

No. 145 Octubre - Diciembre 2017

ISSN 0120-5919

SISTEMAS

Tarifa Postal Reducida Servicios Postales Nacionales S.A. No. 2015-186 4-72, vence 31 de Dic. 2017



Blockchain: Reflexiones y retos emergentes



ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

XVI Jornada de Gerencia de Proyectos de TI

Más allá de la Transformación Digital

Del 14 al 16 de marzo de 2018
Club de la FAC - Calle 64 # 3B- 21, Bogotá

Cada año trae nuevos desafíos impuestos por el ritmo acelerado de la innovación y el avance disruptivo de la tecnología. Estos desafíos están presentes tanto en las organizaciones, que se enfrentan a una inevitable renovación de sus estrategias, como para los usuarios y beneficiarios de dichas estrategias que deben descubrir nuevas formas de hacer las cosas.

Al igual que lo hace un director de orquesta al garantizar que todos los músicos tocan la melodía correcta en el momento oportuno, así mismo los directores de proyecto buscan garantizar la gestión correcta de sus proyectos. Para lograrlo, los directores de proyecto utilizan una gran variedad de instrumentos y herramientas, que bien utilizadas pueden generar una melodía agradable al oído.

Este año la XVI Jornada de Gerencia de Proyectos de TI tratará diversos aspectos de la gerencia de proyectos y la transformación digital. Transformación que nos entrega esa variedad de instrumentos que requieren de una gestión adecuada, desde múltiples perspectivas – técnica, estratégica y de liderazgo - para lograr una gestión integral de proyecto.

Los esperamos en este espacio de encuentro y crecimiento profesional, para compartir experiencias, discutir sobre los nuevos retos y las diversas formas de hacer que las cosas sucedan.

Coordinadores Académicos:

Hilda C. Chaparro L, MSc, PMP & Alberto Domínguez, MSc, PMP, PMI ACP



Calle 93 No. 13 - 32 - Oficina 102
Teléfonos: 6161407/09 - 3015530540
 cursos@acis.org.co - acis@acis.org.co
www.acis.org.co

En esta edición

Editorial

Blockchain, tecnología disruptiva y oportunidad de negocio

Surge un nuevo paradigma que habilita la desintermediación, la descentralización y la desinstalación.

4

Columnista Invitado

En la Blockchain confiamos

La tecnología Blockchain es un mecanismo para depositar la confianza en algo que nadie controla, pero que es verificable y conocido por cualquiera, eliminando el doble gasto.

8

Investigación

Blockchain en Colombia: perspectivas y algunas tendencias

Este documento contempla un breve análisis de la encuesta realizada por la Asociación Colombiana de Ingenieros de Sistemas –ACIS–, sobre *blockchain*.

14

Cara y Sello

Tensiones de los criptoactivos

¿Control y poder ejercidos por todos? ¿Si la información es de todos, el poder quién lo ejerce? ¿La tecnología que los soporta va más allá? ¿Por qué son satanizados y de pasada la tecnología blockchain que los soporta? Varios consultores, ingenieros de sistemas y un abogado profundizan en este entorno invadido por interrogantes.

22

Uno

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

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.

45

Dos

Blockchain, una mirada a la descentralización de las transacciones y de la información

Las nuevas tecnologías de la información pueden generar valor a las empresas e industrias en una forma disruptiva y, dependiendo de su envergadura y proyección de crecimiento, también cambiar el mundo y la forma de conectarlo. *Blockchain* es una de ellas e incide en el modelo actual de negocios, en industrias como la financiera y de bienes raíces, generando una mejora en los servicios para brindar mayor valor a los clientes.

52

Tres

Regulación de blockchain como fenómeno disruptivo

Sin ir más allá de lo poco dicho sobre la necesidad de regulación de las nuevas tendencias tecnológicas, el presente escrito busca dar una perspectiva general de la incidencia de *blockchain* en los nuevos modelos económicos que se sirven de los datos y la información como activos vitales, primordiales e incluso exclusivos en su desarrollo.

60

Publicación de la Asociación Colombiana de
Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del
Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales
Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Dirección General

Jeimy J. Cano Martínez

Consejo de Redacción

Francisco Rueda F.
Gabriela Sánchez A.
Manuel Dávila S.
Andrés Ricardo Almanza J.
Emir Hernando Pernet C.
Fabio Augusto González O.
Jorge Eliécer Camargo M.

Editor Técnico

Jeimy J. Cano Martínez

Editora

Sara Gallardo Mendoza

Junta Directiva ACIS

2016-2017

Presidente

Edgar José Ruiz Dorantes

Vicepresidente

Luis Javier Parra Bernal

Secretario

Juan Manuel Cortés Franco

Tesorero

José Libardo Borja Suárez

Vocales

Sandra Lascarro Mercado
Ricardo Munevar Molano
Jorge Enrique Molina Zambrano

Directora Ejecutiva

Beatriz E. Caicedo Rioja

Diseño y diagramación

Bruce Garavito

Impresión

Javegraf

Los artículos que aparecen en esta edición no
reflejan necesariamente el pensamiento de la
Asociación. Se publican bajo la responsabilidad
de los autores.

Octubre - Diciembre 2017

Calle 93 No. 13-32 Of. 102
Teléfonos 616 1407 – 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

NASCO

NACIONAL DE COMPUTADORES S.A.

APOYA ESTA PUBLICACIÓN

TEL: 6 06 06 06- CR 15 No 72-73



Confía en 4-72,
el servicio de envíos
de Colombia

Línea de atención al cliente:
(57 - 1) 472 2000 en Bogotá
01 8000 111 210 a nivel Nacional

.....
www.4-72.com.co

¡Escríbanos!

Revista Sistemas

**Asociación Colombiana de
Ingenieros de Sistemas (ACIS)**

Diríjase a la editora de la revista:

Sara Gallardo M.

saragallardo@acis.org.co



Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

Blockchain, tecnología disruptiva y oportunidad de negocio



Jeimy J. Cano M.

Surge un nuevo paradigma que habilita la desintermediación, la descentralización y la desinstalación.

Estamos avanzando hacia un escenario cada vez más digital, más ágil y más exigente en el que la convergencia tecnológica se convierte en una constante para crear posibilidades antes inexploradas, de la mano de las nuevas demandas de los clientes. Este escenario establece una serie de tensiones entre las personas, los procesos, la tecnología y las regulaciones, encaminada a un cambio de para-

digma en la manera de ver el mundo y a motivar una nueva postura ante las propuestas discontinuas de hoy y las que se presentarán en el futuro sobre la forma en que hacemos las cosas.

Considerando lo anterior, la tendencia de empoderar cada vez más al cliente se afianza desde diferentes aspectos y propuestas, habida cuenta que es él, quien tiene el interés, la necesidad y la

demanda de productos y/o servicios diseñados a la medida, que cumplan con sus expectativas dentro de un marco de trabajo que lo mantenga siempre “motivado” alrededor de una propuesta de valor personalizada.

Así las cosas, se plantea una dinámica económica mucho más descentralizada, con menos intermediarios y variada oferta, que configura un patrón de comportamiento cambiante en los diferentes participantes de una sociedad digitalmente modificada. En este sentido, los avances tecnológicos como *blockchain* encuentran un espacio privilegiado para conectar a los individuos como pares, y permitirles la posibilidad de negociar directamente el bien que representa el valor para los interesados.

