Blockchain: “Cadena de bloques”. Reflexiones sobre seguridad y control

Resumen
La tecnología *blockchain* o “cadena de bloques” es una oportunidad que se revela en el contexto de una sociedad digitalmente modificada para acelerar los procesos de desintermediación, descentralización y desinstalación a favor de los individuos y su acceso a productos y/o servicios. En este sentido, este documento explora algunos elementos de su implementación, así como los retos de seguridad y control, con el fin de establecer una reflexión base que llame la atención sobre las actuales y futuras lecciones propias de la inevitabilidad de la falla en esta tecnología.

Palabras clave
Cadena de bloques, *blockchain*, seguridad, criptografía, consenso

Jeimy J. Cano M.

Introducción

En un mundo de cambios acelerados y de mayores exigencias por parte de los consumidores, las tecnologías de información y comunicaciones establecen referentes de transformación, que permiten a los individuos tener mayor participación en la dinámica de la innovación generando expectativas cada vez más desafiantes, que exigen una apresurada convergencia tecnológica.

En este contexto, las personas reconocen nuevos ecosistemas digitales, en los cuales es posible acceder a productos o servicios diferenciados y per-

sonalizados, que permiten concretar una experiencia particular y ajustada con las perspectivas de los clientes. En tal sentido, proliferan las propuestas y demandas de bienes o productos que cumplan requisitos insospechados de los consumidores, quienes en última instancia reclaman menor intermediación, bajos costos en las transacciones y mayores garantías de confiabilidad de las tecnologías de información y comunicaciones.

Estas consideraciones de los nuevos compradores, sugieren el desarrollo de una formade comercio en la que sea posible concretar una relación entre pares que permita negociar de forma confiable, tener un registro de la transacción validado por las partes, mantener la confidencialidad de la negociación y, sobre todo, acceder de forma más ágil y directa al bien o servicio que se requiere. Este nuevo tipo de relación puede generar tensiones con las lecturas actuales de los negocios, particularmente en los entes de supervisión por posibles incrementos de actos contrarios a la ley que se pudiesen suscitar sin un "control central" (Plansky, O'Donnell y Richards, 2016).

La "cadena de bloques" nace como una tecnología que responde a una necesidad de los ciudadanos para recobrar "el control" de sus operaciones y acciones, generando inestabilidad en los estándares actuales basados en la centralización y verificación por parte de terceros. En este sentido, el *blockchain*, representa un desafío para la dinámica social actual, para los Estados, los grupos financieros y en general para las instituciones garantes de la confianza en una comunidad, como quiera que ahora es posible crear relaciones de confianza basados en protocolos de conexión entre pares con medidas de control y verificación que crean mayor confianza.

Si bien este tipo de tecnologías que habilitan la descentralización establecen ventajas de interés para los participantes del contexto empresarial y comunitario, es claro que demandan un reto técnicamente complejo que implica cuidar muchos más detalles en la implementación del mismo. En consecuencia, comprender lo que ocurre técnicamente en la operación de la tecnología *blockchain*, es profundizar en un sistema articulado por un protocolo de comunicaciones abierto, basado en firmas digitales, validaciones de bloques de transacciones, intentos de fraude y diversos participantes, bien en un contexto abierto o en comunidades cerradas.

Por tanto, este documento busca presentar una aproximación a la tecnología de "cadena de bloques" y algunos de sus retos en los temas de seguridad y control que pueden ser de interés para mantener una implementación menos insegura, que dé cuenta de la inevitabilidad de la falla en esta tecnología.

Características básicas de la "cadena de bloques"

La tecnología de cadena de bloques se compone de tres grandes partes, que combinadas e integradas, permiten concretar una sistema de conexión o relación entre pares que aumenta la confianza en las relaciones de los participantes del sistema. Los tres componentes son: la criptografía, la cadena de bloques y el consenso.

La *criptografía* "tiene la responsabilidad de proveer un mecanismo fuerte

de codificación segura de las reglas del protocolo que rigen el sistema", el cual lo hace resistente a la manipulación, robo, introducción de información errónea en la cadena de bloques y asegura las identidades digitales que generalmente están cifradas (Preukschat, 2017).

La *cadena de bloques*, es "la base de datos diseñada para el almacenamiento de los registros realizados por los usuarios", asegurada a través de la criptografía, manteniendo la integridad de la información registrada de cada una de las transacciones realizadas. El cuerpo de cada bloque se compone de un contador de transacciones y las transacciones en sí mismas.

