Blockchain (no todo lo que brilla es Bitcoin)

Gonzalo Luján Villarreal[1]

Desde hace ya algunos años, y en especial durante el año 2017, las criptomonedas fueron noticia en los medios de todo el mundo debido a la falta de controles en su gestión y, sobre todo, al ascenso exponencial de su valor, que ha generado ganancias millonarias para quienes invirtieron tempranamente en estos bienes digitales. El caso más resonante es el del Bitcoin, la criptomoneda más popular y de mayor aceptación a nivel mundial. Sin embargo, existen muchas otras, algunas de ellas muy populares en la comunidad, como Etherium, Ripple, MaidSafeCoin o Lisk. Wikipedia[2] posee una lista actualizada de las criptomonedas actuales más populares, y todo apunta a que nuevas criptomonedas seguirán surgiendo en el corto plazo, impulsadas por particulares, organizaciones e incluso gobiernos (como el reciente anuncio del gobierno de Venezuela del

[1] *Doctor en Ciencias Informáticas, d*ocente-investigador de la Universidad Nacional de La Plata, miembro de PREBI-SEDICI y coordinador del Portal de Revistas, Portal de Libros y Portal de Congresos de la UNLP. Subdirector del Centro de Estudios en Gestión de Información (CESGI) de la Comisión de Investigaciones Científicas de la Provincia de Buenos Aires. Docente de la Facultad de Informática de la Licenciatura en Sistemas, la Licenciatura en Informática y el Doctorado el Ciencias Informáticas . http://orcid.org/0000-0002-3602-8211. *gonzalo@prebi.unlp.edu.ar*[1]
PREBI-SEDICI, Universidad Nacional de La Plata
CESGI, Comisión de Investigaciones Científicas

2 Criptomoneda https://es.wikipedia.org/wiki/Criptomoneda

lanzamiento del "Petro"[3]). Más allá del surgimiento de esta monedas virtuales, es interesante comprender la tecnología que está detrás y que se espera irrumpirá en la forma en que individuos, organizaciones y gobiernos gestionan la información e intercambian todo tipo de bienes y servicios. En líneas generales, todo apunta a la eliminación de intermediarios, la automatización de controles, la agilización en el traspaso de cualquier bien (una casa, un auto, acciones o dinero) y la disminución de costos que todo esto conlleva. Esta tecnología se conoce como Blockchain, y es cada vez más utilizada para múltiples aplicaciones.

Gestión de datos en el siglo XX: datos centralizados

Las aplicaciones informáticas, y las organizaciones que las emplean, han utilizado en las últimas décadas las bases de datos como la principal herramienta para gestionar y acceder a su información. Una base de datos, en el sentido tradicional, es un conjunto de archivos que mantienen información estructurada en entidades relacionadas entre sí. Estos archivos son alojados en un contenedor físico (por ejemplo, un disco rígido dentro de un servidor), y son accedidos a través de un software, conocido como servidor de bases de datos, que brinda distintos servicios sobre las bases de datos de gestiona:

- autenticación (¿quién puede acceder a los datos?);
- autorización (¿a qué datos accede cada usuario?);
- integridad (los datos y las relaciones entre ellos son almacenados de manera segura, evitando así su corrupción y posterior pérdida);
- acceso eficiente (mediante la construcción de índices, planificación de consultas, bloqueos temporales de registros, etc.);
- transacciones (permite realizar operaciones complejas, que involucran muchos datos, de manera segura);

3 Maduro anuncia la creación del Petro, la criptomoneda de Venezuela. Fuente: Diario El Mundo, España. http://www.elmundo.es/internacional/2017/12/03/5a24553922601d8a298b461b.html

- replicación (mantenimiento de múltiples copias de toda o parte de la base de datos, a fin de brindar un acceso más eficiente –por ejemplo, por ubicación geográfica- y minimizar la pérdida de información).

En este modelo, los usuarios de la base de datos (las aplicaciones que la utilizan) no tienen acceso directo a los archivos, sino que existe una única entidad "autorizada" (el servidor de bases de datos) que se encarga de brindar los accesos a la información contenida. De este modo, esta entidad es la encargada de hacer de intermediaria entre usuarios que necesitan intercambiar información utilizando este banco de datos centralizado. La entidad mantiene control total sobre los datos, determina las regulaciones, restricciones y formas de acceso a ellos, y sirve finalmente como un intermediario que brinda confianza entre las partes que realizan las transacciones.

