ISBN 978–987–633–574–4

Métricas para blockchain

Javier Díaz[1], Mónica D. Tugnarelli[2], Mauro F. Fornaroli[2],
Facundo N. Miño[2], Lucas Barboza[2]

[1]Facultad de Informática – Universidad Nacional de La Plata
jdiaz@unlp.edu.ar
[2] Facultad de Ciencias de la Administración – Universidad Nacional de Entre Ríos
{monica.tugnarelli, mauro.fornaroli, lucas.barboza}@uner.edu.ar

Abstract. En este artículo se presentan un conjunto de métricas iniciales para abordar el análisis de rendimiento de tecnologías blockchain, principalmente con herramientas aplicadas a la Blockchain Federal Argentina y una primera aproximación a mediciones sobre Hyperledger Fabric. Considerando que si bien hay aspectos conocidos para medir el rendimiento, aun no existe un marco común que facilite la tarea de lograr una medición comparativa entre las distintas soluciones de blockchain, lo cual, y considerando el sostenido uso de esta tecnología en un amplio campo de aplicación, se muestra como un área de vacancia sobre la cual consideramos que es necesario avanzar con el objetivo de evaluar el rendimiento en diferentes casos de uso y escenarios.

Keywords: blockchain, métricas, BFA, Ethereum, Hyperledger

1 Introducción

En este artículo se presentan los avances del PID-UNER 7059 denominado "*Tecnología Blockchain para aseguramiento de evidencia digital en entornos Forensic Readiness*" que tiene como objetivo principal analizar el impacto de la utilización de esta tecnología aplicada a la preservación, integridad y trazabilidad de evidencia digital, la cual es obtenida a priori de los activos señalados como esenciales en una organización, en un entorno preventivo como lo es Forensic Readiness, también llamado Preparación Forense [1].

El PID cuenta con varias etapas, en las cuales se trabaja con blockchain sin criptomoneda asociada para lograr implementar un prototipo donde realizar pruebas que permitan analizar cómo reacciona esta tecnología frente a los requerimientos de Forensic Readiness tanto para el proceso de asegurar la evidencia como para el mantenimiento de la cadena de custodia.

En trabajos anteriores [2] se ha analizado las características de diferentes tipos de blockchain disponibles en el mercado y, de acuerdo a los objetivos planteados en esta investigación, se focaliza el análisis en dos soluciones representativas, una plataforma pública, distribuida y descentralizada como Ethereum [3] y la solución privada Hyperledger Fabric [4] de administración centralizada, considerando para este análisis

aspectos tales como: privacidad, seguridad, velocidad de validación de transacciones, casos de uso, estándar abierto, entre otros [5] .

2 Métricas

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.
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, lo cual considerando el sostenido uso de esta tecnología en distintos ámbitos se muestra como un área de vacancia sobre la cual consideramos que es conveniente avanzar.
Al respecto, se delinearon algunas métricas iniciales sobre la Blockchain Federal Argentina como ejemplo de Ethereum y una primera revisión del tema sobre Hyperledger Fabric instalada como base de pruebas en laboratorio. Para el primer caso se utilizaron dos herramientas disponibles en el sitio de BFA, *bfascan*[1] desarrollada por Última Milla y un monitor implementado con *Grafana*[2] , las cuales se presentan en el siguiente punto.

2.1 Métricas sobre BFA

La Blockchain Federal Argentina [6] es una plataforma multiservicios abierta y participativa basada en tecnología Ethereum y pensada para integrar servicios y aplicaciones sobre blockchain. Está conformada por sectores públicos, privados, académicos y de la sociedad civil que participan desde la ingeniería organizacional hasta el despliegue de la infraestructura donde ningún sector tiene mayoría y eso evita que pueda ser manipulada. Cuenta con una variedad de casos de uso interesantes y con la ventaja de que el servicio de Sello de Tiempo 2.0 de BFA provee una hora oficial segura para usar en distintos procesos, el cual permite demostrar que el contenido de cualquier documento digital existió en un momento y que desde entonces no ha cambiado.
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. Cabe destacar que la Facultad de Ciencias de las Administración cuenta con un nodo sellador administrado por dos integrantes de este equipo de investigación.

