



asuntos
públicos

— .cl



Centro de estudios del desarrollo

f /asuntospublicos

@ced_cl

Novedades

28/12/2018

Economía

Aproximaciones a la tecnología BlockChain y posibles implementaciones en Chile

21/12/2018

Política

El ideal de la participación deliberativa: conceptos básicos y desafíos para Chile

23/11/2018

Política

Oposiciones Políticas a Gobiernos Democráticos: Definiciones y roles para el caso chileno

19/10/2018

Política Sectorial

Breve comentario sobre las invenciones de los trabajadores en la empresa

08/10/2018

Política Sectorial

Comentarios sobre la propuesta del nuevo crédito SIFS para la Educación Superior

Acerca de

Este informe ha sido preparado por el Consejo Editorial de asuntospublicos.cl.

©2000 asuntospublicos.cl.
Todos los derechos reservados.

Se autoriza la reproducción, total o parcial, de lo publicado en este informe con sólo indicar la fuente.

Informe 1346

Economía

28/12/2018

Aproximaciones a la tecnología BlockChain y posibles implementaciones en Chile

Diego Córdova Yukich¹

Durante el 2018, BlockChain fue la tecnología disruptiva² de moda. Acaparó la atención en seminarios, artículos y agenda pública. De hecho, a comienzos del año 2018, el Ministerio de Economía, Fomento y Turismo convocó a seis mesas de trabajo público-privadas para la elaboración de un informe respecto a BlockChain y su uso en sectores estratégicos.

El objetivo de este informe es dar una aproximación a la tecnología BlockChain, el contexto preliminar, sus características, atributos y limitaciones, además de dar a conocer los usos e implementaciones que podría tener esta tecnología en Chile según el informe del Ministerio de Economía. Éstos se concentran en seis áreas específicamente: Comercio, Servicios Financieros, Identidad Digital, Sistemas Registrales, Energía y Salud.

I. Contexto de origen

Antes de entrar a definir qué es la tecnología BlockChain, considero importante, en primer lugar, prestar atención al contexto bajo el cual esta se origina.

Entre finales de la década de los ochenta y comienzos de los noventa, a propósito del crecimiento explosivo de Internet, surge un grupo de individuos que velaba por la privacidad y seguridad de las comunicaciones en la red conocido como los Cypherpunks. En torno a estos intereses, comienzan a implementar mayores estándares de criptografía en Internet para alcanzar la privacidad de los usuarios, potenciaron procesos de anonimización y, entre otras cosas y siguiendo la lógica de la privacidad en la red, comienzan a dibujar las primeras nociones del efectivo digital y anónimo. Sin embargo, la infraestructura tecnológica de la época hacía inviable su implementación.

Años más tarde, en el año 2008, el mundo sufre un importante colapso económico: La crisis subprime, generándose especial desconfianza en instituciones como empresas, bancos y gobiernos.

¹ Abogado, Universidad Diego Portales, Magister en Derecho Civil Patrimonial de la misma casa de estudios, Consejero del Instituto Chileno de Derecho y Tecnologías, y Asociado en Gutiérrez & Arrieta Abogados. Contacto: diego.cordova@ga-abogados.cl

² Una tecnología disruptiva se define como "aquella que rompe con el status quo y lleva a nuevos productos y/o servicios". Ejemplo de hace unos años atrás serían los smartphones.

En este contexto aparece el misterioso Satoshi Nakamoto, desconociéndose realmente quién es, dudándose incluso si acaso se trata de una persona real o más bien se trata de un seudónimo o incluso una agrupación.

Con la aparición de Nakamoto se retoma la idea del dinero digital y anónimo, instalada en los noventa por los Cypherpunks, al publicar su artículo³ en el que se concibe por primera vez el BitCoin como una moneda 100% digital y desintermediada.

Estas características de BitCoin, el ser digital, en primer lugar, y desintermediado, en segundo lugar, hace que éste cuente con dos desafíos:

1. Requiere hacerse cargo del “problema del Doble Gasto”.
2. Por la desconfianza en las instituciones eliminar a las autoridades intermediarias.

