Protocolos de consenso

Javier Díaz [1], Mónica D. Tugnarelli [2], Mauro F. Fornaroli [2]
Lucas Barboza[2], Facundo Miño[2], Juan I. Carubia Grieco[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, monica.tugnarelli, mauro.fornaroli[@.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 continua con la presentación de los avances del PID-UNER 7059 que aborda el estudio de esta tecnología focalizando su aplicación para asegurar la preservación de evidencia digital obtenida de activos esenciales, en un entorno preventivo como lo es Forensic Readiness. Este artículo describe los mecanismos de consenso adoptados por las blockchain seleccionadas así como algunos riesgos de seguridad conocidos y relevantes a la hora de considerar la implementación de una de ellas para cumplimentar el objetivo buscado.

Palabras clave: blockchain, protocolos de consenso, PoA, evidencia digital, seguridad

Contexto

El artículo presenta los 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

En artículos anteriores analizamos diferentes características respecto de la tecnología blockchain que incluyeron:

- Relevamiento de casos de uso a nivel regional y nacional, destacando la iniciativa y puesta en funcionamiento de la Blockchain Federal Argentina (BFA) [1].
- Análisis de diferentes tipos de blockchain a los fines de contar con una base de conocimiento previa para la implementación de prototipos en laboratorio, seleccionando para ello dos soluciones representativas de blockchain: una pública basada en Ethereum y otra privada Hyperledger Fabric. Además, se diseño un esquema genérico del proceso de almacenamiento de hashes que aseguren la evidencia de los activos esenciales determinados. [2]
- Presentación de métricas preliminares sobre la perfomance de la Blockchain Federal Argentina como ejemplo de Ethereum y una primera revisión del tema sobre Hyperledger Fabric instalada como base de pruebas en laboratorio [3]

En el presente trabajo revisamos los protocolos de consenso utilizados por las soluciones de blockchain seleccionadas para avanzar en la identificación y análisis de riesgos de seguridad que podrían afectarlas.

Es conocido que la tecnología blockchain utiliza criptografía y tecnología de *timestamp* en la capa de datos (Data), que emplea conexiones peer-to-peer para el intercambio de información en la capa de red, que implementa algoritmos de consenso para validar la información y que usa scripts y algoritmos para implementar smart contracts en diversos lenguajes de base. Este entorno de trabajo asegura varias cuestiones relacionadas con la consistencia, la trazabilidad y la inmutabilidad de la información, pero no por ello queda exento a posibles ataques de seguridad que lo comprometan.

El PID 7059 tiene por objetivo primario analizar las prestaciones de la tecnología Blockchain para asegurar la integridad y trazabilidad de la cadena de custodia en un entorno de Forensic Readiness [4], que como método preventivo requiere de respuestas precisas del entorno tecnológico para resguardar los datos considerados como evidencia digital. Por este motivo es imprescindible que esta tecnología asegure un entorno de confianza y privacidad para las partes intervinientes en el posible proceso judicial.

En ese marco, uno de los componentes principales es el mecanismo de consenso utilizado por BFA y por Hyperledger Fabric, tema que se aborda a continuación así como una breve descripción de los principales problemas de seguridad conocidos para dichas implementaciones.

Mecanismos 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. [5,6,7]

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.

Riesgos de seguridad

En función de lo planteado brevemente en los párrafos anteriores, es necesario relevar las principales vulnerabilidades que afectan a la tecnología blockchain ya que no son inmunes a los ataques y al fraude, tales como los dos que se describen a continuación:

A) 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.

Este problema también puede darse por un error tal como sucedió en enero de este año donde la red de pruebas de Ethereum 2.0, Kintsugi, se bifurcó en por lo menos 3 redes diferentes quedando fuera de servicio durante algunos días. En este caso, y según lo informado por el desarrollador de Ethereum [8], el inconveniente se debió a una prueba de verificación de error dentro de la red, que tiene por objetivo crear bloques inválidos cambiando ciertas características, de manera de verificar que los validadores puedan identificar el fallo e invalidar el bloque. Sin embargo, algunos de los nodos selladores identificaron bloques inválidos como correctos, creando una nueva cadena.

