S15 CDT Ciencia, Docencia y Tecnología

Suplemento CDyT
VOL. 13 | N° 15 | 2023 ISSN 2250-4559

PID 7059

Tecnología Blockchain para aseguramiento de evidencia digital en entornos Forensic Readiness

Javier Díaz [(1)], *Mónica D. Tugnarelli* [(2)], *Mauro F. Fornaroli* [(2)], *Lucas Barboza* [(2)], *Facundo N. Miño* [(2)], *Fabián Pineda* [(2)], *Juan Ignacio Carubia Grieco* [(2)]

Autores: [(1)] Facultad de Informática – Universidad Nacional de La Plata, [(2)] Facultad de Ciencias de la Administración – Universidad Nacional de Entre Ríos. Monseñor Tavella 1424. Concordia. CP (3200). Entre Ríos, Argentina
Contacto: monica.tugnarelli@uner.edu.ar

ARK: http://id.caicyt.gov.ar/ark:/s22504559/uk5xvakex

Resumen

En este proyecto se propuso analizar las prestaciones de la tecnología Blockchain para asegurar la integridad y trazabilidad de la cadena de custodia bajo la metodología Forensic Readiness que, como método preventivo, requiere de estrictas respuestas del entorno tecnológico para resguardar los datos considerados evidencia digital.

La prueba de concepto se realizó sobre la Blockchain Federal Argentina que brinda una plataforma multiservicios abierta y participativa para integrar servicios y aplicaciones basada en Ethereum y, por otra parte, sobre el desarrollo Open Source Hyperledger Fabric que es una red permisionada privada, con acceso restringido y donde la identidad de los participantes es conocida. Estos dos entornos se utilizaron sin criptomoneda asociada.

Como resultados se ha logrado una comparación de las mismas en cuanto a su perfomance, la respuesta de los algoritmos de consenso, la escalabilidad y la identificación de incidentes de seguridad relacionados con esta tecnología, así como un bosquejo del procedimiento de resguardo de evidencia.

Palabra claves: Forensic Readiness, Blockchain, cadena de custodia, BFA, Hyperledger

Introducción

Blockchain puede describirse como una base de datos distribuida y organizada bajo una estructura de conjunto de bloques que se van encadenando entre sí mediante dos códigos hash que actúan como enlaces: uno para el bloque de datos creado anteriormente y otro para que se comparta y grabe en el bloque que se cree a continuación, de forma tal de obtener una lista enlazada o cadena de bloques. Cada bloque que se encadena se vuelve inmutable y en eso radica la fortaleza de seguridad y verificabilidad de esta tecnología en la que, cuanto mayor es el grado de replicación de los bloques, más sencillo resulta detectar adulteraciones [1].

La aplicación más visible de esta tecnología son las criptomonedas, siendo el Bitcoin una de las más reconocidas que fue presentada por Satoshi Nakamoto [2] como un sistema de dinero en efectivo/pago electrónico basado en pruebas criptográficas, en contraposición al sistema financiero tradicional que utiliza un esquema basado en confianza con instituciones financieras que actúan como intermediarias. De esta manera la criptomoneda permite que, sin necesidad de un tercero, dos partes realicen transacciones entre ellas por medio de criptografía, (operaciones computacionalmente imposibles de revertir con las tecnologías actuales), redes pares, una cadena de firmas digitales, un servidor de sellado de tiempo y los nodos suficientes para lograr el consenso distribuido requerido para validar cada transacción.

Más allá de su aplicación en las criptomonedas, la tecnología fue considerada en todo su potencial de habilitar consensos distribuidos para que cada transacción en línea pueda ser verificada en cualquier momento futuro. Esto es posible porque blockchain contiene un registro determinado y verificable de cada transacción realizada y los datos que se introducen son permanentes. Es decir, una vez escrito un nuevo hecho este no se puede borrar ni modificar, lo cual se consigue replicando el registro de información entre varios nodos, de manera que cualquier alteración implicaría modificar el registro de cada uno de los participantes.

Esta tecnología permite tener una red distribuida en la que no existe ninguna entidad central o intermediario que coordine las interacciones, sino que se trata de una red peer-to-peer (P2P) en la que los participantes se comunican entre pares. Debido a ello, cuando se desea introducir un nuevo hecho en el registro compartido, se requiere alcanzar un consenso entre los participantes para determinar en qué bloque se registrará esa información.

Las transacciones en un bloque se consideran que ocurrieron en el mismo momento de tiempo, por ende, los bloques se enlazan entre sí en un orden cronológico lineal y, a medida que la cadena de bloques se enlaza, crea un registro público irrefutable soportado por un esquema de encriptación de clave pública y claves hash.

Lo expuesto permite imaginar múltiples prestaciones de la tecnología relacionadas a transacciones, a la seguridad, a la trazabilidad y a la transparencia. Sería posible poner en la cadena de bloques cualquier tipo de archivo/dato que requiera aseguramiento con hash.

Por su parte la metodología Forensic Readiness, o también llamada Preparación Forense, propone que la evidencia digital se recolecte y asegure de manera anticipada, es decir, antes de la ocurrencia de un incidente de seguridad. Este término fue enunciado por John Tan [3] quien lo describió principalmente a través de dos objetivos: maximizar la capacidad del entorno para reunir evidencia digital confiable y minimizar el costo forense durante la respuesta a un incidente.

En este enfoque, que fue analizado en proyectos anteriores [4] [5] [6], los datos que se recolectan pueden ser utilizados como insumo para el análisis de incidentes de seguridad y también como prueba legal, lo que involucra el aseguramiento de la prueba a medida que se realiza la recolección activa de los datos, tarea que fue realizada, en el primer proyecto utilizando funciones hash para resguardar la integridad de la evidencia digital.

En concordancia, la ISO/IEC 27037:2012 [7] establece que la evidencia digital es gobernada por tres principios fundamentales:

a. Relevancia: la evidencia digital debe estar relacionada con los hechos investigados,
b. Confiabilidad: la evidencia debe ser repetible y auditable, de tal manera que un tercero que aplique el mismo método utilizado, llegue al mismo resultado y
c. Suficiencia: la evidencia recolectada debe ser suficiente para sustentar los hallazgos obtenidos por el analista forense.