De manera silenciosa, este paradigma que quiebra los “pasos intermedios” de los clientes con sus necesidades ha venido construyendo la confianza necesaria para establecer un nuevo concepto de transacción segura, en una red (sin control central) en la que existen “activos digitales” (generalmente de interés por muchos clientes) como pueden ser dinero, acciones, propiedad intelectual, música, registros de estudiantes, entre otros, los cuales se pueden adquirir y negociar en una forma confiable, dejando un registro de la transacción que de manera simultánea se anuncia a todos los participantes.

Por tales razones, la presente edición de la revista *Sistemas* busca conocer mejor esta nueva tecnología y establecer un marco general de referencia, con la participación de profesionales, académicos e inquietos tecnológicos, quienes aportan valiosas reflexiones

acerca de la nueva propuesta disruptiva, como lo es la “cadena de bloques”.

Desde la economía de “favores y obligaciones” en “comunidades autosuficientes, pequeñas e íntimas, en las que sus integrantes se conocían y el intercambio no generaba conflictos” —como señala nuestro columnista invitado, el abogado Daniel Villarroel Barrera—, la sociedad ha atravesado por múltiples caminos en su socialización, convivencia y la forma de hacer negocios.

Después de una larga trayectoria con infinidad de alternativas, mecanismos y figuras, hoy nos encontramos en medio de la tecnología *blockchain*, identificada por muchas personas con las criptomonedas, específicamente el *bitcoin*. Tecnología que trasciende el uso con una serie de aplicaciones de soporte para las organizaciones y sus diferentes procesos.

En la entrevista a Edwin Zácipa, director ejecutivo de Fintech Colombia, obtuvimos información sobre las acciones más relevantes, los obstáculos superados y el futuro de esta joven entidad que busca convertir a Colombia en el tercer país más fuerte de la región en fintech, lo que supone el desarrollo de nuevas competencias técnicas, capacidades en innovación y marcos regulatorios que habiliten tales opciones.

El tradicional foro convocado para cada número fue denominado “Tensiones de los cryptoactivos” y reunió a seis expertos entre consultores, ingenieros de sistemas y un abogado para profundizar en ese entorno invadido de interrogantes, entre ellos: ¿El *blockchain*

es una opción para crear una nueva forma de interacción entre las personas, los productos/servicios y las empresas? ¿Las criptomonedas representan realmente una disrupción tecnológica o una disrupción social? ¿Qué haría falta para que *blockchain* sea una tecnología de uso masivo? ¿Son las criptomonedas una nueva forma de activos que debemos regular y desarrollar? ¿*Blockchain* es realmente una opción para lograr nuevas disrupciones digitales? Si es así, ¿qué debería pasar? ¿Están preparadas las organizaciones para potenciar el uso del *blockchain*? ¿Qué conocimiento deben tener los ingenieros para apropiarse y desarrollar nuevas opciones con *blockchain*?

Las conclusiones del foro más que plantear respuestas, establecen un escenario de alternativas para concretar—como se sugirió en el debate— más pruebas de concepto que hagan tangibles los beneficios y las posibilidades de esta tecnología dentro de las empresas.

Para la investigación se realizó una encuesta que reunió más de 83 profesionales que constituyeron la muestra base para conocer la percepción de las personas del gremio sobre la tecnología *blockchain*. Los resultados más significativos muestran que esta tecnología se ve como una disrupción

tecnológica y como una oportunidad de negocio. Sin embargo, como no se tiene mucha información sobre la misma y su estado de madurez es bajo, aún no logra cautivar a los ejecutivos de las organizaciones.

Sobre temas específicos varios colaboradores nos enviaron sus artículos, a través de los cuales se analizan algunas de las posturas alrededor de la tecnología *blockchain* y su alcance. Rafael Bettin Díaz se refiere a la descentralización de las transacciones y de la información. Los abogados Iván Darío Marrugo y Andrés Felipe Contreras se ocupan de la regulación de *blockchain* como fenómeno disruptivo. Y, el suscrito, formula algunas reflexiones sobre la seguridad y el control en la cadena de bloques.

Como se puede advertir, esta nueva tecnología *blockchain* aún está en sus primeras etapas de apropiación y madurez, lo que implica que habrá nuevos avances y retos que, tanto los profesionales de las tecnologías de información como las empresas, deben asumir y superar para concretar una nueva revolución digital en la que la desintermediación y la descentralización configuran una renovada apuesta orientada al cliente, ofreciéndole mayor información y la posibilidad de decidir con quién cierra un negocio. 🌐

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 por la Universidad Externado de Colombia. Ph.D in Business Administration por Newport University, CA. USA. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners. Es director de la Revista *Sistemas de la Asociación Colombiana de Ingenieros de Sistemas—ACIS—*.



ACIS

ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

La Asociación Colombiana de Ingenieros de Sistemas (ACIS), presente en las redes sociales para servir al sector informático del país y del exterior.

 /acis

 @acis_co

 /aciscolombia

 /aciscol

 /ACIScolombia

 www.acis.org.co

Calle 93 No. 13 - 32 - Oficina 102
Teléfonos: 6161407/09 - 3015530540
acis@acis.org.co

En la Blockchain confiamos



La tecnología Blockchain es un mecanismo para depositar la confianza en algo que nadie controla, pero que es verificable y conocido por cualquiera, eliminando el doble gasto.

Daniel Villarroel Barrera

En las sociedades antiguas, las personas no conocían ni manejaban el concepto de dinero, compartían sus bienes y servicios a través de una economía de favores y obligaciones; eran comunidades autosuficientes, pequeñas e íntimas, en las que sus integrantes se conocían y el intercambio no generaba conflictos. Pero como sabemos, esta economía no duró para

siempre. Las comunidades fueron creciendo y ya no era tan sensato el uso de la economía de favores y obligaciones, y tampoco teníamos la certeza de la equivalencia de los bienes intercambiados, situación que se tornó exponencial con el aumento de la densidad poblacional. Lo anterior, aunado al fenómeno de la especialización generó el problema de ¿cómo gestionar el

intercambio de bienes y servicios bajo este contexto?¹

En una economía con numerosos actores, productos y servicios, el intercambio de favores y obligaciones, se convierte en un verdadero nudo gordiano al tratar de definir el equivalente de cada producto y servicio, más, cuando ya no los vamos a consumir de manera inmediata. Tomando el ejemplo de Glyn, si hay 100 artículos diferentes que se truecan en el mercado, los compradores y los vendedores tendrán que conocer 4.950 tasas de canje; y si los artículos que se truecan son 1.000, los compradores y los vendedores tendrán que vérselas con 499.500 tasas de canje distintas.² A esta problemática debe sumarse que, no todos los días las personas van a querer carne o leche, de ahí que no se puedan intercambiar algunos productos o servicios entre sí, y se dificulte interactuar en el mercado, hecho sumado a la distancia geográfica entre los actores.

Algunas comunidades intentaron crear un sistema de trueque centralizado (ya vamos viendo por dónde va el asunto), pero la verdadera solución tuvo lugar con la creación del dinero, que surge como una creación mental, como una nueva realidad de las propias comunidades, como un medio universal de intercambio, que permite convertir casi cualquier bien o servicio en ese medio. Carl Menger, demostró que el dinero proviene del mismo mercado, no del Estado. El dinero emerge gradualmente en la búsqueda de una forma ideal de *commodity* para el intercambio indirecto. En lugar de intercambiar entre sí, las personas adquieren un bien no para consumir, sino para comerciar. Ese bien se convierte en dinero, el *commodity* más comerciali-

zable. En distintos lugares y distintos momentos se crearon diversos tipos de dinero como cualquier forma ideal de intercambio: conchas, ganado, pieles, sal, grano, tela, cauris, cebada, el ciclo de plata, oro, cigarrillos, alcohol –muchos siguen existiendo de manera inconsciente–, y la más conocida, la moneda, pieza estandarizada de metal acuñado.

