacitación del personal, así como la adaptación de procesos ya establecidos para su digitalización efectiva. La ausencia de una interfaz amigable o herramientas visuales para usuarios no técnicos puede desalentar el uso cotidiano de la tecnología, haciendo necesario el desarrollo de aplicaciones específicas orientadas a facilitar la adopción.

A pesar de estos desafíos, se destaca que la tecnología fue recibida con interés por parte de algunos sectores dentro de la universidad. Sin embargo, para fomentar una adopción más amplia es fundamental continuar con acciones de sensibilización, talleres de formación, y generar casos de uso concretos que demuestren el valor real que puede aportar la BFA a las actividades universitarias cotidianas.

4.5 Recomendaciones

4.5.1 Instrucciones para una futura integración completa

Con el fin de evitar redundancias, se omitirán en esta sección aquellos pasos que coincidan con los ya descritos durante la implementación en la red de prueba.

1 - Acceso a una máquina virtual con los recursos de hardware especificados anteriormente

2 - Instalación de Git

3 - Instalación de Docker y Docker compose

4 - Creación del archivo docker-compose.yml

En el caso de un nodo conectado a la red principal, el archivo se encuentra configurado con los siguientes parámetros:

```
version: "3.8"

services:
  bfanodo:
    image: bfaar/nodo:latest
    container_name: container-bfanodo
    restart: always
    ports:
      - 8545:8545
      - 8546:8546
      - 30303:30303
    volumes:
      - lvm_device:/home/bfa
volumes:
  lvm_device:
    driver: local
    driver_opts:
```

```
type: 'device'  
device: '/mnt/data/'  
o: 'bind'
```

5 - Despliegue del contenedor del nodo

6 - Sincronización de la red

7 - Creación de una cuenta (dirección) en la Blockchain

8 - Creación de una cuenta en la BFA y validarla

Para ser parte de BFA se necesita completar y firmar un Formulario de Solicitud de Incorporación, en el cual se acepta el Contrato de Colaboración. Éste debe ir acompañado del Estatuto, Contrato Social u otra forma de documento del cual surja la existencia de la Entidad solicitante (exceptuadas instituciones de la Administración Pública Nacional y gobiernos provinciales) y el acto de designación o personería de quien firma.

Una vez que el nodo se incorpora a la red de la BFA, el proceso denominado Destilería se encarga automáticamente de asignar el gas necesario para realizar transacciones. A diferencia de los nodos en la red de prueba (testnet), no es necesario solicitar gas manualmente a través del grupo de Telegram.

9- Desbloquear la cuenta

Una vez configurado el nodo se realizan los siguientes pasos:

1 - Clonación del repositorio del servicio de la API TSA 2

2 - Despliegue del servicio de la API TSA 2

3 - Búsqueda del archivo de keystore

4 - Almacenamiento del archivo de keystore dentro de la carpeta “api” de la TSA 2

5 - Configuración del archivo.env con las variables de entorno

Las variables necesarias se consiguen de la misma manera, con la diferencia de que la dirección del contrato inteligente es la siguiente:

```
CONTRACT_ADDRESS=0x7e56220069CAaF8367EA42817EA9210296AeC7c6  
node dist/index.js
```

Desde este punto, el servicio queda disponible para realizar pruebas de sellado de archivos utilizando herramientas como Postman o scripts personalizados.

Las consultas HTTP se realizan de la misma forma que en la red de prueba.

4.5.2 Recursos adicionales necesarios para garantizar la sostenibilidad del nodo

Para asegurar la continuidad y evolución del nodo de prueba instalado en la Universidad Nacional de Tucumán (UNT) como parte de la Blockchain Federal Argentina (BFA), se identifican ciertos recursos clave que resultan necesarios para garantizar su sostenibilidad a largo plazo. La permanencia de este nodo no solo depende del éxito técnico inicial, sino también de una estrategia institucional que contemple aspectos humanos, tecnológicos y organizativos.