[1] BFA SCAN http://www.bfascan.com.ar/
[2] Monitor https://bfa.ar/monitor

Sobre esa distribución de nodos se realizó la captura de datos y se aplicaron las herramientas disponibles de análisis.
La siguiente tabla y gráficos muestran datos obtenidos sobre la Blockchain Federal Argentina en cuanto a cantidad de nodos operativos, volumen de transacciones y cuentas creadas en la BFA:

Cantidad de nodos que componen la red	-Cantidad total de nodos transaccionales.	90 nodos transaccionales
	-Cantidad total de nodos selladores	21 nodos selladores en línea y operativos
Transacciones del día	Cantidad total de transacciones realizadas desde las 0:00hs	Información variable: promedio de 10.000 transacciones en días laborables.
Total de transacciones	Cantidad total de transacciones realizadas.	Información variable: acumulado 5350650
Total de Direcciones	Total de cuentas creadas en la BFA.	Información variable: 805

Tabla 1. Recopilación de datos BFA con BFA Scan 16/8/21. Fuente: Elaboración propia

Fig.1 Captura de información estadística con BFAScan 16/8/21. Fuente: Web BFAScan

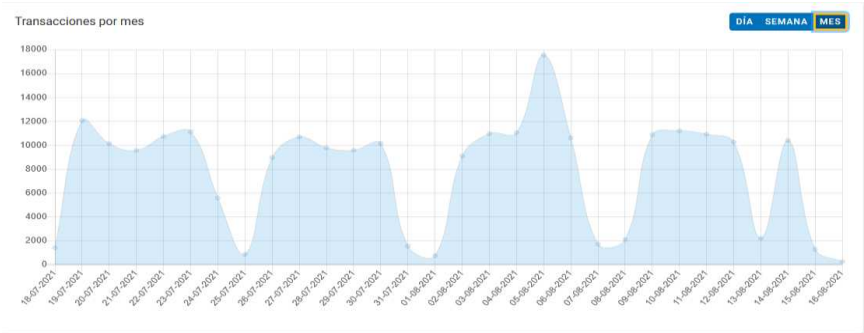

Fig.2 Captura de información estadística con BFAScan 16/8/21. Fuente: Web BFAScan

En base a la información anterior se proponen algunas métricas iniciales:

- **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.

Además de la herramienta anterior, el sitio *BFASCAN* ofrece una API llamada *API REST BFA Scan* que presenta distintos métodos para obtener información contenida en la BFA.

a) **Método getBlocks** *url: http://201.190.184.52/bfascan/Blocks/getBlocks*

- HTTP GET. Devuelve información de los últimos 10 bloques.
- HTTP POST. Devuelve información de los últimos 100 bloques, o de uno en particular (a partir del hash).
- HTTP POST para usuarios registrados: Devuelve información de los últimos *n* bloques (como máximo 1000), o de uno en particular (a partir del hash). La consulta requiere un token que es enviado en un correo electrónico luego del registro.

De la información retornada por el método *getBlocks*, pueden utilizarse los *timestamps* de cada registro para calcular el tiempo promedio de creación de un bloque. Por ejemplo:

- **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).

Otro campo que devuelve la consulta en cada registro es *transactions_associated*. Este valor podría utilizarse para calcular la cantidad de transacciones promedio por bloque sumando la cantidad de transacciones de cada bloque por el total de bloques.

- **CPTB_BFA: Cantidad promedio de transacciones por bloque** = suma de las transacciones asociadas a cada uno de los bloques devueltos por la consulta / el total de bloques devueltos por la consulta.

b) Método getTxs *url: http://201.190.184.52/bfascan/transactions/getTxs*

- HTTP GET. Devuelve información de las últimas 10 transacciones creadas en la BFA.
- HTTP POST. Devuelve información de las últimas 100 transacciones, o de una en particular (a partir de su hash)
- HTTP POST para usuarios registrados: Devuelve información de las últimas transacciones (como máximo 1000), o de una en particular (a partir del hash). La

consulta requiere un token que es enviado en un correo electrónico luego del registro.