El núme-ro máximo de transacciones que un bloque puede contener depende del tamaño del bloque y el tamaño de cada transacción (Preuk-schat, 2017; Zheng, Xie,Dai, Chen y Wang, 2017).

El *consenso*, es el reto mayor de la tecnología *blockchain*: ¿cómo alcanzar consenso entre pares que no son dignos de confianza? El desafío es asegurar que los libros contables o registros de cada nodo o participante de la red son todos iguales e inalterables. El consenso se basa en "un protocolo común que verifica y confirma las transacciones realizadas, y asegura la irreversibilidad de las mismas" (Preukschat, 2017; Zheng, Xie, Dai, Chen y Wang, 2017).

Estos tres componentes funcionando de manera integrada, constituyen las siguientes características claves de la tecnología de "cadena de bloques" como son: (Zheng, Xie,Dai, Chen y Wang, 2017; Lin y Liao, 2017)

Descentralización. Se habilita la posibilidad de relaciones de confianza entre participantes desconocidos, sin una autoridad central que vigile y verifique, las cuales a través de la interacción de los elementos previamente detallados es capaz de asegurar un registro confiable de las transacciones realizadas.

Persistencia. Las transacciones se pueden validar rápidamente, y aquellas inválidas no serían admitidas por "mineros honestos", es decir aquellos nodos que son capaces de validar las firmas digitales de cada bloque. Es casi imposible eliminar o deshacer transacciones, una vez que están incluidas en la "cadena de bloques".

Anonimato. Cada usuario puede interactuar en la "cadena de bloques" con una dirección generada, que no revela la identidad real del usuario. Nótese que estas direcciones pueden ser rastreables para implementaciones de "cadenas de bloques" públicas. En una implementación privada se puede establecer el nivel de anonimato requerido para realizar o proteger las transacciones.

Transparencia. El registro de datos y su actualización por el sistema "cadena de bloques" es transparente,lo que permite aumentar la confianza entre todos los participantes de la red.

Taxonomía de los sistemas de "cadena de bloques"

De acuerdo con Lin y Liao (2017) existen tres tipos de "cadena de bloques" que se pueden tener en cuenta para adelantar implementaciones de iniciativas usando estatecnología, éstas son: las públicas, las privadas y los consorcios.

Las públicas, en las que cualquier participante puede acceder y consultar las transacciones realizadas, incluso participar del proceso para obtener consenso. Esto supone una red descentralizada de computadores que utiliza un protocolo común asumido por los participantes, para registrar transacciones en la cadena de bloques. Esta implementación supone una base de datos descentralizada de transacciones, dado que no se controla quien participa en la cadena de bloques.

Las privadas en las que, sólo aquellos nodos que han obtenido la condición de usuarios, están sujetos a un protocolo predeterminado, para registro de anotaciones y verificación de cambios en la cadena. En este sentido, se tiene una visión más centralizada de la implementación de una cadena de bloques, en la que cada uno de los nodos asegura la estabilidad del sistema y existe una base de datos repartida en varios nodos.

Finalmente, los consorcios que son conformados por diferentes empresas que crean una cadena de bloques privada y, por lo general, se encuentra asociada a unaplataforma particular. En este tipo de implementación el control de la cadena queda restringido a un número menor de participantes y el consenso lo puede determinar el consorcio.

La figura 1 muestra los tipos de cadenas de bloque.

Retos de seguridad y control de la cadena de bloques

La tecnología cadena de bloques, como cualquier implementación de tecnología es susceptible de la inevitabilidad de la falla. Si bien esta tecnología tiene características que sugieren un alto nivel de confianza en su desarrollo, es importante tener en cuenta que es proclive a limitaciones que pueden comprometer tanto la información como su adecuado funcionamiento. No existe tecnología invulnerable y ésta no es la excepción.

