SDC Supervielle - de Cores Abogados

Tecnología & Derecho

JUNIO 2018

¿Por qué debería confiar en una Blockchain?

HABLEMOS DE CONFIANZA

Por Sandra Garín

Cuando comenzamos el abordaje de la tecnología blockchain, hay una palabra que se repite una y otra vez: confianza.

Nacida como la tecnología que permite el funcionamiento de un sistema de pago electrónico completamente realizado entre pares, esto es, indiferente a cualquier autoridad emisora o controladora de los saldos, lo cierto es que, combinando distintas tecnologías preexistentes, las blockchain tienen la potencialidad, eventualmente, de sustituir a cualquier tercero de confianza.

Pero ¿qué es lo que haría esta potencialidad efectivamente factible?

Según lo que trasciende, parecería ser que la blockchain nos hace esta oferta: sustituir personas, instituciones, entidades públicas y privadas por matemática, criptografía, software, etc.

Y nosotros nos preguntamos ¿por qué deberíamos confiar en una blockchain en lugar de entidades y personas que han ganado nuestra confianza luego de décadas, incluso siglos, dentro de la corta historia de la humanidad?

Es fácil notar que dependiendo de las características de los depositarios de confianza, varía el ámbito donde despiertan sus entusiastas y seguidores. No es de extrañar que los primeros que hayan depositado confianza en esta tecnología, hayan sido integrantes del ecosistema tecnológico.

Sin embargo, en muy poco tiempo, esta tecnología se ha hecho un lugar en la industria, no sólo financiera (para la que fue originalmente creada), sino que ha demostrado ser extremadamente versátil, encontrándose en pleno desarrollo para distintas aplicaciones industriales, registrales, comerciales, resolución de controversias, etc.

¿QUÉ ES BLOCKCHAIN?

Podemos encontrar muchas definiciones de blockchain, algunas ponen más énfasis en la utilidad que tendría que en las características de la tecnología en sí misma. Creemos que poner énfasis solamente en la utilidad que hoy en día se conoce, tiene el riesgo de dar una visión muy limitada al respecto, dado que cada progreso técnico, o nuevo desarrollo, afectaría esa definición.

Podemos afirmar que una blockchain es una base de datos (información) que tiene las siguientes características: **i)** la información se registra de forma cronológica - cada registro o asiento se denomina transacción- y por ello, también se

habla de "*ledger*"; **ii)** las transacciones pasan a integrar grupos de transacciones denominados bloques (de ahí parte del nombre) -aunque podrían haber casos de un bloque por cada transacción-; **iii)** cada grupo de transacciones se enlaza al grupo de transacciones siguiente, lo que ocasiona que cuanto más bloques se generan luego de cada transacción, se fortalece la inmutabilidad de la misma, generando la cadena (segundo componente del nombre); **iv)** la totalidad del registro de transacciones se encuentra en poder de cada uno de los miembros, cada anotación es enviada a todos los integrantes (sistema distribuido); **v)** el sistema distribuido implica que ninguno de los miembros por sí solo puede alterar las anotaciones, estando regido por reglas (protocolo de consenso).

Adicionalmente, sobre estas cadenas de información pueden ejecutarse programas, como los Smart Contracts, aspecto que se encuentra en pleno desarrollo.

Pero ¿por qué debería generar confianza esta forma de registro de información?

Sin dudas la respuesta viene por el lado de la tecnología aplicada. Destacamos que todas las herramientas que se utilizan para la construcción de la blockchain, ya existían de forma independiente, y lo innovador fue ponerlas a trabajar conjuntamente.

LA CIENCIA DETRÁS DE LA CONFIANZA

En las blockchain se usan las siguientes herramientas matemáticas/criptográficas y tecnológicas, existiendo algunas particularidades o variantes de una blockchain a otra, pero que pueden describirse con carácter general más o menos así:

1. Utilización de funciones hash (criptografía): las funciones hash se utilizan tanto para la formación de la firma digital (que se traduce en una clave pública y una clave privada), así como para armar las cadenas de forma ordenada. Lo importante que hay que retener de las funciones hash es que dada determinada entrada (valor, texto, archivo), se obtendrá un valor alfanumérico de longitud fija. Es muy poco probable que dos entradas distintas den un mismo hash (colisión), así como también, cualquier alteración en la entrada, tiene como resultado un valor distinto. El cálculo es unilateral, esto es, teniendo la entrada, es muy fácil obtener el valor del hash, pero lo contrario es extremadamente difícil. Esto hace que sea una herramienta de muy fácil uso para comprobar la autenticidad de una entrada, ya que se aplica la función hash y se comparan los resultados. La consecuencia es la fidelidad de la información registrada, así como también contribuye a la inmutabilidad (al utilizarse para la formación de los bloques); alterado un valor, deberían reconstruirse todos los siguientes bloques, lo que es difícil por aplicación del punto 3.

2. Sellado de tiempo: la marca de tiempo se produce por un protocolo que da certeza de que un evento (dato) se ha producido en determinado momento y no ha sido alterado con posterioridad. La novedad es que en la blockchain, este dato se integra al hash y se enlaza con la marca temporal anterior.

3. Sistema distribuido: este mecanismo permite que los miembros (aspecto que varía dependiendo del tipo de blockchain) tengan acceso al registro completo. Para regular su funcionamiento se utilizan protocolos de consenso que implican más o menos energía y hardware dependiendo del algoritmo. Esto hace que modificar una anotación sea muy difícil, porque se requiere que la mayoría se ponga de acuerdo en modificar el protocolo. Este punto, tiene una debilidad y es que si, por acaso, un pequeño grupo controlara la mayor parte de la red, podría modificarse la anotación. Es por ello que también, una blockchain controlada por una sola entidad o por unos pocos, carecería de sentido.

Justamente, lo que se afirma, es que el conjunto de todas estas herramientas, permiten la interacción entre sujetos que no tienen confianza alguna entre sí. En este sentido, podemos observar, claramente, la influencia en un posible cambio en la instrumentación de distintos hechos de la realidad que deben ser contemplados y considerados: **¿podría implicar un cambio conceptual del documento público y de la autenticidad? ¿se podría desconocer un documento cuyo hash coincide? ¿y el sello de tiempo?** Es fácil ver las oportunidades y desafíos que tenemos por delante.