Al igual que con el método *getBlocks* podrían utilizarse los *timestamps* de los registros devueltos por la consulta para calcular el tiempo promedio de creación de una transacción (o tiempo entre transacciones). Por ejemplo:

- **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)

Estas consultas podrían repetirse a intervalos de tiempo regulares, y luego realizar una estimación a partir de todos los tiempos promedios obtenidos.

El monitor BFA de Grafana, y a partir de la información que se muestra, permite obtener información para otra métrica inicial:

- **CPBS_BFA**: Cantidad promedio de bloques sellados por nodos (a partir de la información de último bloque sellado en *x* período de tiempo (permite consultar por últimos *n* minutos, horas, días) Estos valores se podrían calcular en distintos momentos de tiempo y luego calcular un promedio sobre estos para una mejor estimación.

Fig.3 Captura de información de monitoreo 16/8/21. Fuente: Web Monitor

Y otro indicador:

- **TF_BFA**: Tiempo de finalización: tiempo necesario para alcanzar la inmutabilidad de transacciones y bloques.

2.1 Métricas sobre Hyperledger

En cuanto a Hyperledger Fabric que es la blockchain instalada en laboratorio, provee un archivo llamado *configtx.yaml* para la configuración de ciertas características de la red. En él 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.

Cuanto menores sean los valores de *Batch timeout* y *Batch size*, mayor va a ser el número total de bloques generados por segundo. En cambio, mientras mayor sean sus valores, menor será el número de bloques generados por segundo.
Reduciendo el valor de *Batch timeout* disminuirá la latencia, pero a expensas del rendimiento total. Por el contrario, aumentar el *MaxMessageCount* hará que aumente el rendimiento total pero a expensas de la latencia de la transacción. Esta latencia, que se obtiene de restar tiempo de confirmación – tiempo de envío, es una vista de toda la red relacionada a la cantidad de tiempo que tarda una transacción en hacerse efectiva y propagarse por toda la red.
En términos generales, no existen valores ideales a definir, por lo que se deberán hallar de acuerdo a los requerimientos del prototipo instalado en el marco de este proyecto de investigación y luego aplicar las métricas definidas en el punto anterior para ver su correlación entre esquemas de blockchain.
Y, como agregado, las diferentes versiones de Hyperledger Fabric (HLF), por ejemplo, HLF v0.6 y HLF v1.0, deben compararse en el mismo marco de evaluación para demostrar las ventajas / desventajas de rendimiento de las nuevas versiones [7].

3. Conclusiones y trabajos futuros

En este trabajo se han presentado algunas primeras métricas que servirán de base para medir la calidad, performance y escalabilidad de las aplicaciones de blockchain. El beneficio de contar con métricas que ayuden a identificar y encontrar posibles problemas en el funcionamiento de la blockchain, que permitan analizar el trabajo de los nodos actuando a la vez y de manera descentralizada, 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 ayudará a crear un entorno más controlado y seguro de operar.

Como trabajos futuros se aplicarán las métricas propuestas por un periodo suficiente para establecer un banco de pruebas como base para el análisis, tanto sobre la blockchain BFA como en la Hyperledger desplegada en laboratorio y realizar ajustes en caso de ser necesario. Además se avanzará en lograr indicadores relacionados con aspectos de seguridad en la cadena de bloques, principalmente tratar de medir como es la relación del esquema de seguridad implementado versus las funcionalidades que debe brindar la blockchain.

Referencias

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

[2] Díaz, Francisco Javier; Tugnarelli, Mónica Diana; 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

[3] Ethereum. https://ethereum.org/en/

[4] Hyperledger. https://www.hyperledger.org/use/fabric

[5] 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

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

[7] 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.