En primer lugar, corresponde hacerse cargo del problema del Doble Gasto. Y para ello conviene presentar el problema con un ejemplo: Juan envía un documento PDF por correo electrónico a Daniela. Daniela, como destinatario recibirá una copia, sin embargo, Juan también conservará una copia y podrá disponer de ella cuantas veces quiera.

Hasta antes del BitCoin existía lo que se conoce como “Internet de la Información”. El uso de Internet estaba marcado por permitir compartir información, como en el ejemplo. Sin embargo, ¿Qué pasa cuando uso Internet ya no para compartir información, sino que para compartir valor como dinero? Ejemplo: Si Juan envía (digitalmente) \$100 a Daniela, la idea es que no pueda volver a usar esos \$100. Ya que, al tratarse de valor, supone que el dinero ya no está en el patrimonio de Juan, como ocurriría en el mundo físico.

La respuesta que intuitivamente debiera surgir es pensar en los bancos o instituciones financieras como entidades de confianza. De hecho, así es como funcionan las transacciones electrónicas y como se habían desarrollado hasta antes del BitCoin.

Sin embargo, y aquí aparece el segundo problema del cual se hace cargo BitCoin, cabe recordar que, tras haberse perdido la confianza en las instituciones intermediarias a propósito de la Crisis Subprime, lo que Satoshi Nakamoto pretende es, justamente, prescindir de ellas.

La solución a estos dos problemas o desafíos que plantea BitCoin se encontró en el desarrollo de la tecnología BlockChain o “Cadena de Bloques”. Y es esta tecnología, más que el BitCoin, lo que ha llamado más la atención de los expertos. Advierto al lector que, de aquí en adelante no profundizaré más respecto al BitCoin ni a las criptomonedas, para concentrarme derechamente en la tecnología que soporta a estas: BlockChain.

II. ¿Qué es BlockChain?

Por una razón pedagógica, a continuación, se responderá la pregunta ¿Qué es BlockChain? por medio de la presentación, en forma parcelada, de sus principales características.

³ Nakamoto, Satoshi en “Bitcoin: a peer to peer electronic cash sistem”, disponible (en inglés) en <https://bitcoin.org/bitcoin.pdf>

1. BlockChain es una base de Datos Distribuida entre nodos

La tecnología BlockChain fue diseñada como una base de datos que opera como si fuese un libro de contabilidad público para el registro de las transacciones hechas en BitCoin.

Que sea “distribuida” quiere decir que se aloja en todos y cada uno de los servidores participantes de la red de BlockChain como si se tratara de un entramado de servidores. Cada uno de estos servidores conectados que participan de la red se conocen como “nodos”.

La lógica que está detrás de las redes distribuidas permite, consecuentemente, la implementación de un modelo de confianza distribuida, el cual se diferencia de los modelos tradicionales de confianza centralizada en los cuales una tercera parte autorizada y de confianza concentra el poder de decisión y, consecuentemente, es el depositario exclusivo de la confianza en la red. De este modo, la tecnología BlockChain propicia que, prescindiendo de la autoridad de control, los participantes de la red se vinculen unos con otros sin que ninguno de ellos tenga poder de alterar la información compartida o incluir transacciones que no satisfagan las reglas acordadas⁴.

Adicionalmente, las redes distribuidas entre varios nodos permiten disponibilidad operacional de la solución tecnológica, en contraposición a las redes centralizadas. Por ejemplo, con aplicaciones como WhatsApp, Facebook o Netflix, cuando se “cae el sistema”, al tratarse de un servicio centralizado, colapsa el servicio a nivel general. Si estas mismas aplicaciones corrieran de forma distribuida, su disponibilidad operacional sería mayor.