- **Soporte técnico especializado:** es fundamental contar con personal capacitado de forma continua en tecnologías Blockchain, administración de nodos y seguridad informática. La complejidad técnica de la BFA requiere un equipo capaz de operar el nodo, interpretar los registros del sistema, actualizar componentes y resolver incidentes.
- **Infraestructura estable y escalable:** aunque el nodo de prueba se implementó en un entorno controlado, para su sostenibilidad será necesario asegurar recursos computacionales dedicados, como máquinas virtuales en la nube o servidores con disponibilidad permanente, respaldo eléctrico, conectividad redundante y políticas claras de mantenimiento.
- **Acompañamiento institucional:** la sostenibilidad del nodo también demanda respaldo formal por parte de las autoridades universitarias. Esto implica la incorporación del nodo a los planes estratégicos de digitalización institucional y la articulación con otras áreas (académicas, administrativas, legales) que puedan beneficiarse de su funcionamiento.
- **Capacitación y cultura digital:** la adopción real de Blockchain en una universidad requiere sensibilizar y formar a usuarios no técnicos en el uso de herramientas asociadas, la comprensión del modelo de funcionamiento distribuido, y los beneficios prácticos para su área. Esto incluye desde charlas introductorias hasta la creación de manuales o tutoriales específicos.

En resumen, la sostenibilidad del nodo no depende únicamente de su configuración inicial, sino de una visión integral que lo considere como parte de una infraestructura estratégica, con impacto potencial en la modernización de la gestión universitaria y en la apertura hacia tecnologías emergentes.

5 - Conclusiones

La implementación de un nodo de prueba en la Universidad Nacional de Tucumán como parte de la testnet de la Blockchain Federal Argentina permitió comprender en profundidad el funcionamiento técnico de esta infraestructura, desde la instalación del nodo y la API TSA 2 hasta la ejecución y análisis de pruebas de sellado y verificación de archivos. La experiencia evidenció la factibilidad de integrar servicios descentralizados en el ámbito académico y técnico, resaltando la estabilidad y eficiencia del sistema en un entorno controlado.

Sin embargo, más allá de los aspectos técnicos, este trabajo pone de manifiesto una realidad fundamental: la utilidad de esta infraestructura no reside solamente en su correcto funcionamiento, sino en su adopción efectiva. Si no se promueve el uso activo, la capacitación y el acompañamiento institucional para incorporar estas herramientas en procesos reales, todo el esfuerzo técnico corre el riesgo de quedar subutilizado. La tecnología por sí sola no transforma; necesita una comunidad que la sostenga, la entienda y la impulse.

A nivel personal, este proyecto significó mucho más que cumplir con un requisito académico. Representó una oportunidad para explorar tecnologías emergentes, superar desafíos reales y trabajar en un entorno colaborativo. Más allá del resultado, nos llevamos una experiencia enriquecedora que marca un antes y un después en nuestra formación profesional.

6 - Bibliografía

Blockchain Federal Argentina – Sitio oficial de la BFA, <https://bfa.ar/> consultado a partir del 19 de noviembre de 2024.

Blockchain Federal Argentina – Repositorio público de la BFA. GitLab, <https://gitlab.bfa.ar/public>, consultado el 1 de diciembre de 2024.

Blockchain Federal Argentina – Especificación para una TSA de BFA, <https://docs.google.com/document/d/19PYSiAkInGXLEbSDqWOh-1zSrY4rr20Palr1H8MjaEQ>, consultado el 13 de febrero de 2025.

Greykoda – Nodo y API para Docker [Repositorio GitLab], <https://gitlab.bfa.ar/greykoda/nodo-y-api-para-docker>, consultado el 20 de diciembre de 2024.

TSA2 [Repositorio GitLab], https://gitlab.bfa.ar/renn_um/tsa2, consultado el 6 de abril de 2025.

Building and interacting with a private Ethereum blockchain using Geth CLI, <https://medium.com/coinmonks/building-and-interacting-with-a-private-ethereum-blockchain-using-geth-cli-7f753cd841e7>, consultado el 22 de diciembre de 2024.

Ethereum Stack Exchange – What's the difference between pending block and txpool?, <https://ethereum.stackexchange.com/questions/42598/whats-the-difference-between-pending-block-and-txpool>, consultado el 2 de marzo de 2025.

Blockscout Developer FAQs, <https://docs.blockscout.com/faqs/developer-faqs>, consultado el 3 de marzo de 2025.

Docker Documentatio, <https://docs.docker.com/>, consultado el 10 de diciembre de 2024.

GitLab Documentation, <https://docs.gitlab.com/>, consultado el 1 de diciembre de 2024.

Generador SHA256 en línea, <https://hash.online-convert.com/es/generador-sha256>, consultado el 10 de marzo de 2025.