Considerando estos requisitos, una instancia fundamental para garantizar su admisibilidad como elemento de prueba es la preservación de la Cadena de Custodia como aval de la integridad y trazabilidad de la evidencia. Esta cadena de custodia debe estar claramente documentada y con un registro detallado desde su recolección hasta su almacenamiento, por lo que se plantea, con especial interés, la aplicación de la tecnología blockchain para cumplimentar este requisito.

Objetivos propuestos y cumplidos

General

Analizar el impacto de la utilización de la tecnología blockchain aplicada a la preservación, la integridad y trazabilidad de la evidencia digital.

Objetivos secundarios:

- Integrar esquemas de recolección de datos y bases de datos de resguardo de evidencia con una solución de blockchain.
- Analizar la relación entre la escalabilidad de blockchain y los algoritmos de consenso.
- Avanzar en la identificación de incidentes de seguridad y el análisis de aspectos de seguridad informática relacionada con la tecnología blockchain.

Metodología

La prueba de concepto planteada para alcanzar los objetivos de este proyecto se desarrolló principalmente con una metodología experimental en laboratorio informático, a través de la instalación de la blockchain privada Hyperledger, la utilización de las prestaciones de la Blockchain Federal Argentina y las experiencias del despliegue del nodo sellador con el que la Facultad de Ciencias de la Administración participa en la BFA.

Para la configuración del entorno de trabajo con la blockchain pública se usó la infraestructura disponible con la instalación de un nodo transaccional en la red de prueba (test2), sobre Ubuntu Server, de acuerdo a los requerimientos técnicos especificados por BFA en su Wiki. Por otra parte, para la instalación de Hyperledger Fabric

se empleó contenedores de Docker1 para desplegar servicios en una máquina virtual de 4GB RAM, 150GB de disco HDD, 4 núcleos y Ubuntu Server como sistema operativo, sobre una infraestructura propia que utiliza XenServer2 (XCP-ng) como plataforma de virtualización. En esta estructura mínima se definieron clientes, nodos pares y un nodo que actúa de Autoridad de Certificación para los usuarios.

Se realizaron también actividades de revisión bibliográfica, relevamiento de casos de uso en organizaciones regionales y nacionales, actualización del estado de la tecnología, análisis de plataformas disponibles y sus prestaciones.

Síntesis de resultados y conclusiones

Los resultados alcanzados y su discusión se plasman en publicaciones presentadas en eventos científicos, pero también en términos de formación de recursos humanos y en las capacidades desarrolladas por el grupo, las que impactan en continuidad de actividades de investigación.

A continuación, se presenta una síntesis de los resultados de las etapas del proyecto:

1) Base de conocimiento: Se realizó una revisión bibliográfica y actualización del estado del arte sobre nuevas tecnologías, aplicaciones y desarrollos basados en blockchain. Esta actividad se desarrolló de manera permanente durante la ejecución del proyecto debido a la continua aparición de nuevos desarrollos y aplicaciones de blockchain.

2) Relevamiento de casos de uso: Se relevaron casos de uso a nivel nacional y regional, obteniendo un panorama general de la adopción de la tecnología y áreas de vacancia, como por ejemplo en este último caso su uso en ámbitos judiciales, cuestión que en el último tiempo ha tenido un marcado avance en las diversas posibilidades que ofrece Blockchain.

Entre las iniciativas se destaca la puesta en funcionamiento de la Blockchain Federal Argentina (BFA) [8] que brinda una plataforma pública para integrar servicios y aplicaciones sobre blockchain. BFA sigue el modelo de Múltiples Partes Interesadas por lo que participan de ella entidades del sector público, privado, académico y de la sociedad civil que aportan la infraestructura, desarrollo y soporte técnico. Cabe mencionar que integrantes de este proyecto participan como responsables de la implementación y mantenimiento del nodo sellador de la Facultad de Ciencias de la Administración de la UNER, siendo ésta última un miembro parte de la BFA.

Ejemplos de casos de uso relevados: [9]

- Administración pública: Garantizar la integridad de documentación oficial (Boletín Oficial, Carpeta Ciudadana CABA.); Certificación de dominios de internet (NIC Argentina); Mediciones de altura de los ríos (PNA).
- Instituciones: Verificación de documentos notariales digitales (Colegio Escribanos CABA); Verificación de registros de graduados universitarios (SIU); Certificación de recepción ofertas de proveedores (SIU-Diaguita).
- Industria: Trazabilidad Citrícola (KYAS-SENASA); Comercialización commodities agrícolas (Plataforma Agree Market); Validación de boletos de compraventas de inmuebles (Bildenlex).

1. Docker Docs. https://docs.docker.com/

2. XCP-ng. https://xcp-ng.org/

La tecnología blockchain aporta para estos usos: seguridad jurídica y legislativa, garantías de integridad en la documentación, fortalecimiento del control ciudadano, transparencia en la publicación de datos, trazabilidad, valor agregado en los productos, auditoria de información por partes interesadas y el uso de Smart Contracts para inmutabilidad de las negociaciones y contratos, entre otras.

3) Análisis de estructuras y tipos de blockchain. Se relevaron los diferentes tipos de blockchain, sus principales características, aplicaciones y demás aspectos relacionados. [10]

En síntesis y de manera general, las redes blockchain pueden clasificarse como [11], [12], [13], [14]:

- **Públicas:** donde cualquiera puede acceder a los datos de la cadena de bloques. Normalmente son transparentes, los usuarios son anónimos, no existe un administrador de la red y las transacciones se validan mediante un protocolo de consenso.
- **Privadas:** son aquellas donde existe una entidad central que se encarga de controlar la cadena de bloques, definir la lista de participantes autorizados, otorgar permisos, proponer transacciones y validar los bloques. Puede decirse que no existe descentralización ni consenso ya que es una única entidad quien administra la red. Los usuarios finales dependen de una interfaz provista por el administrador para leer o enviar transacciones.
- **De Consorcio o Federadas**, son las que tienen un conjunto de participantes predefinido, tales como empresas u organizaciones, quienes se encargan de la administración conjunta de la red y de asegurar el mantenimiento sincronizado de las copias del registro compartido. El acceso a los datos puede ser público o privado. Son redes parcialmente descentralizadas, adecuadas para aplicaciones en donde se generan grandes volúmenes de transacciones entre entidades con requerimientos de confianza mutua.