El uso de metales preciosos, pero principalmente razones políticas, motivaron el surgimiento de las monedas, a la acuñación. Las primeras de la historia, las hizo acuñar hacia el año 640 a.C. el rey Aliates de Lidia, en Anatolia. La acuñación dio lugar a que la autoridad (la representación del Estado de ese momento) certificara cuánto metal precioso contenía la moneda, garantizando así su emisión y contenido, generando confianza en los actores. La acuñación era una respuesta al fraude entre pares, con la que un tercero garantizaba que el metal precioso que se entregaba fuera genuino³ y auténtico, y además, que aquél que falsificara el dinero fuese perseguido y sancionado.

Adicionalmente, es necesario entender dos realidades del constructo psicológico – nuestra invención mental– del dinero, que son ciertas desde hace tiempo, pero siguen distorsionadas en el imaginario colectivo y en nuestra realidad:

- (i) El metálico (monedas y billetes) es solo parte del dinero, la más familiar, pero no la principal ni su única

¹ David Graeber, *Debt: The First 5.000 Years*, Brooklyn, N. Y. MelvilleHouse, 2011.

² Glyn Davies, *A History of Money: from Ancient Times to the Present Day*, Cardiff. University of Wales Press, 1994.

³ Por ejemplo no hubiera plomo en el lingote de plata.

forma. Para el caso colombiano, el dinero en circulación en la economía corresponde a la denominada base monetaria. De conformidad con la información del Banco de la República,⁴ la base monetaria –M3– de Colombia, para agosto de 2017, es de 452.644 miles de millones,⁵ de los cuáles existen en circulación, alrededor de 64.176,3 miles de millones en monedas y billetes, por lo que realmente, la principal parte del dinero de nuestras economías son exclusivamente bits; y

- (ii) El dinero hoy no está respaldado por oro o algún otro bien, solo conlleva confianza (dinero fiduciario o fiat); en últimas, el dinero es cualquier cosa que la gente esté dispuesta a utilizar para representar de manera sistemática el valor de otras cosas, con el propósito de intercambiar bienes y servicios; y funciona, porque estamos dispuestos como colectividad a aceptar ese medio, y confiamos en que cuando lo usamos, nos lo van a recibir por bienes o servicios, trabajando como el sistema de confianza mutua más fuerte.

Después de muchos siglos, resurgió la idea de volver a los orígenes de nuestra realidad intersubjetiva, entendiendo que no era necesario un tercero administrando de forma centralizada, que nos ofrecía/vendía confianza, en el cual tampoco confiábamos tanto y había cometido tantos descalabros; y esta idea se plasmó en un *paper* por Satoshi Nakamoto, publicado el 31 de octubre de 2008.⁶ Para esa fecha seguía existiendo la desconfianza en el intercambio indirecto y las relaciones, con la diferencia que ahora existe una herramienta que no tenían los sume-

rios, la tecnología; en este caso, el *Protocolo de Bitcoin*.

Bitcoin es una red conformada por hojas de cálculo digitales,⁷ descentralizadas, alojadas y distribuidas en computadores repartidos por el mundo, que permite la transferencia de bits de información seguros y no repetibles, de una persona a otra, sin importar su ubicación. Estos bits de información están garantizados por una forma digital de título de propiedad –denominada firmas digitales por Satoshi–, para verificar los derechos de propiedad sin tener que depender de terceros. Esta red se llama *blockchain* (cadena de bloques) y es supervisada por cada uno de los usuarios de la red. Cualquier persona puede participar en la red *Bitcoin*, enviando o recibiendo *bitcoins*, o incluso manteniendo una copia de la hoja de cálculo para observar su funcionamiento. La red es completamente libre, pública y abierta.

Pero ahora ¿por qué tiene valor el *bitcoin* si no deja de ser una base de datos distribuida en miles de computadores en el mundo, y en últimas, una serie de unos y ceros? La respuesta está en que el *bitcoin*, más allá de los atributos propios del dinero, es en sí mismo un sistema de pago. Usualmente, pensamos en el peso colombiano y el sistema de pago⁸ de manera independiente. Todos estamos acostumbrados a pensar en divisas separadas de los sistemas de pago, toda vez que de

⁴ <http://www.banrep.gov.co/es/agregados-monetarios-crediticios>

⁵ Sin siquiera considerar la economía paralela derivada de actividades ilegales.

⁶ <https://bitcoin.org/bitcoin.pdf>

⁷ Hoja de cálculo corresponde a la traducción que le damos a ledger.

⁸ Por ejemplo PSE, tarjetas de crédito, pasarela, PayPal, etc.

nada sirve contar con una moneda, si no puedo entregarla a alguien con quien no comparto proximidad geográfica para el correspondiente intercambio de bienes y servicios, para lo cual requiero un sistema de pago. Además, los sistemas de pago tradicionales presentan dos grandes problemas: (i) pocas personas tienen acceso a ellos, y (ii) generan un doble gasto, al requerir de un intermediario.

El protocolo tiene como objetivo eliminar estos problemas, a través de la unión en la estructura del código, de la función de dinero con un sistema de pago. Esta conexión es lo que hace a *Bitcoin* diferente de cualquier manifestación de dinero en la historia, pues agrega la red de pago. La tecnología permite hacer transacciones digitales, de forma escalable y global, a través de criptografía para verificar las transacciones y salvaguardar la integridad de los activos subyacentes, sin la necesidad de la intervención de un tercero.⁹

Bitcoin no fue siempre un dinero con valor. Dos meses después de la publicación del *paper*, surgió el “Bloque Génesis”, los primeros *bitcoins*¹⁰ generados a través del concepto de Satoshi y guardados en una base de datos, alojada en algunos computadores repartidos por el mundo. El 5 de octubre de 2009, 1.309,03 *bitcoins* fueron transados por USD1. Con el tiempo, los *earlyadopters* corroboraron que efectivamente se podía transferir una unidad sin gastar dos veces, que se trataba de un sistema que dependía de la potencia de los computadores, que esto bastaba para verificar las transacciones y que era posible mover bits representados en títulos a cualquier parte del mundo de forma completa-

mente segura, peer-to-peer, sin la intervención de un tercero, poniendo a disposición de cualquier persona conectada a Internet el libro contable, con un registro que guarda las cantidades, los tiempos y las direcciones públicas de cada transacción. En últimas, se validó que cada unidad se convierte en una forma digital de propiedad, que el sistema de pago era útil, y la contabilidad adjunta era portátil, divisible, segura, fungible, duradera y escasa, llegando a un valor por *bitcoin* cercano a los USD10.000.¹¹

Bitcoin junta las mejores características del dinero de la historia, pero añade una red de pago que permite el comercio sin tener que depender de terceros. Aquí es donde se encuentra el valor de uso al que se refiere el teorema de regresión de Mises, para explicar cómo el dinero adquiere su precio en términos de los bienes y servicios que obtiene. Si fuera posible que *Blockchain* se separara de alguna manera de *bitcoin* (algo que no es posible), el valor del *bitcoin* caería instantáneamente a cero. Entendido lo anterior, debemos precisar que *bitcoin* no es lo mismo que *Blockchain*. *Bitcoin* fue el primer y es el más grande caso de uso de *Blockchain*, y toda la explicación de *Bitcoin* pretende dar las luces de esta tecnología, pero es muy difícil entender *Blockchain* sin *Bitcoin* y ver todas sus aplicabilidades sin entender lo anterior.