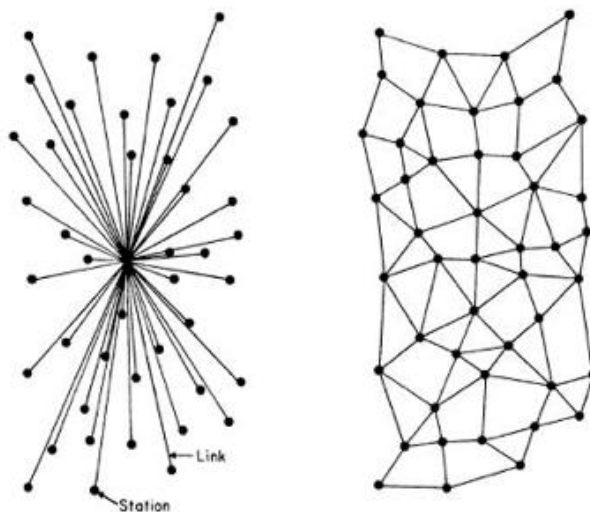


Figura n°1: diferenciación entre redes centralizadas y distribuidas

⁴ Ministerio de Economía, Fomento y Turismo, Informe BlockChain, un camino a la 4ta Revolución Industrial, p. 6.

2. BlockChain es un registro inmutable encadenado en “bloques”

El registro de información contenida en BlockChain se hace por medio de “bloques”. Cada bloque contiene una marca de tiempo junto con un enlace al bloque anterior, con ello permite que el registro de transacciones se ordene en forma cronológica y sin aceptar modificaciones, de manera que solo se añade información, quedando un registro histórico y acumulativo de información.

Estos bloques son, consecuentemente, sucesivos, consensuados y seguros. Y se van ligando en cadena al bloque anterior por medio de criptografía avanzada. BlockChain al tratarse de una red distribuida, permite que, una vez generado un bloque, este se replica en todos y cada uno de los nodos participantes de la red⁵.

3. BlockChain utiliza criptografía avanzada y “mineros”.

Para generar un bloque, consolidarlo y agregarlo a la cadena es necesario resolver un algoritmo criptográfico. El cual, una vez que éste es resuelto, habilita que el bloque sea validado y replicado entre todos y cada uno de los participantes.

En el lenguaje de BlockChain a quienes resuelven este algoritmo se les denomina “mineros”. Los mineros son, básicamente, los nodos que ofrecen su poder de procesamiento computacional para competir por ser el primero en descifrar el código del bloque anterior para, así, validar el siguiente bloque de información que se añadirá a la cadena. Una vez resuelto el algoritmo, y validado por los demás nodos, el bloque se une a la cadena y el minero que ha resuelto el algoritmo recibe un porcentaje de la transacción como premio.

III. ¿Por qué estas características hacen de BlockChain una red segura y de confianza?

En consideración a que su base de datos se encuentra distribuida en múltiples dispositivos a la vez, sin una base de datos central o bien, prescindiendo de un sistema centralizado, dificulta que sea hackeada, o alterada.

Adicionalmente, al encontrarse encriptada, además de ser almacenada con indicación exacta de fecha y hora, hace que cualquier modificación o intento de ataque difícilmente pase inadvertido. La implementación de criptografía avanzada, hace de BlockChain una tecnología sumamente segura ya que, para ser atacada, sería necesario, en primer lugar, contar con un poder de procesamiento tal que permita alterar el código y, en segundo lugar, necesitaría ser atacado el total de los nodos en el mismo instante. Esto redundaría en que para aquel nodo que quiera hacer trampa resulte más sencillo seguir las reglas del sistema que intentar romperlas⁶.

⁵ Nakamoto, op cit, p. 6.

⁶ Jens Hardins, “BlockChain” en “Bits de Ciencia: Temas candentes en ciencia de la computación”, Departamento de Ciencias de la Computación, Universidad de Chile, 2017, p. 45.