Otra clasificación posible surge de considerar quiénes poseen permisos para crear bloques, a saber:

- **Sin permisos (*permissionless*)**: cualquier entidad puede procesar transacciones, participar de los protocolos de consenso y crear bloques.
- **Con permisos (*permissioned*):** solo una lista o conjunto de entidades predefinidas, y con identidades conocidas, pueden participar del procesamiento de transacciones, lo que agrega una capa más para el control de acceso e identificación.

En definitiva, las redes públicas pueden o no tener permisos, mientras que las privadas y las de consorcio o federadas suelen ser de tipo permisionadas. Las aplicaciones de blockchain con criptomonedas, como Bitcoin o Ethereum, son ejemplos de redes públicas sin permisos, mientras que el proyecto Hyperledger permite implementar redes de blockchain privadas con permisos.

Por último, desde el punto de vista de la realización de las transacciones, se puede hacer una diferenciación entre off-chain y on-chain, donde:

- **Transacciones on-chain (dentro de la cadena)**: son las que ocurren dentro del blockchain, adquieren validez sólo cuando la cadena de bloques se modifica para registrar la transacción en el ledger distribuido y son visibles para todos

los nodos participantes. El tiempo de esta operación depende del volumen de transacciones y la cantidad de nodos selladores que actúan en la red. Por lo general los mineros cobran una comisión por sus servicios de validación y autenticación de transacciones.

- **Transacciones off-chain**: en este tipo de transacciones los datos en cuestión permanecen fuera de la cadena de bloques, quedando dentro de la blockchain el ID y el hash que la identifica. En contraste con las transacciones on-chain, los datos no son de acceso público y las transacciones se ejecutan de manera inmediata. Implican un acuerdo entre las partes para realizar la transacción y, si fuera necesario, la participación de un tercero para validar la operación.

Ethereum versus Hyperledger: De acuerdo a los objetivos de esta investigación se han analizado dos soluciones representativas de blockchain, una pública y otra privada, considerando para esto prestaciones tales como: privacidad, seguridad, velocidad de validación de transacciones, casos de uso, estándar abierto, entre otros ítems. Así se seleccionó la infraestructura disponible de BFA que toma el software de Ethereum [15], utilizando Prueba de Autoridad (PoA), sin criptomoneda asociada y como plataforma publica, distribuida y descentralizada y, por otra parte, el desarrollo Open Source Hyperledger Fabric de la Linux Fundation [16], que es una red permisionada privada, con acceso restringido y donde la identidad de los participantes es conocida.

Para ambas soluciones se analizaron sus prestaciones, se definieron algunas métricas, se realizó un análisis de riesgo, se analizaron los protocolos de consenso y las principales vulnerabilidades que las afectan.

4) Procedimiento de recolección de evidencia digital. Se bosquejó un esquema genérico de recolección de evidencia digital y su envío a la Blockchain, el cual fue utilizado como marco de pruebas de laboratorio y se presenta en la siguiente figura:

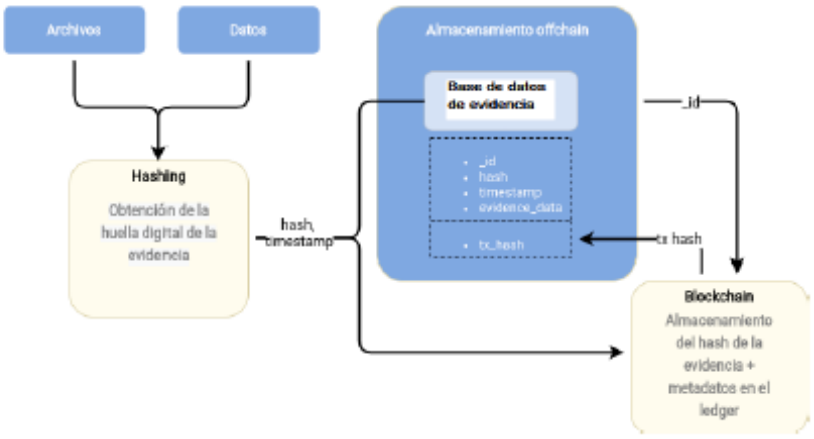

Figura 1. Esquema de recolección de evidencia

En la imagen se describe el proceso de almacenamiento de los hashes de la evidencia recolectada de los activos esenciales determinados, junto a los metadatos de la misma, en el ledger (libro de registro distribuido) para permitir la correlación. De esta

manera se resguarda la información de la evidencia en una base de datos con mayor rapidez y seguridad, en comparación a las transacciones on-chain.

El procedimiento es el siguiente:

- Se determina el activo digital sobre el cual se realizará la recolección de datos considerados evidencia.
- Se obtiene el hash o identidad digital de esos datos que junto al sello de tiempo (timestamp) proporcionarán la integridad.
- La evidencia se almacena en una base de datos off-chain o directorio privado
- El hash y los metadatos de la evidencia se registran en la blockchain.

Algunos puntos que se tuvieron en cuenta al momento de realizar las pruebas de concepto:

a. a. En vista de los requisitos relacionados con Forensic Readiness, es necesario contar con una blockchain donde los datos, posiblemente confidenciales, puedan almacenarse fuera de la cadena de bloques.
b. El sello de tiempo es un mecanismo que permite generar una "prueba de existencia" de un archivo digital. En este sentido, BFA ofrece su propio servicio de servicio de TSA (*Time Stamping Authority*).
c. Como en Hyperledger Fabric no se necesita el consenso de todos los nodos para validar las transacciones, se utiliza un algoritmo BTF (Tolerancia a las fallas bizantinas) [17] con la posibilidad de usar más de un mecanismo de consenso para resolver los problemas de confianza entre los nodos.
d. Hyperledger Fabric ofrece mayor customización para casos de uso que requieran estricta privacidad.
e. Al ofrecer transacciones sin costo, BFA cuenta con una "Destilería de Gas" que regula el envío de ether a nodos transaccionales. Esto puede tener impacto y ser un limitante según el volumen de datos recolectados.