Blockchain no es sólo dinero. De forma sencilla, la tecnología *Blockchain* con-

⁹ Basta remitirnos al *paper* de solo nueve páginas de Satoshi para entender realmente este sistema de pago.

¹⁰ *bitcoin* en minúscula como el activo o unidad contable que se transa en Bitcoin-. *Bitcoin* en mayúscula como el protocolo u hoja de cálculo.

¹¹ Ahora, cuestión distinta es cuál es el verdadero precio del *bitcoin* pero eso da para otro artículo.

templa cualquier transferencia de información –cualquier activo– peer to peer, en una red descentralizada, en la que la verificación y la validación de cada interacción o transacción, antes de su ejecución, es proporcionada por todas las partes en la red,¹² a través de una hoja de cálculo digital compartida totalmente en un orden lineal y cronológico, que contiene todas las interacciones y transacciones, denominadas en conjunto bloques, mediante un complejo algoritmo (*hashes* encriptados), que usa detalles de todas las transacciones anteriores.

La tecnología *Blockchain* ofrece soluciones para los costos y desconfianza por la centralización e intermediación. Asimismo, la intervención de terceros en las transacciones genera problemas frente a la existencia de incentivos desalineados o perversos por estos terceros, que podemos llevar a un sinnúmero de áreas como el cumplimiento del pago de los servicios públicos, el control de los títulos de propiedad, los registros públicos o privados, entre otras.

Pero el asunto no para acá; entendiendo la posibilidad de contar con una herramienta descentralizada, cualquier acto o intervención nuestra podría adelantarse a través de esta tecnología, y se nos ocurrió que no tenía límite alguno y que nuestra confianza estaría depositada en algo que nadie controla, pero que es verificable y conocido por cualquiera, sin ser duplicado, alterado ni falseado, con una historia digital común. Esta tecnología también nos abrió la posibilidad a que las obligaciones de los contratos pudieran ejecutarse automáticamente, dejando el activo digital o su representación digital como el pago, en control de la pro-

pia red,¹³ sin que su cumplimiento dependiera de la voluntad de las partes, tratándose de una transacción algorítmicamente computarizada, de ahí el valor que tiene, por ejemplo, *Ethereum* al permitir la transferencia de cualquier bien y no solo dinero, dando lugar a los contratos inteligentes, que tanto se están explorando actualmente.

Dado que el código *bitcoins* abierto, innumerables desarrolladores han pretendido mejorarlo o expandirlo, modificando alguna de las reglas de su protocolo o a través de otro modelo o usando reglas distintas, para crear monedas o *tokens* distintos, denominados *altcoins* (*alternativecoins*). Hoy, existen más de mil criptomonedas que representan un mercado de más de 220 billones de USD,¹⁴ sin perjuicio de que muchas de las *altcoins* nos generan serias dudas sobre su verdadero valor y la seriedad de su protocolo.

Debido a que consideramos que casi todo activo (tangibles e intangibles) se puede representar de forma digital (no olvidemos que al final es un *token*), incluyendo acciones o participaciones en un proyecto, a través de las ICO (Initial Coin Offer), se ofrecen *coins* o *tokens* –existe una discusión legal y técnica sobre la diferencia de estos elementos– para que cualquier persona del mundo pueda adquirirlos como un mecanismo de participación y financiación en la correspondiente empresa o proyecto. Este mecanismo su-

¹² Las partes en la red se denominan nodos y no existe un límite de los mismos, al menos para las *blockchain* públicas.

¹³ Existen muchas definiciones de contrato inteligente que se apartan del uso de la tecnología *Blockchain* pero que no consideramos se tratan efectivamente de contratos inteligentes.

¹⁴ <https://coinmarketcap.com/>

para cualquier otro conocido, e incluso hace ver al *crowdfunding* como obsoleto. Las ICO han sido objeto de recientes pronunciamientos por varias autoridades en distintos países, y fraudes y *scams* de terceros no han dejado de aparecer ante estas creaciones.

Sin lugar a dudas, no todo es perfecto, la tecnología tiene problemas, la escalabilidad de la cadena de bloques, para citar solamente uno; y como el dinero

no lo puede todo, no podemos pretender que *Blockchain* lo solucionará todo. Pero, piensa en dónde se necesita contar con un récord de propiedad y/o dónde más, una tercera parte de su puesta confianza no es requerida. Imagínate ese futuro y empieza a comprender la plenitud de las oportunidades de la tecnología *Blockchain*, que tomará forma en términos no imaginados. 🌐

Daniel Villarroel Barrera. Socio fundador de SurBTC y business partner de varios proyectos de Blockchain y fintech. Abogado de la Universidad del Rosario, con un Máster en Derecho Empresarial de la Universidad Autónoma de Madrid (España). Cuenta con diversos estudios en Derecho Americano en el Southwestern Legal Foundation. Ha sido profesor titular de pregrado y posgrado en las áreas de derecho comercial y de empresa en la Facultad de Derecho de la Universidad del Rosario, fellow del Center for American and International Law y conferencista de temas de fintech, inversión y emprendimiento. Asimismo, ha sido profesor de la Universidad de Los Andes, en el área de blockchain e innovación en educación continuada. Es árbitro y secretario del Centro de Arbitraje de la Cámara de Comercio. En la actualidad es socio de la firma VTA legal, encargado del área de derecho financiero, de la industria de fintech y de nuevas tecnologías.

Blockchain en Colombia: perspectivas y algunas tendencias

Resumen

Este documento contempla un breve análisis de la encuesta realizada por la Asociación Colombiana de Ingenieros de Sistemas –ACIS–, sobre *blockchain*. La investigación se desarrolló a través de la plataforma *surveymonkey*, abierta a la Comunidad Virtual de esta entidad, durante el mes de noviembre de 2017. Los resultados muestran algunas tendencias preliminares sobre el tema, un bajo conocimiento de la tecnología de la cadena de bloques, su poca madurez y las pocas iniciativas al respecto, en diferentes sectores.

Palabras clave

Cadena de bloques, *blockchain*, encuesta, tendencias, ingenieros.

Jeimy J. Cano M.

Introducción

La tecnología *blockchain* genera tanto retos como expectativas en el contexto del gremio de ingenieros de sistemas. En este escenario fue puesta en marcha una encuesta básica para conocer el estado de conocimiento y desarrollo

de la tecnología, así como aquellos elementos que pueden motivar una mayor apropiación de dicho avance tecnológico.

El estudio compuesto por diez (10) preguntas buscaba explorar el terreno de la tecnología *blockchain* en el gre-

mio de los profesionales de las TIC, en diferentes sectores de la economía del país. Los interrogantes planteados fueron:

1. En qué sector de la industria trabaja usted:

- a. Banca
- b. Academia
- c. Farmacéuticos
- d. Salud
- e. Militar
- f. Seguros
- g. Telecomunicaciones
- h. Energía
- i. Otro, indique:

2. Para usted, *blockchain* en su industria es: (marque las que considere convenientes)

- a. Una amenaza
- b. Una disrupción tecnológica
- c. Una moda
- d. Una oportunidad de negocio
- e. Otra, detalle:

3. ¿Su empresa está considerando implementar *blockchain*?

- a. Si
- b. No
- c. No sabe

3.A Si la respuesta fue afirmativa, puede indicar ¿en qué tipo de proyecto?