Casi al mismo tiempo la BFA sufrió un inconveniente similar donde los selladores quedaron en distintas bifurcaciones

resultando en unas horas sin sellar, lo cual fue solucionado manualmente mediante el grupo de trabajo Selladores levantando y sincronizando los nodos.

Sobre esta problemática en 2020 se realizó una prueba de concepto, conocida como ataque Erebus [9]. Este ataque está específicamente desarrollado para redes P2P como las de blockchain, buscando dividir la red objetivo, mientras que de manera silenciosa se gana el control de la mayor parte de la misma para hacer que efectivamente la red deje de funcionar. Además agrega una manipulación maliciosa en las conexiones con el fin de tomar el control de la misma usando como base un ataque Man-in-the-middle. Como consecuencia la red entra en un estado de no consenso, que termina dividiendo la red y que incluso podría derivar en un ataque de 51% sobre la blockchain.

B) 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, mas aun 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 deberá considerar tanto para BFA como para Hyperledger Fabric.

Líneas de Investigación, Desarrollo e Innovación

Siguiendo la línea de investigación mencionada en el contexto de este trabajo, se desarrollan 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 y la cadena de custodia.

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.

A la fecha se han cumplimentado diversas etapas en pos del logro de esos objetivos, restando la profundización sobre el tema seguridad el cual es complejo y de permanente actualización.

Por consiguiente, en este artículo se presentaron los resultados preliminares de este análisis, resaltando:

- Si se plantea el resguardo de fragmentos de evidencia forense debe asegurarse un entorno de confianza y privacidad.
- 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.
- Parte de la ventaja de PoA se convierte también en una vulnerabilidad si consideramos el problema de bifurcación.
- La identificación de los participantes le otorga los requisitos indispensables de transparencia y autenticación, pero se debe tener en cuenta la prevención de una posible suplantación de identidad

Formación de Recursos Humanos

Este proyecto propicia la formación de un docente en co-dirección de proyectos, la formación en actividades de investigación de dos docentes y de un estudiante que se encuentra realizando su trabajo final de la carrera Licenciatura en Sistemas, de un becario del Programa de Becas de Formación (Iniciación en Investigación) de la UNER 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.

Referencias

[1] Díaz, Francisco Javier; Tugnarelli, Mónica D; Fornaroli, Mauro F.; Barboza, Lucas. Blockchain para aseguramiento de evidencia digital en entornos Forensic Readiness. XXII Workshop de Investigadores en Ciencias de la Computación (WICC 2020). ISBN: 978-987-3714-82-5 http://sedici.unlp.edu.ar/handle/10915/103377

[2] Díaz, Francisco Javier; Tugnarelli, Mónica D.; Fornaroli, Mauro F.; Barboza, Lucas; Miño, Facundo. Implementación de Blockchain para aseguramiento de evidencia digital en entornos Forensic Readiness. Libro de actas XXVI Congreso Argentino de Ciencias de la Computación (CACIC 2020). ISBN: 978-987-4417-90-9 http://sedici.unlp.edu.ar/handle/10915/113243

[3] Díaz, Francisco Javier; Tugnarelli, Mónica D.; Fornaroli, Mauro F.; Barboza, Lucas; Miño, Facundo. Métricas para blockchain. Libro de actas XXVII Congreso Argentino de Ciencias de la Computación (CACIC 2021). ISBN: 978-987-633-574-4 http://sedici.unlp.edu.ar/handle/10915/129809

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

[5] Mecanismos de Consenso Ethereum.https://ethereum.org/es/developers/docs/consensus-mechanisms/

[6] Mecanismos de Consenso BFA. https://bfa.ar/blockchain/protocolos-de-consenso

[7] Mecanismos de Consenso Hyperledger Fabric https://hyperledger-fabric.readthedocs.io/es/latest/fabric_model.html

[8] Marius van der Wijden (2022) https://twitter.com/vdWijden/status/1479377978400419843

[9] 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

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

[11] 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)