5) Métricas para blockchain. A medida que se avanzó con las etapas del PID, se hizo necesario contar con algunos indicadores que ayuden a medir la perfomance y el rendimiento de cada tipo de blockchain, debido a que si bien se plantean aspectos conocidos para la medición del rendimiento no hay un marco común que facilite la tarea de lograr una medición comparativa en las diferentes implementaciones de las soluciones de blockchain.

Al respecto, se delinearon algunas métricas iniciales sobre la Blockchain Federal Argentina y una primera revisión del tema sobre Hyperledger Fabric [18] [19]. Para el primer caso se utilizaron dos herramientas disponibles en el sitio de BFA, *bfascan* [3] desarrollada por Última Milla y un monitor implementado con *Grafana*[4].

Métricas sobre BFA: Es de destacar que en cuanto a su operatoria cada entidad que administra un nodo de BFA es responsable de su mantenimiento y monitoreo y no existe en la red un sistema central de administración. Como apoyo, BFA implementa 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 tiene una ubicación centralizada, sino que está distribuido geográficamente y entre varias partes de la organización.

3. BFA SCAN http://www.bfascan.com.ar/

4. Monitor https://bfa.ar/monitor

Sobre esa distribución de nodos se realizó la captura de datos y se aplicaron las herramientas disponibles de análisis, como por ejemplo se muestra en las siguientes figuras información estadística general y detallada sobre el funcionamiento de los nodos selladores, total de transacciones diarias y totales y la identificación del último bloque y su minero

Figura 2. Información transaccional BFA

Figura 3. Información estadística BFA

Algunas de las métricas iniciales que se propusieron en esta etapa fueron:

- **TPT_BFA**: Tiempo promedio de una transacción = Transacciones del Día / tiempo transcurrido desde las 0:00hs (al momento de calcular).
- **CTPN_BFA**: Cantidad de transacciones promedio por nodo = Total de Transacciones / Total de Nodos Selladores
- **CTND_BFA**: Cantidad de transacciones promedio por nodo del día = Transacciones del Día / Total de Nodos Selladores.
- **TPCB_BFA: Tiempo promedio de creación de bloque** = tiempo transcurrido desde el primer al último bloque devueltos por la consulta / el total de bloques devueltos por la consulta. (cuando más bloques puedan consultarse más precisa podrá resultar la aproximación).
- **CPTB_BFA: Cantidad promedio de transacciones por bloqu**e = suma de las transacciones asociadas a cada uno de los bloques devueltos por la consulta / el total de bloques devueltos por la consulta.
- **TPCT_BFA: Tiempo promedio de creación de una transacción** = tiempo transcurrido entre la primera y la última transacción retornada / cantidad de transacciones retornadas (lo mismo que en el caso anterior, a mayor cantidad de registros consultados más aproximada podría ser la estimación)

Métricas Hyperledger: En cuanto a Hyperledger Fabric, este provee un archivo llamado *configtx.yaml* para la configuración de ciertas características específicas de la red y que impactan en su perfomance. En dicho archivo se encuentran dos parámetros

importantes *BatchSize y BatchTimeout* que permiten configurar el rendimiento y la latencia de las transacciones.

Batch size: Define cuántas transacciones recopilará el nodo ordenador antes de cerrar un bloque. Ningún bloque superará el tamaño de *AbsoluteMaxBytes* ni tendrá más de *MaxMessageCount* transacciones dentro. El tamaño ideal de construcción del bloque es de *PreferredMaxBytes*. Las transacciones que sean mayores a este tamaño aparecerán en un bloque propio.

Batch timeout: es un mecanismo de reserva si el bloque no se llena en un tiempo específico. Este valor proporciona un límite superior para el tiempo que se tarda en cerrar un bloque de transacciones. Al disminuir este valor se mejorará la latencia, pero al hacerlo demasiado pequeño puede que se reduzca el rendimiento al no permitir que el bloque se llene a su capacidad máxima.

En ambos casos, el contar con métricas ayudó en la identificación de posibles problemas en el funcionamiento de las plataformas, a analizar el trabajo de los nodos, a identificar cuellos de botella, a determinar el uso de recursos, a optimizar los protocolos de consenso y a detectar la ocurrencia de ataques sobre la seguridad de la red, entre otras cuestiones.

6) Análisis de Protocolos de consenso. Los mecanismos de consenso, también llamados protocolos o algoritmos de consenso, permiten que los sistemas distribuidos creen un entorno para colaborar y mantenerse seguros. Este mecanismo implica la aceptación de todos los nodos miembros de la blockchain sobre la información que hay en la misma. Es decir, que todos los nodos aceptan que el último bloque ha sido agregado a la cadena de manera correcta, que es el mismo para todos, que no presenta manipulaciones ni datos erróneos.

Tanto BFA como Hyperledger Fabric usan el mecanismo de consenso llamado Proof of authority (PoA) con algunas variaciones según la implementación [20] [21] [22] [23].

En la Prueba de Autoridad existen varios nodos de autoridad los cuales están identificados y reciben el nombre de selladores. En este contexto, la identidad significa la identificación personal de un sellador en el mundo real, como por ejemplo en la Blockchain Federal Argentina donde cada nodo sellador debe solicitar su ingreso, presentar documentación legal que certifique su identidad y ser aceptado por (n/2)+1 nodos selladores. Como característica distintiva los 21 nodos selladores operativos de la BFA pertenecen a diferentes sectores (académico, industria, organizaciones públicas, privadas). Esto brinda un control total sobre qué nodos pueden sellar bloques en la red, sirviendo como primera protección para asegurar que un sellador malicioso no pueda generar problemas.