Así es como, por ejemplo, los bancos y entidades financieras registran y mantienen información sobre las transacciones que realizan sus clientes, los mercados de acciones registran el traspaso de acciones entre las personas, o los registros automotores mantienen información (registros) sobre el o los dueños de cada vehículo. Si tomamos el caso del banco, un cliente quiere transferir dinero de una cuenta a otra, solicita al banco realizar la operación, el banco autoriza (o rechaza) la operación, y luego actualiza los registros correspondientes: movimiento de egreso en la cuenta origen, movimiento de ingreso en la cuenta destino, y saldos de ambas cuentas. Finalmente, cobrará al cliente algo de dinero por los servicios que brinda sobre su dinero. Si más de un banco interviene en esta operación, ambas entidades mantendrán sus propias copias de estos movimientos, lo que genera nuevos costos, retrasos y la necesidad de conciliar los registros entre las entidades.

Datos distribuidos: un nuevo paradigma para la gestión de la información

La Blockchain, o cadena de bloques, es una forma completamente diferente de gestionar datos. En vez de tener una única copia centralizada de los datos, todos los nodos que conforman la red tienen su propia copia de la blockchain, y esta copia es idéntica para todos los nodos. Al alterarse una copia, las modificaciones se replican (casi) instantáneamente en todos los nodos de la red, lo que equivale a mantener un libro de movimientos

compartido donde se registra toda la historia de las transacciones. Se podría imaginar esto como una gran planilla de cálculo, duplicada miles de veces en una red de computadoras diseñada especialmente para actualizar la planilla regularmente. La información mantenida en una blockchain existe como una base de datos compartida que es continuamente conciliada entre las partes. Al no existir una única copia de la blockchain, los registros son públicos para todos los nodos y fácilmente verificables por cualquiera de ellos. Esto también minimiza el accionar de los hackers, ya que no existe una base de datos centralizada para hackear o corromper, sino miles o millones de copias que son revisadas y verificadas constantemente.

El nombre Blockchain se da a partir de la estructura con la que se organizan los registros en este gran libro compartido. Cada vez que se genera una nueva transacción, esta se inserta en un bloque lógico de información, agrupado junto con otras transacciones. Cada bloque de transacciones es incorporado a una lista de bloques, conectándolo con el bloque anterior mediante un enlace. De ahí el concepto de "cadena": cada bloque, conformado por un conjunto de transacciones, forma un eslabón de la cadena.

Sin embargo, a diferencia de las bases de datos tradicionales, existe una particularidad en cuanto al tipo de modificaciones que pueden realizarse sobre una blockchain: una vez que una transacción ha sido incorporada a este registro, no puede modificarse ni eliminarse. En caso de alterar el contenido de una transacción, los algoritmos de control de integridad detectarán un problema de inmediato dado que la firma o marca de seguridad, basada en criptografía, se alterará con dicho cambio y no coincidirá con el valor esperado. Por lo tanto, en caso de querer deshacer (eliminar) una transacción, la única opción posible es generar una nueva transacción *opuesta* a la que se quiere deshacer. Por ejemplo, si la blockchain gestiona acciones de empresas, y si el usuario A le entregó por error X acciones de la empresa E al usuario B, la única forma de deshacer esta transacción es generar una nueva donde el usuario B le entregue X acciones de la empresa E al usuario A.

Este modelo distribuido podría, como es de esperarse, abrir la puerta para fraudes o engaños: un nodo malintencionado podría alterar el contenido de una transacción, o incluso podría sumar unilateralmente

transacciones a un bloque. Esto generaría en dicho nodo una copia de la blockchain diferente de la que poseen otros nodos, que intentará replicar en la red. Ya se ha visto que no es posible alterar una transacción ya incorporada sin que otros nodos noten este cambio, pero ¿cómo se evita que un nodo adicione transacciones por su cuenta? Antes de incorporar una transacción a este banco de datos compartido, todas las partes deben aprobar esta transacción, mediante lo que se conoce como *algoritmos de consenso.* Estos algoritmos de consenso constan de una serie de reglas que permiten determinar si una copia de la blockchain es válida o no. De este modo, si un nodo introduce unilateralmente cambios en una blockchain, cuando intenta distribuir esta información en la red de nodos, estos detectarán de inmediato la incongruencia y desestimarán esa copia de la cadena, aislando de la red al nodo que intentó introducir el cambio hasta tanto (en el mejor de los casos) no corrija el error, lo que equivale a obtener una copia válida de la cadena.