Dentro de los desafíos y ataques a la seguridad de la cadena de bloques, identificados a la fecha, están:

Ataques a las estampas de tiempo. El atacante altera el contador de tiempo de la red del nodo y el nodo engañado puede aceptar una cadena de bloques alternativa. Las graves consecuencias de esto son el doble gasto y el desperdicio de recursos computacionales du-

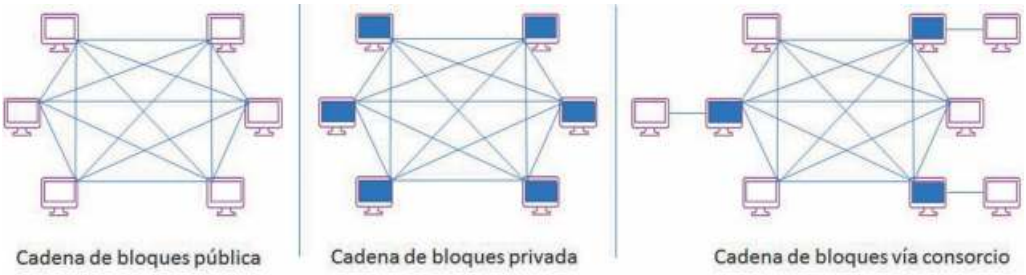

Figura 1. Tipos de cadenas de bloque (Tomada de: Lin y Liao, 2017, p.655)

rante el proceso de minería (Vyas y Lunagaria, 2014). Si esto ocurre en diferentes nodos al tiempo, puede crear un incremento del consumo de energía y afectar la respuesta de sistema en su proceso de validación, así como un incremento de transacciones en espera para ser verificadas.

Ataque del 51%. ¿Qué pasaría si los mineros se pusieran de acuerdo y se coordinaran para falsear la cadena de bloques? Si se quiere alterar la integridad de la cadena de bloques, es necesario tener el 51% del poder computacional de toda red que conforma la cadena de bloque.

Esto es, contar con la misma capacidad de cómputo que el resto de la red, más un uno por ciento (1%) adicional para crear bloques falsos, hacerlos pasar por válidos y anexarlos a la cadena de bloques (Márquez, 2017).

Ataques a los hash de los bloques. El reto en este ataque es alterar el valor del *hash* de una transacción recientemente autorizada, pero no confirmada, sin invalidar la firma. Si la transacción no confirmada llega a un nodo que hace minería y lo hace antes que la transacción válida, será la primera la que quede registrada en los otros nodos. El tiempo de validación de la transacción se vuelve una variable clave para asegurar la dinámica y confiabilidad del sistema como un todo. Esta problemática ha sido corregida en *Ethereum* (Márquez, 2017; Zheng, Xie,Dai, Chen y Wang, 2017).

Como se puede observar con estos tres ataques, el sistema de cadena de bloques se puede ver comprometido y disminuido en su confiabilidad. Parte de la fortaleza de esta tecnología es el uso de criptografía asimétrica basada en curvas elípticas, las cuales gozan de alta resistencia a ataques de criptoanálisis. Sin embargo, esta realidad puede cambiar pronto con la aparición y puesta en operación de la computación cuántica, donde se tiene una capacidad de procesamiento superior, pudiendo debilitar la fortaleza de los algoritmos implementados a la fecha y, por lo tanto, socavar la confianza entre las partes participantes.

Reflexiones finales

Noticias recientes informan que “La industria de la creación de bitcoins consume 22,5 teravatios por hora (TWh) de energía al año, lo que equivale a más- de 13 millones de barriles de petróleo. Al producirse 12,5 bitcoins cada 10 minutos, el costo promedio de energía que se consume para cada uno equivaldría a 20 barriles de crudo” (Stafford, 2017), lo que lo convierte en un negocio rentable, en la medida que éstos se produzcan con electricidad a bajo costo e infraestructura computacional de alto desempeño.

Lo anterior, revela el creciente interés que diferentes sectores manifiestan para utilizar la tecnología de cadena de bloques. En esta línea, se vienen adelantando esfuerzos de estandarización para el desarrollo e implementación de esta tecnología, donde particularmente los consorcios (previamente comentados) están presentes y mantienen un liderazgo evidente, sin perjuicio de las iniciativas articuladas desde la ISO (*International Standard Organization*), como la creación del comité técnico 307 sobre *blockchain* y la tecnología de libro mayor distribuido (en inglés *distributed ledger technologies*) (Anjum, Sporny y Sill, 2017).

Si bien esta tecnología está en sus primeras etapas de desarrollo, es importante anotar que las implementaciones privadas tomarán mayor fuerza a través de los consorcios particularmente en la banca, no obstante las iniciativas en el dominio público que constantemente estarán marcando la pauta en el ejercicio de descentralización, desintermediación y desinstalación que supone el despliegue de la cadena de bloques.