Hyperledger Fabric, de por sí una plataforma permisionada, utiliza el mecanismo de consenso PoA con base en Kafka Orderer donde los participantes autorizados con acceso controlado validan las transacciones. Cuando la mayoría valida una transacción, hay consenso y se confirma.

Las versiones posteriores de Hyperledger han incorporado el protocolo de consenso Raft basado en el liderazgo, donde los nodos "seguidores" replican las entradas de registro creadas por el "líder" y también pueden elegir un nuevo nodo líder en caso de que este deje de enviar mensajes después de un tiempo configurado. En la red de pruebas se han levantado 5 nodos para simular las partes interesadas.

Además, si bien Kafka es tolerante a fallos, no lo es frente a fallos bizantinos, lo que podría provocar que el sistema no llegue a un acuerdo en el caso de nodos maliciosos o defectuosos.

Entonces, en ambas implementaciones, la identidad de los participantes es conocida abandonando el concepto de anonimato que se asocia a las criptomonedas, lo que sustenta la autentificación de los mismos.

Otro aspecto a considerar es la modalidad de operación, en cuanto a que BFA es descentralizada y todos los nodos pueden acceder al log de registro. En cambio, en Hyperledger el registro no es público y tiene un carácter centralizado. Esta última característica tiene ventajas y desventajas conocidas, tales como mayor control de las operaciones, riesgo de que la centralización produzca "cuellos de botella" y que el nodo "líder" sea objeto de un ataque de denegación de servicios, conceptos relacionados con la disponibilidad.

7) Análisis de vulnerabilidades y riesgos de seguridad. Se analizaron las principales vulnerabilidades y riesgos de seguridad que afectan actualmente a la tecnología blockchain, tales como los dos que se describen a continuación:

- **Bifurcación (Fork):** Este tipo de incidentes tiene que ver con los cambios en las reglas de consenso, por ejemplo, ante una actualización del software de la red de blockchain. Al publicarse una nueva versión del software de la blockchain, cambia el acuerdo sobre las reglas de consenso en los nodos. Las actualizaciones pueden dar lugar a dos tipos de nodos: nodos nuevos, que ya tienen la nueva versión del software, y nodos viejos, que aún no han actualizado a la nueva versión. Como resultado algunos de los nodos selladores pueden llegar a identificar identificaron bloques inválidos como correctos, creando una nueva cadena. Dividir la red puede traer inconvenientes de funcionamiento (nodos sin sellar, estado de no consenso) y también deja la base para ataques del 51%.
- **Phishing:** En este tipo de ataque se intenta obtener las credenciales de un usuario. Si bien el campo de acción es mayor en las wallets y blockchain con criptomonedas es un riesgo a considerar, más aún cuando un componente principal para que funcione el entorno seguro que se pretende desplegar es la autenticación de los participantes. Un posible ataque podría consistir en conseguir los datos de identificación/acceso de un sellador, así como otro tipo de información confidencial lo que puede resultar en pérdidas para el usuario, la red blockchain y para el entorno confidencial que se pretende implementar, por lo cual esta vulnerabilidad se consideró con especial relevancia tanto para BFA como para Hyperledger Fabric.

Como conclusión, si se plantea el resguardo de fragmentos de evidencia forense debe asegurarse un entorno de confianza y privacidad, para lo cual el mecanismo de consenso PoA presenta ventajas tales como eficiencia en los tiempos de transacción y el consenso general de la red, lo que es positivo para la escalabilidad. Pero parte de la ventaja de PoA se convierte también en una vulnerabilidad si consideramos el problema de bifurcación.

Ineludiblemente para el problema que planteamos en este proyecto, la identificación de los participantes otorga los requisitos indispensables de transparencia y autenticación, pero no se debe perder de vista las estrategias de prevención de una posible suplantación de identidad

8) Análisis de riesgo sobre blockchain. Como complemento de las etapas anteriores se realizó un análisis de riesgo utilizando como base la metodología Magerit 3.0 [24] adaptándola a los requerimientos del entorno de trabajo de las blochchain consideradas en el proyecto. Para esto se identificaron el alcance del análisis, los Activos, las amenazas y las Salvaguardas, a los fines de estimar el impacto (lo que podría pasar) y el riesgo (lo que probablemente pase) [25].

Se consideró como alcance del análisis de riesgo desde que se registra una transacción hasta el almacenamiento y protección de los datos que se recolectarán como evidencia.

En cuanto a los activos esenciales son aquellos que marcan los requisitos de seguridad para todos los demás componentes del sistema, que en este caso son:

Nombre	Descripción
Activo esencial Id: **[esencial]**	[info] información [ed] evidencia digital [service] blockchain

Figura 4. Activos esenciales

A continuación se especificaron los activos: Datos, Servicios, Software, Hardware y Usuarios relacionados con el tema tratado.

Como dimensiones de seguridad de los activos bajo amenaza fueron consideradas:

- **[D]**- **Disponibilidad**: propiedad que determina que los entes autorizados pueden acceder al recurso cuando lo requieran.
- **[I]**- **Integridad de los datos**: propiedad que determina que el activo no ha sido alterado por entes no autorizados.
- **[C]**- **Confidencialidad**: propiedad que determina que el activo no se expone ante entes no autorizados.
- **[A]**- **Autenticidad:** propiedad que determina que el ente autorizado es quien dice ser o que se garantiza la fuente de los datos.
- **[T]**- **Trazabilidad**: propiedad que determina que las actuaciones de un ente pueden ser imputadas exclusivamente a ese ente con constancia fehaciente de las transacciones realizadas por el mismo en cada etapa.

Y para cada uno de los activos se diseñó una tabla de valoración en relación a estas dimensiones de seguridad, como por ejemplo:

Activo [D]	Dimensiones de seguridad				
	[D]	[I]	[C]	[A]	[T]
Evidencia digital	[x]	[x]	[x]	[x]	[x]
Passwords		[x]	[x]	[x]	
Datos validación credenciales			[x]	[x]	
Datos de control de acceso	[x]		[x]	[x]	[x]
Logs					[x]

Figura 5. Tabla de valoración para activo Datos

Luego, se presentó un catálogo de posibles amenazas sobre los activos de la organización con foco en el activo principal. Para cada amenaza, identificada según la clasificación de la tabla, se tipifica el tipo de error, el activo, las dimensiones de seguridad afectadas y una descripción complementaria de la amenaza, como por ejemplo:

[A.2] Suplantación de identidad de los usuarios	Dimensiones
Tipos de activo: Datos/información Hardware Personal Origen: A – Ataques a la seguridad	Autenticidad Confidencialidad Integridad Disponibilidad
Descripción: terceros no autorizados que acceden a recursos o servicios de la red y pueden operarlos. Aplica para BFA e Hyperledger.	