IV. De los posibles usos de la tecnología BlockChain y su implementación en Chile

Al tratarse de una tecnología desarrollada a propósito del registro de transacciones de criptomonedas ha llamado especialmente la atención dentro de la industria financiera como bancos e instituciones financieras.

Un ejemplo de la aplicación del sistema BlockChain dentro del ámbito de las operaciones de dinero es con las remesas:

Imaginemos un inmigrante haitiano que quiere enviar dinero a su familia desde Chile a Haití, la comisión sería mucho más baja por medio de una red descentralizada como BlockChain, pagándose un porcentaje al minero que resuelve el algoritmo y valide el bloque. En cambio, si lo hiciera por medio de los actores tradicionales, los porcentajes de comisión serían más altos y, consecuentemente, llegaría menos dinero a la familia en Haití.

Sin embargo, su importancia trasciende al ámbito financiero, toda vez que posibilita la gestión de información compartida en una plataforma única, que permite compartir información y abarcar a todos sus participantes manteniendo, en base a su tecnología, certeza y seguridad en el sistema.

El impacto de la desintermediación posibilita aplicaciones en diversas industrias en que el registro confiable, transparencia y costos de transacción son variables críticas.

Fuera del sector financiero, por ejemplo, está el caso del MIT, que desarrolló una aplicación denominada BlockCerts⁷, por medio de la cual permitió a sus egresados el acceso a los certificados en formato digital por medio de una aplicación para smartphones.

En BlockChain registra una clave pública y a cada egresado se le envía su correspondiente clave privada. Al alojarse los datos ya no a nivel centralizado en la red de MIT, si no que en un sistema descentralizado como BlockChain permite a los egresados el manejo de sus datos al contar ellos con la clave que permite dar con el certificado.

A nivel nacional, a propósito de las distintas aplicaciones de uso que se visualiza para la tecnología BlockChain, a finales de la administración de Michelle Bachelet el Ministerio de Economía convocó una mesa de trabajo público privada para evaluar las posibilidades de implementación de esta tecnología. El resultado de este trabajo arrojó, en agosto de 2018 y bajo la administración de Sebastián Piñera, un informe en que se da cuenta de posibles usos de esta tecnología en 6 sectores estratégicos para evaluar si resulta conveniente o no la aplicación de esta nueva tecnología⁸:

1. Identidad Digital

Se identificó como principal desafío, la multiplicidad de mecanismos de autenticación disponibles en Chile. Así, teniendo como referentes los casos de Suiza y Brasil, se llegó a la conclusión de que BlockChain permitiría implementar un sistema en que los datos y modelos de identificación se encuentren unificados, incorporando diversos niveles de autenticación.

⁷ Para más información sugiero visitar <https://www.blockcerts.org/>

⁸ El informe completo está disponible en el siguiente enlace: <http://energiaabierta.cl/estudios/>

2. Comercio

En el caso de la aplicación de BlockChain en el comercio, se tomó en cuenta los principales ejes que éste tiene en la actualidad: Pago, logística, comercio exterior y comercio electrónico. Al respecto se identificó la seguridad como el principal atributo que ofrecería BlockChain.

3. Servicios Financieros

Considerando que BlockChain nace a propósito del BitCoin como un sistema alternativo de moneda, se identificó como principales oportunidades la implementación de la tecnología en los medios de pago y en financiamiento.

A propósito de los medios de pago se identificó la posibilidad de generar una Criptomoneda estable que tenga su equivalente en pesos. Y, respecto del financiamiento, se identificó la posibilidad de implementar la tecnología BlockChain en iniciativas como Crowdfunding, financiamiento contra facturas y como modelo de compensación de facturas por pagar.

4. Sistemas registrales

En este caso se concentró el estudio, principalmente, en el uso de BlockChain en el sistema de registro de propiedad de los Conservadores de Bienes Raíces. Al respecto se tomó como referencia los casos de Estonia, Dubai y Suecia. Identificándose casos como el de Estonia en que no es BlockChain la tecnología que soporta el sistema registral.