Por su parte, las aseguradoras estarán atentas a concretar con agilidad iniciativas asociadas con contratos inteligentes, que en síntesis son "un código informático que actúa como un acuerdo vinculante entre dos o más partes cualesquiera, sin necesidad de un intermediario, y cuyas cláusulas se programan previamente otorgándole la capacidad de autoejecutarse" (Vivas, 2017, p.140), con lo cual se permite un uso del seguro de manera ágil, confiable y ajustado a la verificación de reglas previamente establecidas, lo que cambia la experiencia de los tomadores de los mismos cuando se requiere la cobertura ante un siniestro particular.

Las consideraciones de seguridad y control, si bien son inherentes a las propuesta de la cadena de bloques, deberán evolucionar para contar con herramientas nativas sobre las diferentes implementaciones que se hagan ahora y en el futuro, para adelantar evaluaciones de vulnerabilidades, efectuar validaciones y correlaciones de registros de auditoría, además de funciones o capacidades para realizar investigaciones forenses y, sobre manera, comprender con claridad cuáles serían las acciones a realizar frente a un incidente que se pueda concretar en una implementación de una cadena de bloques.

El futuro de la tecnología de cadena de bloques aún está por escribirse y por tanto, desde la lectura de la inseguridad de la información, habrá siempre espacio para retar lo conocido hasta la fecha y establecer nuevos escenarios que comprometan tanto a la información como al funcionamiento de la tecnología, no para inutilizar esta propuesta disruptiva, sino para motivar desarrollos que hagan aún más resistentes las implementaciones de la cadena de bloques en mediano y largo plazo.

Referencias

Anjum, A., Sporny, M. y Sill, A. (2017) *Blockchain* Standards for Compliance and Trust. *IEEE Cloud Computing*. July/August. 84-90

Architecture, Consensus, and Future Trends. *Proceedings of 2017 IEEE 6th International Congress on Big Data*. IEEE Computer Society. 557-564. Doi: 0.1109/BigDataCongress.2017.85

Lin, I. y Liao, T. (2017) A Survey of *Blockchain* Security Issues and Challenges. *International Journal of Network Security*. 19, 5. 653-659

Márquez, S. (2017) Seguridad y *blockchain*. En Preukschat, A., Kuchkovsky, C., Gómez, G., Díez, D. y Molero, I. (2017) *Blockchain. La revolución industrial del internet*. Barcelona, España: Gestión 2000. 227-233

Naganuma, K., Yoshino, M., Sato, H. y Suzuki, T. (2017) Auditable zero-

coin.*Proceedings of 2017 IEEE European Symposium on Security and Privacy Workshops (Euro-S&PW)*. IEEE Computer Society. 59-63. Doi: 10.1109/EuroSPW.2017.51

Plansky, J., O'Donnell, T. y Richards, K. (2016) A Strategist's Guide to *Blockchain*. *Strategy+Business*. Issue 82. Spring. Recuperado de: http://www.strategy-business.com/article/A-Strategists-Guide-to-Blockchain

Preukschat, A. (2017) Los fundamentos de la tecnología *blockchain*. En Preukschat, A., Kuchkovsky, C., Gómez, G., Díez, D. y Molero, I. (2017) *Blockchain. La revolución industrial del internet*. Barcelona, España: Gestión 2000. 23-30

Stafford, J. (2017) How Many Barrels Of Oil Are Needed To Mine One Bitcoin? Oilprice Website. Recuperado de: https://oilprice.com/Energy/Crude-Oil/How-Many-Barrels-Of-Oil-Are-Needed-To-Mine-One-Bitcoin.html

Vivas, C. (2017) Aplicaciones transversales de la *blockchain*. En Preukschat, A., Kuchkovsky, C., Gómez, G., Díez, D. y Molero, I. (2017) *Blockchain. La revolución industrial del internet*. Barcelona, España: Gestión 2000. 137-147

Vyas, C. y Lunagaria, M. (2014) Security Concerns and Issues for Bitcoin. *IJCA Proceedings on National Conference cum Workshop on Bioinformatics and Computational Biology NCWBCB.* 2, 10-12.

Zheng, Z., Xie, S.,Dai, H., Chen, X. y Wang, H. (2017) An Overview of *Blockchain* Technology:Architecture, Consensus, and Future Trends. *Proceedings of 2017 IEEE 6th International Congress on Big Data*. IEEE Computer Society. 557-564. Doi: 10.1109/BigDataCongress.2017.85

Jeimy J. Cano M., Ph.D, CFE*. Profesor Asociado. Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph.D in Business Administration de Newport University, CA. USA. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners. Director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS-.*