Figura 6. Tabla Amenaza: Ataque a la seguridad con dimensiones afectadas

Además, para la medición del impacto se elaboró una tabla de riesgos relacionado la, probabilidad de ocurrencia, la medición del impacto en caso de producirse y dimensión de seguridad amenazada, resultando en:

N°	Riesgo	Probabilidad			Impacto			Dimensión Amenazada
		Baja	Media	Alta	Leve	Moderado	Catastrófico	
R1	[N.1] Fuego	X					X	[D]
R2	[E.1] Errores de administrador		X			X		[I] [D] [C] [A] [T]
R3	[E.2] Vulnerabilidades código		X			X		[I] [C] [D] [T]
R4	[E.3] Errores de monitoreo	X				X		[T]
R5	[A.1] Suplantación identidad de nodos		X				X	[A] [C] [I] [D]
R6	[A.2] Suplantación identidad usuarios		X				X	[A] [C] [I] [D]
R7	[A.3] Ataques protocolos consenso		X				X	[A] [I] [D] [T]
R8	[A.4] Denegación de servicios		X				X	[D]

Figura 7. Tabla de riesgos

Para finalizar se obtuvo la matriz que relaciona el riesgo, la probabilidad de ocurrencia y medición del impacto, la que muestra varios puntos vulnerables los cuales deben ser contemplados en profundidad más aun considerando que la blockchain que se propone se utilizará el resguardo de evidencia digital bajo Forensic Readiness lo que demanda como requisito de restricción que este entorno asegure la integridad, la confiabilidad, la disponibilidad, la trazabilidad y la debida autenticación de participantes.

Asimismo se denota la necesidad de considerar un plan de recuperación de desastres para todos los participantes de la blockchain y establecer el nivel de seguridad mínimo que se ofrecerá a los usuarios.

Consideraciones finales y perspectiva a futuro

En esta reseña se presentaron los principales resultados del desarrollo de las etapas del PID – UNER 7059. Es de destacar que, a pesar de los inconvenientes y restricciones

impuestos por el Aislamiento Social, Preventivo y Obligatorio que afectó casi toda la duración de este proyecto, se han cumplido los objetivos propuestos en su presentación.

En cuanto al tema abordado, el cual de por si es complejo al ser una arquitectura distribuida, su constante actualización y nuevas áreas de aplicación hace que sea necesario continuar profundizando sobre el mismo.

Dadas las implicancias de un proceso legal que requiera el uso de la evidencia almacenada, es fundamental contar con una tercera parte que permita validar y asegurar la integridad de las transacciones de forma independiente, independencia que al momento es asegurada por la estructura de múltiples partes interesadas de BFA.

En cambio, en Hyperledger Fabric al ser privada se deberá incorporar uno o más nodos de confianza para otorgar esa independencia, nodos que no sólo tendrán participación en la validación y confirmación de transacciones, sino que además guardarán su propia copia de los registros.

Al respecto, y como trabajo futuro, en breve será ineludible avanzar sobre las implicancias jurídicas de esta tecnología en relación a la legislación vigente en Argentina y su necesaria adaptación ante la irreversible irrupción tecnológica.

Indicadores de producción

En el marco del proyecto distintos integrantes del equipo de trabajo dirigieron 1 tesis de posgrado, 1 trabajo final de grado y 1 becario de iniciación a la investigación. Se fortaleció la formación de 4 docentes investigadores.

Se realizaron 6 publicaciones con referato (con presentación en congresos y eventos científicos), 1 publicación sin referato, 1 publicación en revista internacional de difusión científica.

Se dictará 1 curso de créditos académicos como consecuencia de la investigación realizada (Introducción a Blockchain. Curso de Créditos académicos, primer semestre 2023) y se asistió a 9 cursos como parte de la formación específica sobre temas del proyecto.

Elaboración de material audiovisual y escrito sobre el tema Consideraciones mínimas de seguridad informática en tiempos de pandemia en el marco del proyecto de extensión "Análisis propuestas para enfrentar las problemáticas de la gestión de organizaciones en el contexto actual", aprobado por Resolución "C.D." No 132/20.

Se anexan las siguientes publicaciones con referato:

1. Tugnarelli, Mónica D.; Díaz, Francisco Javier. "Forensic Readiness: Guía de buenas prácticas". Libro de actas CACIC 2019 págs. 1261-1268, Universidad Nacional de Río Cuarto, Córdoba, Argentina. ISBN 978-950-658-472-6. URI: http://sedici.unlp.edu.ar/handle/10915/91351
2. Díaz, Francisco Javier; Tugnarelli, Mónica Diana; Fornaroli, Mauro F.; Barboza, Lucas. "Blockchain para aseguramiento de evidencia digital en entornos Forensic Readiness" Libro de Actas XXII Workshop de Investigadores en Ciencias de la Computación (WICC 2020) Edición virtual, págs. 813-817. Universidad Nacional de la Patagonia Austral, Calafate, Argentina. ISBN: 978-987- 3714-82-5. URI: http://sedici.unlp.edu.ar/handle/10915/103151
3. Javier Díaz, Mónica D. Tugnarelli, Lucas Barboza, Mauro F. Fornaroli, Facundo N. Miño. "Implementación de Blockchain para aseguramiento de evidencia digital en entor-

nos Forensic Readiness". Libro de Actas del XXVI Congreso Argentino de Ciencias de la Computación (CACIC 2020) Edición virtual, págs. 736-744. Universidad Nacional de La Matanza, Buenos Aires, Argentina. ISBN 978-987-4417-90-9. URI: http://sedici.unlp.edu.ar/handle/10915/114463