4. De lo que usted conoce sobre *blockchain*, señale las oportunidades que ofrece esta nueva tecnología: (marque las que considere convenientes)

- a. Confianza
- b. Transparencia
- c. Agilidad
- d. Seguimiento

- e. Validación
- f. Otra, indique:

5. De acuerdo con su conocimiento, ¿cuáles son los tres (3) sectores que más se están movilizando para lanzar iniciativas usando *blockchain*? (Marque sólo 3):

- a. Banca
- b. Academia
- c. Farmacéuticos
- d. Salud
- e. Militar
- f. Seguros
- g. Telecomunicaciones
- h. Energía
- i. Otro, indique:

6. Las criptomonedas (por ejemplo el *bitcoin*) son una de las implementaciones más conocidas de la tecnología *blockchain*. En este momento usted, ha utilizado las criptomonedas para:

- a. No he hecho uso de las criptomonedas.
- b. Hacer pagos de bienes o servicios
- c. Hacer inversiones
- d. Hacer contratos
- e. Registrar escrituras
- f. Pagar extorsiones por secuestro de datos
- g. Otro, indique:

7. El sector financiero ha empezado a movilizar iniciativas utilizando la tecnología *blockchain*. En qué condiciones, usted estaría dispuesto a utilizar o suscribir nuevos servicios financieros con *blockchain*. Marque las que considere convenientes:

- a. Mayor seguridad en las transacciones
- b. Mejor soporte para el servicio
- c. Simplificación de trámites

- d. Personalización del servicio
- e. Mayor agilidad del servicio
- f. Otro, indique:

8. ¿Qué motivaría a su empresa para movilizar proyectos utilizando *blockchain*?

- a. Que hubiese iniciativas del gobierno o entidades del Estado.
- b. Que hubiese mayores casos de éxito en el país.
- c. Que hubiese apoyo, asesoría y capacitación especializada en el tema
- d. Que hubiese mayor sensibilidad y cultura sobre el tema.
- e. Otro, indique:

9. Con relación al nivel de conocimiento y formación sobre la tecnología *blockchain* que existe en las universidades del país, usted piensa que:

- a. Es escaso
- b. No se conoce la tecnología
- c. No hay profesores con el conocimiento
- d. No se ofrecen cursos especializados
- e. No hay implementaciones que mostrar
- f. Otro, indique:

10. Si definitivamente *blockchain* no es una opción para su organización, puede indicarnos ¿cuál(es) es(son) la razón(es)? (Marque las que considere convenientes)

- a. Poco conocimiento del tema
- b. Poco interés en la temática
- c. Se espera que madure la tecnología
- d. No se conocen los riesgos de la tecnología
- e. No hay interés por parte de los ejecutivos
- f. Otro, indique:

Resultados de la encuesta

Luego de cerrar la encuesta en *survey-monkey*, fueron contabilizadas 83 respuestas de los participantes. Si bien el número de profesionales que participaron puede resultar limitado, frente al universo de ingenieros registrados en la Asociación, los datos capturados y su tabulación ofrecen algunas tendencias interesantes para analizar.

Los resultados de la primera pregunta indican una mayor participación de sectores distintos a los tradicionales, la academia y las telecomunicaciones, como se observa en la figura 1.

Academia	31,33%
Farmacéuticos	1,20%
Salud	3,61%
Militar	0,00%
Seguros	2,41%
Telecomunicaciones	9,64%
Energía	2,41%
Otro, indique	43,37%

Figura 1. Demografía de la participación

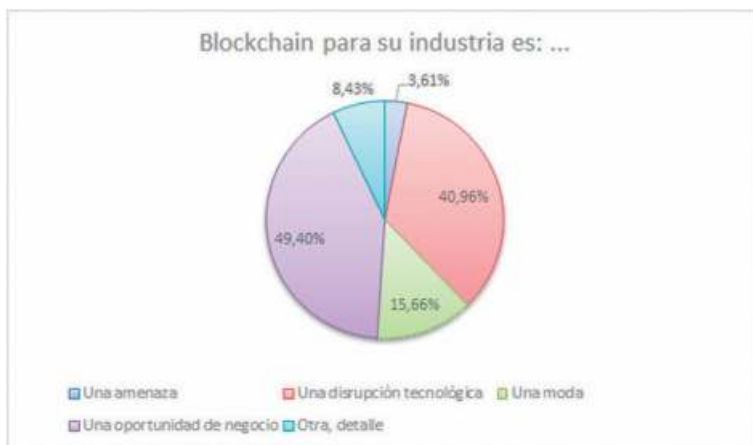


Figura 2. Percepción de *blockchain* en las industrias

La segunda pregunta revela como están viendo desde cada industria la tecnología *blockchain*. Los resultados marcan dos tendencias, en su orden: como una *oportunidad de negocio* y como una *disrupción tecnológica*, ver figura 2.

Es interesante observar que la tecnología de cadena de bloque puede abrir posibilidades de negocio en el entorno y es la motivación que los diferentes sectores tienen en su radar. De igual forma, que su utilización permite crear escenarios y propuestas para cambiar

la manera de hacer las cosas, lo que en últimas resulta en una transformación de la práctica vigente en un sector y la renovación del *status quo* de una industria o de una empresa.

La tercera pregunta indaga sobre la implementación de la tecnología de cadena de bloques. El 92,7% indica QUE NO o que NO SABE si se van a poner en marcha iniciativas en esta temática. Respuesta que confirma el bajo nivel de conocimiento y apropiación de la tecnología.

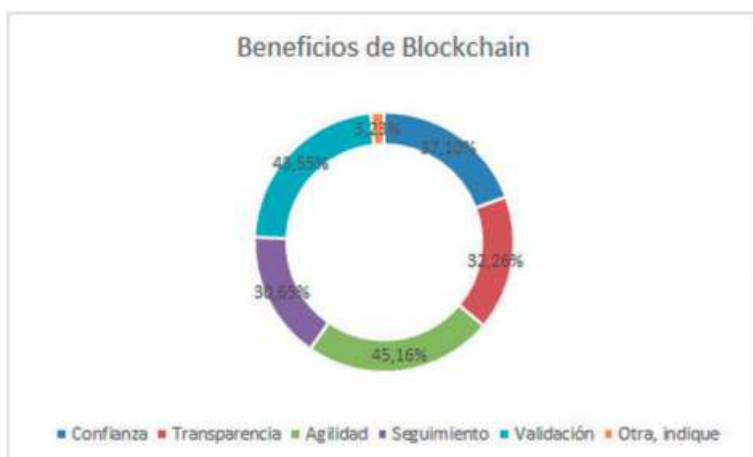


Figura 3. Beneficios de blockchain



Figura 4. Sectores que más avanzan en iniciativa con blockchain

La inquietud número cuatro se refiere a las oportunidades y beneficios que implica la implementación de la cadena de bloques. Las respuestas de los encuestados se concentran en tres elementos: *agilidad de las operaciones*, *validación de las acciones realizadas* y *la confianza que se genera* en la relación entre pares participantes, como se detalla en la figura 3.

La pregunta cinco revisa cuáles sectores son los que más se están movilizan para concretar iniciativas utilizando la cadena bloques. Las res-

puestas establecen que la banca, las telecomunicaciones y los seguros son las tres industrias que a la fecha cuentan con iniciativas de manera acelerada, con el fin de cambiar la forma de hacer las cosas y establecer una renovada relación con las expectativas de los clientes. La figura 4 muestra los resultados consolidados.