Veamos un ejemplo concreto: supongamos que alguien desea registrar una transacción en esta Blockchain. Para ello, envía una solicitud de registro, que es diseminada por una red de computadoras (nodos). Estos nodos utilizan algoritmos para determinar la validez de la transacción, y en caso de verificarse satisfactoriamente, la transacción se combina con otras para formar un bloque de datos para el libro de movimientos. Este bloque se suma a la cadena de bloques que cada nodo posee, de manera permanente e inalterable. Dependiendo de las características de la blockchain (el algoritmo de validación, la información que se registra en cada transacción, etc.), una transacción verificada podría involucrar criptomonedas (ej. Bitcoin), contratos, acciones, registros o cualquier otra información.

Participación y privacidad

La tecnología de la blockchain permite implementar cadenas públicas, donde cualquier usuario de internet puede participar como un nodo de la red, o cadenas privadas, donde sólo ciertos usuarios podrán incorporarse como nodos de la red. En ambos casos, todos los usuarios que desean sumarse como nodos a la red deberán cumplir ciertas condiciones preestablecidas, y la principal diferencia entre una cadena pública y una cadena privada es cómo se gestionan tales condiciones. Como es de esperarse, las cadenas privadas poseen

estrictos sistemas de control que permiten a usuarios con ciertas credenciales el acceso y modificación de la cadena, y dichas credenciales son también gestionadas por la red de nodos participantes. Asimismo, las distintas implementaciones de blockchains permiten definir distintos niveles de privacidad, determinando así qué usuarios de la red pueden leer información sobre transacciones y qué información de cada transacción puede ser leída por cada usuario. Todas las funcionalidades de control de ingreso, gestión de permisos y aseguramiento de la privacidad de los registros son implementadas mediante técnicas de encriptación de datos e intercambio de claves públicas y privadas entre usuarios, tecnología como SSL que ya existe desde hace mucho tiempo y es ampliamente utilizada por todos los usuarios de Internet (por ejemplo, mediante sitios que utilizan el protocolo HTTPS) al realizar operaciones que requieren un alto nivel de seguridad, como por ejemplo al utilizar el Home Banking o al acceder la casilla de correo.

Aplicaciones

La tecnología de la blockchain ofrece a los usuarios de internet la habilidad de crear valor y autenticar información digital. Esto trae un mundo de nuevas aplicaciones para los negocios y el gobierno. Algunos ejemplos incluyen las criptomonedas y los sistemas de pagos, como por ejemplo Bitcoin (Bitcoin, 2009) o Etherium (Etherium Project, 2017), los sistemas de voto electrónico (Barnes, 2017), servicios financieros comerciales (Gupta, 2017), seguros (Gupta, 2017), gobierno abierto (Gupta, 2017), sistemas de salud (Gupta, 2017), almacenamiento de archivos descentralizado (Butterin, 2014), entre otros.

Tomemos por ejemplo una hipotética aplicación de una blockchain para un sistema nacional de salud. Esta blockchain mantiene un registro de toda la información de cada individuo del sistema: estudios, internaciones, enfermedades, actores que intervinieron y sus respectivos roles (hospitales, médicos, enfermeros, laboratorios, obras sociales), pagos, autorizaciones, etc. Toda esta información estará disponible para todas las partes, pero no todas las partes podrán acceder a toda la información por igual, sino que se utilizarán sistemas de seguridad que asegurarán que cada actor pueda acceder sólo a la información que le es permitida. Por ejemplo, cada individuo podría autorizar a un médico a ver toda su historia clínica, lo que