4. Javier Díaz, Mónica D. Tugnarelli, Mauro F. Fornaroli, Facundo N. Miño, Lucas Barboza, Fabián Pineda. "Métricas para blockchain". XXVII Congreso Argentino de Ciencias de la Computación (CACIC 2021) Edición virtual Octubre 2021. Universidad Nacional de Salta, Argentina. ISBN: 978-987-633-574-4. URI: http://sedici.unlp.edu.ar/handle/10915/130537
5. Díaz, J., Tugnarelli, M.D., Fornaroli, M.F., Barboza, L., Miño, F., Carubia Grieco, J.I. (2022). Introduction of Metrics for Blockchain. In: Pesado, P., Gil, G. (eds) Computer Science – CACIC 2021. CACIC 2021. Communications in Computer and Information Science, vol 1584. Springer, Cham. URI: https://doi.org/10.1007/978-3-031-05903-2_19
6. Díaz, Francisco Javier; Tugnarelli, Mónica D.; Fornaroli, Mauro F.; Barboza, Lucas; Miño, Facundo, Carubia Grieco Juan. (2022) Protocolos de consenso. XXIV Workshop de Investigadores en Ciencias de la Computación (WICC 2022). ISBN: 978-987-48222-3-9. URL: https://wicc2022.uch.edu.ar/descargas/Libro-de-Actas-WICC-2022-1.pdf
7. Díaz, Francisco Javier; Tugnarelli, Mónica D.; Fornaroli, Mauro F.; Barboza, Lucas; Miño, Facundo (2022). Análisis de riesgo sobre blockchain. XX Jornadas Nacionales de Administración e Informática. (JAI2022). ISBN: 978-950-698-538-7. URL: https://www.fcad.uner.edu.ar/institucional/libro-de-actas-de-las-xx-jornadas-nacionales-de-administracion-e-informatica/

- Tesis: Implementación de disponibilidad forense para la continuidad digital. Tesista: Mónica D. Tugnarelli Director de tesis: Francisco Javier Díaz. Acceso: https://doi.org/10.35537/10915/97968
- Libro Tesis y Tesistas 2020. Implementación de disponibilidad forense para la continuidad digital. Resumen en español e inglés, págs. 94-97. Facultad de Informática. Universidad Nacional de La Plata. ISBN: 978-950-34-1972-4. http://sedici.unlp.edu.ar/handle/10915/114400

Artículo sin referato realizado en marco de proyecto extensión

- Tugnarelli, Mónica D., Fornaroli, Mauro F. Consideraciones mínimas de seguridad informática. (2021) https://www.fcad.uner.edu.ar/proyecto-extension/consideraciones-minimas-de-seguridad-informatica/

Libros como compilador

- XVII Congreso de Tecnología en Educación & Educación en Tecnología (TEyET2022) Libro de actas. Compiladores: Pesado, Patricia Mabel | Tugnarelli, Mónica Diana. EDUNER. ISBN: 978 950-698-522-6. URI: http://sedici.unlp.edu.ar/handle/10915/139119
- XX Jornadas Nacionales de Administración e Informática (JAI 2022). Libro de actas. Compiladores: Tugnarelli, Mónica Diana | Santana, Sonia Raquel. EDUNER. ISBN: 978-950-698-538-7- URI: https://www.fcad.uner.edu.ar/institucional/libro-de-actas-de-las-xx-jornadas-nacionales-de-administracion-e-informatica/

Bibliografía

[1] Michael Crosby, et. al. BlockChain Technology: Beyond Bitcoin. Applied Innovation Review (AIR). Issue No. 2 June 2016. Berkeley. http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Final-version-Int.pdf
[2] Satoshi Nakamoto (1998). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[3] Tan, John. (2001). Forensic Readiness. http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf
[4] Tugnarelli, M.; Fornaroli, M.; Santana, S.; Jacobo, E.; Díaz, F.J. Análisis de metodologías de recolección de datos digitales. Workshop de Investigadores en Ciencias de la Computación (WICC 2017). ISBN: 978-987-42-5143-5. http://sedici.unlp.edu.ar/handle/10915/61343
[5] Mónica D. Tugnarelli, Mauro F. Fornaroli, Sonia R. Santana, Eduardo Jacobo, Javier Díaz: Análisis de metodologías de recolección de datos digitales en servidores web. Libro de Actas. XXIII Congreso Argentino de Ciencias de la Computación CACIC 2017. VI Workshop de Seguridad Informática, pp. 1230-1238. ISBN 978-950-34-1539-9.
[6] Tugnarelli, M., Fornaroli,M. Santana,S. Jacobo, E. Díaz, J. Analysis of Methodologies of Digital Data Collection in Web Serves. Communications in Computer and Information Science (Springer), Vol. 790, Pag.265. (2018) https://link.springer.com/content/pdf/bfm%3A978-3-319-75214-3%2F1.pdf
[7] Guidelines for identification, collection, acquisition and preservation of digital evidence ISO/IEC 27037:2012
[8] Blockchain Federal Argentina https://bfa.ar/
[9] Díaz, Francisco Javier; Tugnarelli, Mónica Diana; Fornaroli, Mauro F.; Barboza, Lucas. "Blockchain para aseguramiento de evidencia digital en entornos Forensic Readiness" Libro de Actas XXII Workshop de Investigadores en Ciencias de la Computación (WICC 2020) Edición virtual, págs. 813-817. Universidad Nacional de la Patagonia Austral, Calafate, Argentina. ISBN: 978-987-3714-82-5. URI: http://sedici.unlp.edu.ar/handle/10915/103151
[10] Javier Díaz, Mónica D. Tugnarelli, Lucas Barboza, Mauro F. Fornaroli, Facundo N. Miño. "Implementación de Blockchain para aseguramiento de evidencia digital en entornos Forensic Readiness". Libro de Actas del XXVI Congreso Argentino de Ciencias de la Computación (CACIC 2020) Edición virtual, págs. 736-744. Universidad Nacional de La Matanza, Buenos Aires, Argentina. ISBN 978-987-4417-90-9. URI: http://sedici.unlp.edu.ar/handle/10915/114463
[11] Iuon-Chang Lin, Tzu-Chun Liao. A Survey of Blockchain Security Issues and Challenges . International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017
[12] Elli Androulaki, Artem Barger, Vita Bortnikov, et al, 2018. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In EuroSys '18: Thirteenth EuroSys Conference 2018, April 23–26, 2018, Porto, Portugal. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3190508.3190538
[13] BitFury Group. Public versus Private Blockchains Part 1: Permissioned Blockchains. White Paper. Oct 20, 2015 (Version 1.0). https://bitfury.com/content/downloads/public-vsprivate-pt1-1.pdf
[14] BitFury Group. Digital Assets on Public Blockchains. White Paper. Mar 15, 2016 (Version 1.0). ttps://bitfury.com/content/downloads/bitfurydigital_assets_on_public_blockchains-1.pdf