La sexta pregunta indaga sobre el uso de las criptomonedas. Esta nueva forma de transferir el valor ha venido ganando terreno en la sociedad, configurando todo un reto para las autorida-

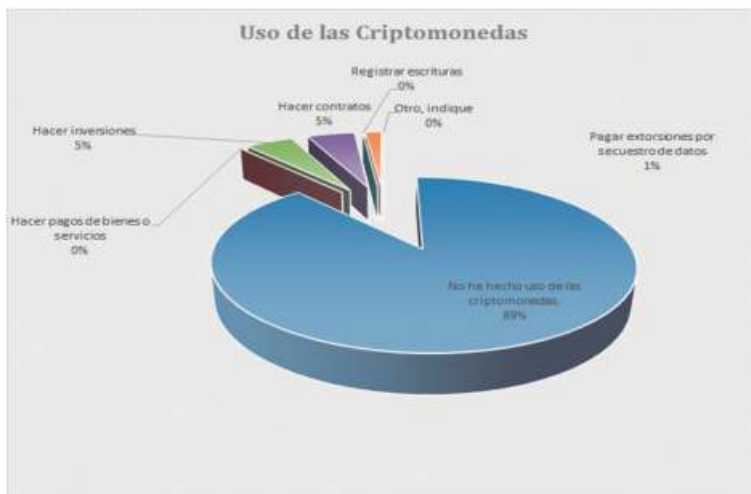


Figura 5. Uso de las criptomonedas

des monetarias y financieras de los países. Sobre este particular los encuestados afirman que *poco han hecho uso de ellas* y los que las han usado se concentran en *hacer inversiones y desarrollar contratos*. No deja de preocupar que algunos han realizado pagos por extorsiones con datos, lo que genera una lectura inadecuada de esta tendencia en el público en general, al asociarla con la delincuencia organizada. La figura 5 ilustra los resultados obtenidos sobre tales aspectos.

La pregunta siete se concentra en las iniciativas que viene desarrollando el sector financiero con *blockchain*. Particularmente este interrogante busca identificar en qué condiciones las personas estarían dispuestas a usar las nuevas propuestas de la banca, basadas en la cadena de bloques. Las respuestas apuntan a: mayor seguridad en las transacciones, simplificación de trámites y mayor agilidad en el servicio, como se observa en la figura 6.

El octavo cuestionamiento realizado en la encuesta identifica aquellos as-

pectos que llevarían a las empresas a desarrollar iniciativas con *blockchain*. Los resultados reflejan tres aspectos claves como son: *que el gobierno movilice esfuerzos en este sentido; que haya mayor apoyo, asesoría y capacitación especializados para el desarrollo de las propuestas y una mayor cultura y sensibilización sobre esta tecnología*.

Llama la atención que las organizaciones esperan que los gobiernos hagan sus apuestas por este tipo de tecnologías, como base para avanzar en proyectos encaminados a capitalizar nuevas oportunidades de negocio. Lo anterior, sugiere una prevención y discreción de la empresa frente a la novedad y los riesgos que supone una inversión en este tipo de iniciativas.

La pregunta nueve indaga sobre el nivel de conocimiento y formación requeridos para avanzar en el país con el uso de la tecnología de cadena de bloques, los resultados señalan el poco entendimiento de la tecnología y la falta de académicos y estudios realizados sobre el tema en el país.

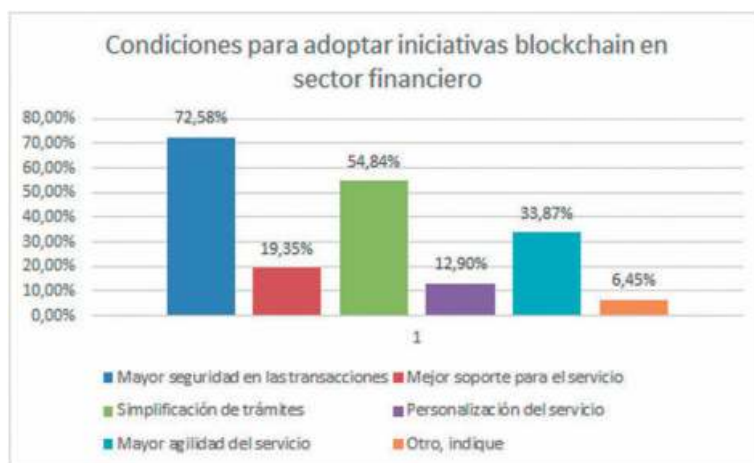


Figura 6. Condiciones de adopción de iniciativas *blockchain* en el sector financiero

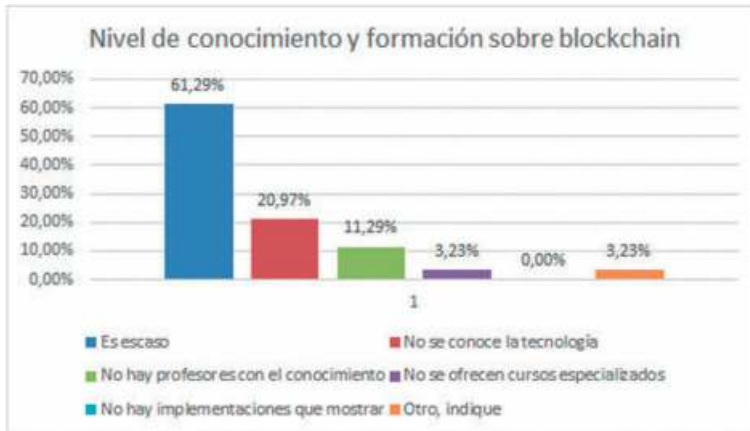


Figura 7. Nivel de conocimiento y formación en *blockchain*

La figura 7 resume las respuestas a esta inquietud.

Finalmente, la pregunta diez explora sobre aquellos para quienes la tecnología de cadena de bloques no es una opción y cuáles son los argumentos que sustentan su posición. Las respuestas, detalladas en la figura 8, establecen tres elementos claves: poco conocimiento del tema, se espera mayor madurez de la tecnología y bajo interés de los ejecutivos.

Aunque estas respuestas por el momento limitan las iniciativas sobre la cadena de bloques en algunas organizaciones, establecen tres condiciones básicas para que un proyecto de *blockchain* se desarrolle en una organización: el entrenamiento y la capacitación sobre implementaciones reales de la tecnología, con pruebas concretas de concepto; una mayor apropiación de la tecnología por parte de los especialistas tecnológicos y de negocio; y una mayor alfabetización digital para los ejecutivos en estos asuntos.

Factores determinantes para motivar nuevas transformaciones en las empresas.

Reflexiones finales

La encuesta realizada por la Asociación Colombiana de Ingenieros de Sistemas –ACIS– sobre la percepción de *blockchain* en el sector, establece una visión general de las preocupaciones, retos y tendencias en torno al uso de esta nueva tecnología.


Los resultados muestran una posición prudente de las empresas con relación a la puesta en marcha de iniciativas, además de una postura de observación activa de los avances, particularmente en el Estado, en procura de tener una claridad previa a los proyectos por desarrollar con base en la tecnología de cadena de bloques.

Es claro que habrá nuevas apuestas con el uso de la cadena de bloques que crearán cambios disruptivos en muchos sectores y cuando eso ocurra,

una nueva dinámica empresarial será la que impulse la transformación digital (WEF-Accenture, 2017) de las organizaciones, y el centro de aquella serán las expectativas de los clientes, quienes serán sorprendidos positivamente, con responsabilidad digital empresarial y unas nuevas plataformas tecnológicas encaminadas a personalizar

su experiencia con el producto y/o servicio.

Referencias

WEF-Accenture (2017) Digital Transformation Initiative. *Research Document*. Recuperado de: <http://reports.weforum.org/digital-transformation> 

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-.