En base a ello se concluyó que, si bien la digitalización de los Conservadores se ha iniciado hace diez años. No se ha nivelado el estándar de digitalización, teniendo Conservadores que van a la vanguardia en materia de tecnología y otros que están desactualizados de una forma preocupante. Ante esa realidad, se consideró como una solución más realista el nivelar el estándar –al menos- al nivel tecnológico disponible en la plataforma “Conservadores Digitales”⁹.

5. Energía

Este grupo de trabajo, reconociendo especialmente los atributos de la tecnología BlockChain, identificó que su aplicación en la industria energética permitiría certificar datos e información de Energía Abierta. De hecho, en la actualidad, el sector energético chileno es de las industrias pioneras en la implementación de BlockChain en Chile.

Otra implementación que se ha identificado es el manejo de datos del “Sello sol”, certificación que da cuenta del uso de energía solar en la elaboración de productos y/o servicios.

Además, cabe mencionar, este grupo de trabajo hace mención a un importante problema que presenta BlockChain: su ineficiencia a nivel energético. El poder de procesamiento que exige esta tecnología es tan alto, que su gasto energético ha llamado especialmente la atención de organizaciones medioambientales y grupos que luchan contra el cambio climático.

⁹ Ministerio de Economía, Fomento y Turismo, op cit, p. 29

6. Salud

En la industria de la salud, se analizó la implementación de BlockChain en subtemas: infraestructura de datos sanitarios, administración de registros personales, analítica de datos, Internet de las Cosas aplicada a dispositivos médicos, identificación digital, cadena de abastecimiento, telemedicina y otros.

Este grupo definió los siguientes puntos como principales para el uso de la tecnología BlockChain: Optimización del sistema de lista de esperas del sistema GES; Uso transparente de las recetas médicas y la gestión de los datos médicos por parte del paciente.

V. A modo de conclusión

Entender la operativa de la tecnología BlockChain no es tarea sencilla. En tal sentido cabe advertir que hay muchísima literatura al respecto, la recomendación es leerla con cuidado. Hay muchos artículos que tienen muchas imprecisiones, así como también, muchos artículos que dan atributos poco razonables a la tecnología BlockChain, como, por ejemplo, que permitiría acabar con el hambre en el mundo o superar la pobreza.

De otra parte, BlockChain plantea importantes desafíos que no se deben pasar por alto a la hora de optar por su implementación: El gasto energético que supone el proceso de minado de un bloque ha llevado a que en un estudio hecho por científicos de la Universidad de Hawái, en Manoa y publicado en la revista Nature Climate Change, se indique que la minería de criptomonedas podría producir suficientes emisiones para elevar las temperaturas globales en 2°C para 2033.

Considero importante reflexionar, además, en torno a la filosofía que está detrás de esta tecnología: Desintermediar y eliminar a las autoridades centrales por los costos que implican y, especialmente, la desconfianza en ellas. Sin embargo, en entornos en que las instituciones funcionan, e incluso cuentan con tal nivel de digitalización que permite disminuir los costos, ¿es necesaria la implementación de BlockChain?

Por último, quisiera advertir que BlockChain, en la fase exploratoria de su desarrollo, se encuentra, como la mayoría de los casos en que se enfrenta una nueva tecnología, altamente desregulada, significando importantes desafíos para reguladores. De hecho, es un elemento prioritario en la agenda digital de varios gobiernos, los cuales están desplegando sus esfuerzos en comenzar a desarrollar estrategias para regular esta tecnología.

Chile no se ha quedado atrás, y en tal sentido es una buena señal el esfuerzo iniciado por la administración anterior para evaluar las posibles aplicaciones de uso en que BlockChain tendría lugar o no. Habrá que prestar atención, por lo tanto, a cómo, con todos los elementos en la mesa, procederán las autoridades y reguladores. Con todo, habrá que ser cauto, toda vez que, una mirada superficial a los atributos de esta tecnología podría llevar al equívoco de pensar que su uso aplica a todo.