[15] Ethereum. https://ethereum.org
[16] Hyperledger. https://www.hyperledger.org/
[17] Lei, Kai & Zhang, Qichao & Xu, Limei & Qi, Zhuyun. (2018). Reputation-Based Byzantine Fault-Tolerance for Consortium Blockchain. 10.1109/PADSW.2018.8644933.
[18] Javier Díaz, Mónica D. Tugnarelli, Mauro F. Fornaroli, Facundo N. Miño, Lucas Barboza, Fabián Pineda. "Métricas para blockchain". XXVII Congreso Argentino de Ciencias de la Computación (CACIC 2021) Edición virtual Octubre 2021. Universidad Nacional de Salta, Argentina. ISBN: 978-987-633-574-4. URI: http://sedici.unlp.edu.ar/handle/10915/130537
[19] Díaz, J., Tugnarelli, M.D., Fornaroli, M.F., Barboza, L., Miño, F., Carubia Grieco, J.I. (2022). Introduction of Metrics for Blockchain. In: Pesado, P., Gil, G. (eds) Computer Science – CACIC 2021. CACIC 2021. Communications in Computer and Information Science, vol 1584. Springer, Cham. URI: https://doi.org/10.1007/978-3-031-05903-2_19
[20] Díaz, Francisco Javier; Tugnarelli, Mónica D.; Fornaroli, Mauro F.; Barboza, Lucas; Miño, Facundo, Carubia Grieco Juan. (2022) Protocolos de consenso. XXIV Workshop de Investigadores en Ciencias de la Computación (WICC 2022). ISBN: 978-987-48222-3-9. URL: https://wicc2022.uch.edu.ar/descargas/Libro-de-Actas-WICC-2022-1.pdf
[21] Mecanismos de Consenso Ethereum.https://ethereum.org/es/developers/docs/consensus-mechanisms/
[22] Mecanismos de Consenso BFA. https://bfa.ar/blockchain/protocolos-de-consenso
[23] Mecanismos de Consenso Hyperledger Fabric https://hyperledger-fabric.readthedocs.io/es/latest/fabric_model.html
[24] MAGERIT versión 3 (versión español). (Octubre 2012) *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*.- Edita: © Ministerio de Hacienda y Administraciones Públicas.- NIPO: 630-12-171-8
[25] Díaz, Francisco Javier; Tugnarelli, Mónica D.; Fornaroli, Mauro F.; Barboza, Lucas; Miño, Facundo (2022). Análisis de riesgo sobre blockchain. XX Jornadas Nacionales de Administración e Informática. (JAI2022). ISBN: 978-950-698-538-7. URL: https://www.fcad.uner.edu.ar/institucional/libro-de-actas-de-las-xx-jornadas-nacionales-de-administracion-e-informatica/
[26] Auqib Hamid Lone, Roohie Naaz Mir. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. https://doi.org/10.1016/j.diin.2019.01.002
[27] Kirill Bryanov. Quantum Computing Vs. Blockchain: Impact on Cryptography. https://cointelegraph.com/news/quantum-computing-vs-blockchain-impact-on-cryptography
[28] C. Fan, S. Ghaemi, H. Khazaei and P. Musilek, "Performance Evaluation of Blockchain Systems: A Systematic Survey," in IEEE Access, vol. 8, pp. 126927-126950, 2020, doi: 10.1109/ACCESS.2020.3006078
[29] Muoi Tran, Inho Choi, Gi Jun Moon, Anh V. Vu, Min Suk Kang. A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network . 2020 IEEE Symposium on Security and Privacy https://erebus-attack.comp.nus.edu.sg/erebus-attack.pdf
[30] H. Chen, M.Pendleton, L.Njilla, and S. Xu. 2020. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. ACM Computing Surveys. 53, 3, Article 67 (June 2020)

PID 7059 **Denominación del Proyecto**
Tecnología Blockchain para aseguramiento de evidencia digital en entornos forensic readiness

Director
Francisco Javier DIAZ

Codirectora:
Mónica Diana TUGNARELLI

Unidad de Ejecución
Universidad Nacional de Entre Ríos

Dependencia
Facultad de Ciencias de la Administración

Cátedra/s, área o disciplina científica
Comunicaciones y Redes
Areas: Arquitectura, Sistemas Operativos y Redes/Seguridad Informática.

Cátedra/s, área o disciplina científica
Laboratorio de nuevas tecnologias, Facultad de Informática, Universidad Nacional de La Plata
Facultad de Ciencias de la Administración, Universidad Nacional de Entre Rios
Convenio marco firmado en 2013, Convenio especifico firmado en 2021

Contacto
monica.tugnarelli@uner.edu.ar

Integrantes del proyecto
Mauro F. Fornaroli. Integrante docente (UNER)
Lucas Barboza. Integrante docente (UNER)
Facundo Miño. Integrante estudiante (UNER)
Fabian Pineda. Colaborador estudiante de postgrado (UNER)
Becario: Juan Ignacio Carubia Grieco

Fechas de iniciación y de finalización efectivas
02/03/20- 22/01/23
Aprobación del Informe Final por Resolución C.S. N° 134/23 (19/05/2023)

<<< Volver al inicio