implicaría compartir una clave especial entre ambas partes. El médico podría solicitar un estudio o tratamiento para un individuo, que en términos de la blockchain implicaría agregar una transacción que tanto el médico como el individuo podrán acceder; este a su vez podrá autorizar a la obra social para acceder a la información del estudio y tratamiento, y la obra social podría emitir una autorización (o sea, generar una nueva transacción) para que el centro de salud o laboratorio realice el estudio o tratamiento requerido por el médico para el individuo en cuestión. Toda esta información será accesible sólo por las partes intervinientes, incluso cada parte podría acceder sólo a una porción de la información. Esto no sólo asegura la privacidad de la información, sino que agilizaría enormemente el intercambio de datos entre las partes (médicos, pacientes, obras sociales, centros de estudios…) y brindaría un mecanismo sumamente eficiente para realizar el seguimiento de cada transacción dentro del sistema, desde que el médico realiza la solicitud hasta que la obra social abona el tratamiento al centro de estudios.

Una mención especial merecen los contratos inteligentes (Buterin, 2014; Delmolino, 2016) que, dicho de manera simple, consisten en un conjunto de reglas que se validan y, cuando se cumplen las condiciones establecidas, se ejecutan automáticamente (por ejemplo, haciendo efectivo el intercambio de bienes o pagos entre las partes). Este tipo de herramientas sirven de base para automatizar las múltiples aplicaciones de la blockchain, eliminando así intermediarios y agilizando enormemente las transacciones. De este modo, además de registrar los movimientos o transacciones entre múltiples partes en una cadena distribuida, estas transacciones pueden incluir las reglas que conforman un contrato entre las partes, el cual se ejecutará automáticamente y generará, posiblemente, nuevas transacciones o incluso contratos derivados. El uso de contratos inteligentes está al día de hoy en sus comienzos, con contratos relativamente sencillos que seguramente irán avanzando en tamaño (cantidad de reglas) y en complejidad (reglas más avanzadas).

En resumen, el cambio de paradigma que propone el uso de la tecnología de Blockchain para la gestión de transacciones entre pares ofrece grandes ventajas, especialmente debido a la supresión de intermediarios y su consiguiente reducción de costos, la transparencia, la trazabilidad, la seguridad y a la agilización de los procesos.

Sin embargo, esto requiere también un cambio estructural muy profundo en las organizaciones y en los gobiernos para adoptar sus procesos a las nuevas herramientas y para aplicar las regulaciones y controles correspondientes. En particular, será un gran desafío para los gobiernos el control y monitoreo en aquellos casos donde las aplicaciones de esta tecnología permiten generar medios de pago alternativos (por ejemplo criptomonedas), que funcionan de manera descentralizados, a escala mundial y fuera del control de los organismos oficiales. De continuar la tendencia de los últimos años, en el futuro cercano veremos surgir nuevos proyectos, aplicaciones y servicios basados en la Blockchain y que, como ha sucedido con la irrupción de grandes avances tecnológicos –desde la revolución industrial hasta Internet– podría impactar en todos los sectores de la economía, la gobernanza y la sociedad en general.

Referencias

1. Bitcoin.org (2009). Bitcoin Developer Guide. Disponible eb: https://bitcoin.org/en/developer (último acceso: 18 de diciembre de 2017)
2. Blockchain for dummies (2017). Manav Gupta. IBM Limited Edition. Publicado por John Wiley & Sons, Inc.
3. Vitalik Buterin (2014). Ethereum White Paper. A next generation smart contract & descentralized application platform. Disponible en https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (Último acceso: 18 de diciembre de 2017)
4. Delmolino K., Arnett M., Kosba A., Miller A., Shi E. (2016) Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9604. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-53357-4_6

5. Digital Voting with the use of Blockchain Technology. Andrew Barnes, Christopher Brake and Thomas Perry. Team Plymouth Pioneers, Plymouth University. Disponible en https://www.economist.com/sites/default/files/plymouth.pdf (últmo acceso: 18 de diciembre de 2017).
6. Etherium Project. Disponible en https://www.ethereum.org (Último acceso: 18 de diciembre de 2017).
7. Proof of Work vs Proof of Stake: Basic Mining Guide. An in-depth guide by BlockGeeks. Disponible en https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/ Último acceso: 18 de diciembre de 2017.
8. The World of Blockchain (2017). Alejandro Reyes, University of Michigan. Disponible en https://medium.com/michiganblockchain/the-world-of-blockchain-f3b268e3d748