Tensiones de los criptoactivos

¿Control y poder ejercidos por todos? ¿Si la información es de todos, el poder quién lo ejerce? ¿La tecnología que los soporta va más allá? ¿Por qué son satanizados y de pasada la tecnología blockchain que los soporta? Varios consultores, ingenieros de sistemas y un abogado profundizan en este entorno invadido por interrogantes.

Sara Gallardo M.

Aunque la tecnología *blockchain* no es nueva y goza de múltiples aplicaciones, de acuerdo con los expertos en el asunto, lo cierto es que despierta muchas preguntas a diestra y siniestra, especialmente cuando la discusión gira alrededor de los criptoactivos que mueven el piso del manejo del poder y el ejercicio de control.

Los cuestionamientos brotan en todas direcciones: entre técnicos y no técnicos, en los círculos ciudadanos tenta-

dos por la posibilidad de triplicar sus arcas, en los bufetes de abogados, en el sector financiero, en el mundo de los negocios y, por supuesto, entre quienes ocupan las poltronas de los poderes ejecutivo, legislativo y judicial.

Y la Asociación Colombiana de Ingenieros de Sistemas (Acis), en su calidad de gremio no podía mantenerse ajena a analizar el ambiente. De ahí que, a través de su revista *Sistemas*, proporcionara el espacio para una edi-

ción dedicada a reflexionar sobre la tecnología *blockchain*, sus implicaciones y su alcance.

A la mesa de debate acudieron Mauricio Pinzón González, director general de Tecnología del Banco de la República; Rafael Hernando Gamboa Bernate, abogado de Data & TIC Consultores; Fabio Alexander Rojas Roldán, director Information Risk Management en KPMG; Julio López Medina, consultor de tecnología en Infuturo Proyectos SAS; Juan Mario Posada Daza, gerente de Consultoría EY (antes Ernst & Young) y Luis Eduardo Daza Giraldo, socio-oficial de cumplimiento en SurBTC y exconsultor de la oficina UNODC de las Naciones Unidas.

“Esta edición está concentrada en el reto que tienen todas las organizaciones, en todos los ámbitos, sobre la tecnología *blockchain* o cadena de bloques, considerando que implica retos y significa un cambio de paradigma”, manifestó el director de la revista Jimmy J. Cano Martínez, como preámbulo

para formular la primera pregunta, en su calidad de moderador.

¿El blockchain es una opción para crear una nueva forma de interacción entre las personas, los productos/servicios y las empresas?

Juan Mario Posada D.

Gerente de Consultoría EY (antes Ernst & Young)

Definitivamente sí es una opción para crear una nueva forma de interacción, porque permea diferentes aristas de los negocios y en las vidas personales. Esta tecnología está siendo utilizada hoy en día de diferentes formas, en los contratos inteligentes, en la integración y monitoreo de todos los frentes. Desde esa perspectiva, sí es una nueva forma que va a demandar un alto esfuerzo en evangelización, en inversión en tecnologías, en gestión del riesgo, porque es necesario que todos los actores involucrados entiendan cuáles son las precauciones que deben tener en el momento de interactuar, que conozcan cuáles son los be-



neficios y qué tipo de esfuerzos demandan, desde el punto de vista tecnológico y de gestión de los riesgos.

Fabio A. Rojas R.

Director Information Risk

Management

KPMG

Blockchain ya está empezando a producir cambios muy importantes en la forma de interacción entre productos, personas, servicios y empresas, pero es necesario superar la idea de que esta tecnología está asociada únicamente al *bitcoin*; seguramente es la vía por la cual se ha hecho más famosa, pero sin duda no la única. El sector financiero la explora fuertemente para evitar intermediarios; asimismo, en el sector asegurador mediante contratos inteligentes, con el fin de ayudarse pa-

ra reducir el fraude; inclusive, en lo relacionado con los vehículos autónomos se exploran posibilidades de utilizar *blockchain* para autenticarse ante el vehículo. Definitivamente, sí plantea cambios dramáticos en la forma en que interactúan las empresas con sus clientes, en el desarrollo de productos y hasta en la misma dinámica interna de las organizaciones. Ethereum, por ejemplo, es una compañía que adopta *blockchain* para establecer su modelo de procesos administrativos sobre la base del consenso y colaboración, en el momento de decidir cómo hacer sus proyectos. Por todo lo anterior, esta tecnología representa un potencial importante para modificar la forma en que las organizaciones funcionan y cómo interactuaremos con ella sus productos y servicios.





Julio López M.

*Consultor en Tecnología
Infuturo Proyectos SAS*

Blockchain y *bitcoin* son dos temas completamente diferentes. Concentrándonos en la definición del primero, destaco que se trata de una evolución de las técnicas de administración de datos: pasamos de bases de datos centralizadas a bases de datos distribuidas y *blockchain* nos trae una novedad que contempla la distribución de copias de la base de datos, copias completas, de tal manera, que esto proporcionará una mayor robustez a los sistemas de información. Además, esta tecnología tiene otra característica y es que lleva la lista de todas las transacciones asociadas y a cada transacción se le asigna una llave basada en todas las anteriores. Esto le da una seguridad adicional al sistema

y es que, por ejemplo, si se saca una transacción de una base de datos financiera, con *blockchain* nos vamos a dar cuenta en forma inmediata de que hay una descompensación dentro de la cadena. Es así que contamos con dos ventajas como la replicación distribuida de la base de datos completa, sumada a la encriptación y la seguridad de que la cadena de transacciones está completa. Como todos los avances tecnológicos, conceptualmente son sencillos. La pregunta es cómo nos va a servir y cómo la vamos a utilizar. Hoy en día se dice que con *blockchain* evitaremos los intermediarios, en lo que se refiere a transacciones o “contratos”, de tal manera que tener la cadena de transacciones y los archivos propios encriptados permitirá asegurar la interacción con una persona “conocida en el sistema”, toda vez que el usuario

se identifica de manera virtual y puede mantenerse anónimo. Por ejemplo, en una transacción de finca raíz, potencialmente ya no es necesario involucrar a la oficina de Registros Públicos y será posible realizar la transacción entre dos personas con la seguridad que brinda el sistema por las razones técnicas mencionadas. Se dice que desaparecerán las entidades de control para verificar la transacción realizada a través de *blockchain*. No obstante, en una transacción de finca raíz son necesarias otras verificaciones y ante el riesgo de suplantación, a pesar de contar con billeteras electrónicas o archivos magnéticos o máquinas para interactuar con esta tecnología, la suplantación permanece como riesgo. Como siempre ha ocurrido con los avances tecnológicos, no estamos considerando *blockchain* en toda su

dimensión; no es el gran cambio ni tampoco producirá en dos años la eliminación de muchos controles, pero sí agilizará los tiempos de procesos hoy en día burocráticos.

Rafael H. Gamboa B.

Abogado

Data &Tic Consultores

Soluciones jurídicas y tecnológicas integrales

Blockchain es una forma de interacción social, vivimos en una sociedad y debemos tener claridad sobre las reglas con las que jugamos. En Derecho hay un principio que dice: “el derecho sigue a los hechos”, lo que quiere decir que las normas lo único que hacen es regular las situaciones que se presentan. Y esta tecnología *blockchain* es un nuevo entorno de interacción en el que se elimina un tercero de confianza,





que existía en las anteriores formas de interactuar dentro de la sociedad. *Blockchain* va a generar un ambiente de confianza más seguro, en la medida en que la tecnología misma la va a soportar, por supuesto, con debilidades y falencias, porque no es inmune a suplantaciones ni a hechos similares. Es importante entender la evolución de las transacciones en la humanidad. La primera arrancó por intercambio de elementos, una forma que cambió para dar lugar a los documentos y metales valiosos que representaban los bienes. Luego evolucionamos hacia la banca central, porque era necesaria la participación de un tercero de confianza. En las transacciones electrónicas este tercero, en muchos casos, es una entidad de certificación. *Blockchain* es mucho más que criptomonedas y sí va a generar una interacción y una satis-

facción más inmediata de las necesidades de las personas que actuamos en sociedad gracias a la tecnología. Las normas deberán adaptarse a estos nuevos desafíos para permitir el funcionamiento de la sociedad.

