Blockchain para aseguramiento de Evidencia Digital en entornos Forensic Readiness

Javier Díaz [(1),] Mónica D. Tugnarelli [(2)], Mauro F. Fornaroli [(2)], Lucas Barboza [(2)]
[(1)] Facultad de Informática – Universidad Nacional de La Plata
[(2)] Facultad de Ciencias de la Administración – Universidad Nacional de Entre Ríos
e-mail:jdiaz@unlp.edu.ar, montug, maufor, lbarboza[@fcad.uner.edu.ar]

Resumen

La tecnología blockchain tiene múltiples usos cuando se trata de validar la integridad, la transparencia y trazabilidad de datos. En este trabajo se presentan los avances del PID-UNER 7059 que abordará el estudio de esta tecnología focalizando su aplicación para asegurar la preservación, integridad y trazabilidad de evidencia digital, obtenida de activos esenciales, en un entorno preventivo como lo es Forensic Readiness.

Palabras clave: blockchain, evidencia digital, Forensic Readiness, seguridad.

Contexto

El artículo presenta los primeros avances del Proyecto de Investigación y Desarrollo PID-UNER 7059 denominado "*Tecnología Blockchain para aseguramiento de evidencia digital en entornos Forensic Readiness*" que se encuadra en una de las líneas de investigación establecidas como prioritarias para su fomento, "Arquitectura, Sistemas Operativos y Redes", de la carrera Licenciatura en Sistemas de la Facultad de Ciencias de la Administración. Se adecua además, a las prioridades de la Universidad Nacional de Entre Ríos por ser un proyecto aplicado a la investigación sobre Tecnologías de la Información y la Comunicación.

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 [3]), 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 requiera 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.

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

Forensic Readiness o 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 [4] 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 [5] [6] [7], 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 dicho proyecto, utilizando funciones hash para resguardar la integridad de la evidencia digital.

De acuerdo con la ISO/IEC 27037:2012 [8] 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.

Líneas de Investigación, Desarrollo e Innovación

Siguiendo la línea de investigación mencionada en el contexto de este trabajo, se llevarán a cabo actividades que propicien la conformación de una base de conocimiento sobre la tecnología blockchain y sus aplicaciones en diversos ámbitos, destacando el aseguramiento de la integridad y trazabilidad de cualquier activo digital que se considere evidencia digital.

Resultados y Objetivos

El PID 7059 tiene como objetivo primario analizar el impacto de la utilización de la tecnología blockchain aplicada a la preservación, la integridad y trazabilidad de la evidencia digital.
Como objetivos secundarios se establecen:

- 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.

Para lograr estos objetivos se analizarán las estructuras y tipos de blockchain, las soluciones disponibles en el mercado y se realizará la instalación y configuración de un entorno de prueba con Hyperledger, sin criptomoneda asociada. Asimismo, se espera obtener un procedimiento automatizado de autenticación y trazabilidad de la evidencia digital.
Como primera etapa del proyecto se relevaron casos de uso a nivel regional y nacional, entre las que se destaca la iniciativa y puesta en funcionamiento de la Blockchain Federal Argentina (BFA) [9] 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.

En el siguiente cuadro se presentan los principales usos relevados:

Tipo de organización: Administración pública	
Aplicación	**Aportes del Blockchain**
• 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)	• Seguridad jurídica y legislativa. • Garantía de integridad y control ciudadano • Transparencia en la publicación de datos • Trazabilidad de datos y mediciones
Tipo de organización: Instituciones	
Aplicaciones	**Aportes de Blockchain**
• Verificación de documentos notariales digitales. (Colegio Escribanos CABA) • Verificación de registros de graduados universitarios. (SIU) • Certificación de recepción ofertas de proveedores. (SIU-Diaguita) • Verificacion de informacion academica en sistema de gestión de alumnos. (UNC)	• Garantía de integridad en documentación. • Valor agregado en la certificación de documentos notariales. • Verificación de información pública. • Auditoría de información por las partes interesadas. • Trazabilidad en la emisión de certificaciones •
Tipo de organización: Industria	
Aplicaciones	**Aportes de Blockchain**
• Trazabilidad Citrícola (KYAS-SENASA) • Comercialización commodities agrícolas (Plataforma Agree Market) • Validación de boletos de compraventas de inmuebles (Bildenlex)	• Verificación de integridad de información en el documento • Permite sortear exitosamente auditorías documentales en los diferentes lugares donde se destina • Agregado de valor al producto • Uso de Smart Contracts para inmutabilidad de las negociaciones y los contratos

Cuadro 1. Aplicaciones de Blockchain a nivel nacional y regional

Formación de Recursos Humanos

Este proyecto propicia la formación en co-dirección de proyectos de un docente, la formación en actividades de investigación de dos docentes de la carrera Licenciatura en Sistemas y de un colaborador estudiante de posgrado de la Maestría en Sistemas de Información que se dicta en la Facultad de Ciencias de la Administración.

Además, se brindará el espacio de participación a aquellos estudiantes que deseen realizar su Trabajo Final de la carrera Licenciatura en Sistemas sobre este tema. Se prevé también, la incorporación de becarios de investigación en el marco del programa de Becas de Iniciación a la Investigación de la UNER.

Referencias

[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. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[3] Kirill Bryanov. Quantum Computing Vs. Blockchain: Impact on Cryptography. https://cointelegraph.com/news/quantum-computing-vs-blockchain-impact-on-cryptography

[4] Tan, John. (2001). Forensic Readiness. http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf

[5] 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

[6] 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.

[7] 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

[8] Guidelines for identification, collection, acquisition and preservation of digital evidence ISO/IEC 27037:2012

[9] Blockchain Federal Argentina https://bfa.ar/

[10] 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

[11] Iuon-Chang Lin,Tzu-Chun Liao. A Survey of Blockchain Security Issues and Challenges. https://pdfs.semanticscholar.org/f61e/db500c023c4c4ef665bd7ed2423170773340.pdf