Mauricio Pinzón G.

*Director General de Tecnología
Banco de La República*

La tecnología *blockchain* sí es una nueva forma de interactuar. Y quiero referirme a lo planteado sobre las copias iguales o pedazos de copias para cada uno, que permiten un lugar común para que diferentes actores en Internet tengan la misma visión. El comprador, el vendedor y probablemente el banco de cada uno de ellos ven exactamente la misma base de datos. O incluso cada persona puede tener su copia y ser la dueña de sus

datos y propiedades digitales. Utilizo la analogía con la “red del pescador”. Internet es una red de comunicaciones con resiliencia, equivalente a la red de acueducto o de energía eléctrica. Cortar un hilo no daña la red. La debilidad en este momento son los sitios centralizados, los nudos en los que reposa la información centralizada que solo tiene una compañía, un organismo, pero que ahora gracias a las copias es mucho más difícil dañar la “red del pescador”.

Jeimy J. Cano M.

De acuerdo con las respuestas es claro que se trata de una nueva forma de interacción que reta la forma como nos relacionamos hoy por hoy. En ese orden de ideas ¿qué haría falta para que blockchain sea una tecnología de uso masivo?

Fabio A. Rojas R.

Lo que haría falta es entender la tecnología. Warren Edward Buffet decía “no inviertas nunca en algo que no entiendas”. Y el asunto con *blockchain* parece demasiado confuso, incluso para individuos muy preparados, y hace que el tema se trate fundamentalmente desde el punto de vista técnico y no desde todos los actores que pueden participar en esta tecnología. Si bien es cierto que hoy muchas personas mueven millones y millones de dólares sin comprender a profundidad cómo funcionan todos los intermediarios, parece que ya se ha llegado a un nivel de comodidad que les permite tratar con confianza en este medio. Con relación a *bitcoin*, por ejemplo, se percibe cada vez un mayor interés en invertir en este medio y las personas buscan enriquecerse de la misma forma que en 1994, cuando empezó Internet y muchos pretendieron volverse millonarios con

la web 1.0, en su momento. Pero existe una diferencia importante entre la época de *NetScape* y la de *blockchain*. Al principio, adentrarse en el mundo de Internet también parecía una tarea compleja, pero con el tiempo familiarizarse con la *web* resultó algo relativamente sencillo y con hacer “clic secundario - ver código fuente” era posible obtener el código HTML y con algún curso básico hasta podíamos construir una página *web* rápidamente. Con *blockchain* y *bitcoin* muchos creen que va a suceder lo mismo, pero la diferencia radica en que hacer clic secundario no será una alternativa para entender tan fácil cómo es que todo funciona. La tecnología *blockchain* se está vendiendo con una idea muy altruista de que se van a eliminar los intermediarios; no hay entidades centrales de control, pero pareciera que éstas se cambian por la dependencia de un equipo de expertos técnicos que manejan y entienden la tecnología. Y cuando un inversor tiene problemas con *bitcoin* y pierde dinero, le resulta muy frustrante no poder determinar por qué tuvo esas pérdidas y es posible que se vean poco inclinados a adentrarse en este asunto, máxime cuando esta tecnología se asocia más con formas de hacer fraude, que con maneras de prevenirlo y es más famosa por su utilización para comprar drogas, sexo y armas en la *darkweb*. Así que deberíamos empezar por entenderla.

Juan Mario Posada D.

Este ciclo ya lo hemos experimentado. Basta citar el momento en que nació el *e-commerce* y había una gran incertidumbre sobre si se iba a masificar y cuándo las personas del común empezarían a usar los beneficios de tales ambientes. Y hoy vemos a un Amazon,

la compañía más grande de *retail* en el mundo, por encima de muchas grandes superficies poderosas históricamente. Y esto sucedió porque las personas aprendieron, no sólo sobre los beneficios que les producía, sino que empezaron a sentirse más seguras en la medida en que el entorno empezó a regular esa nueva modalidad de hacer negocios. Y *blockchain* no dista mucho de eso; en la medida en que las personas empiecen a entender cómo funciona, sin duda se va a masificar, porque ofrece inmediatez, seguridad, privacidad y comodidad, además de los múltiples usos que tiene, como se ha visto aquí con varios ejemplos.

Julio López M.

Me parece oportuno separar las *cryptocurrencies* de la tecnología *blockchain*. Es como si la discusión fuera sobre la transmisión de videos por Internet hace 20 años y la estuviéramos confundiendo con la distribución de pornografía, que es una de sus muchas aplicaciones; el caso del *bitcoin* hay que mirarlo con detenimiento porque su uso se asocia con delitos, pero ese debate se dará más adelante. Sobre el interrogante en torno a *blockchain* pregunto: ¿por qué razón la están mirando las grandes firmas de tecnología, los bancos, las compañías de seguros? No lo están haciendo por las *cryptocurrencies*, éstas están muy lejos de las aplicaciones que la gente técnica está observando. Nosotros, como ingenieros de sistemas, tenemos una responsabilidad en llevar el verdadero concepto a la gente, para diferenciar la pornografía de *youtube*, a pesar de que ese espacio virtual permita también tener videos y pornografía que el usuario clasifica. La tecnología es una herramienta (no puede clasificarse de legal o de ilegal) y lo

que se haga con ella es responsabilidad de quien la utiliza. En cuanto a la masificación de *blockchain* hay una limitación tecnológica de *performance* muy grande. En el sector financiero la infraestructura debe responder en segundos a millones de transacciones por minuto. Tener millones de transacciones a nivel de *blockchain*, manejándolas con copias en varios nodos, sobrecarga cualquier sistema de procesamiento actual, por lo que creo que no estamos técnicamente preparados para su masificación. Noten que en el caso de las *cryptocurrencies*, generar la llave de encriptación de una cadena relativamente pequeña, es un trabajo disputado por unos nodos, que se hacen llamar “mineros” y nadie sabe quién se los gana; es un ejemplo sencillo para ilustrar que este procesamiento no es tan fácil. En un *blockchain* privado, con nodos privados, el manejo del volumen y las CPU que se requieren para ejecutar los algoritmos de encriptación y generar las llaves de encriptación, son un asunto muy complejo; considero que esto no es rápido ni eficiente en un entorno financiero, con la tecnología actual. En un ambiente de oficina de registros públicos, las transacciones son relativamente limitadas y el tiempo de respuesta no es tan exigente como lo puede ser en el sector financiero. Un ejemplo de masificación de la tecnología es la inteligencia artificial, que data de mucho antes de 1975 y no ha dado aún los resultados esperados; en el caso de la traducción asistida por computador, se cuenta principalmente con herramientas de ayuda a traductores.

Fabio A. Rojas R.

La inteligencia artificial puede llevar muchos años, pero lo que impide llegar a una masificación es precisamen-

te que no se entiende. Quizá para los ingenieros el tema es más accesible, pero para los dueños de las organizaciones y quienes toman las decisiones el tema es complejo y, en tal medida, no lo van a poner en práctica por desconocimiento. Hablarles de que ahora la confianza sobre las transacciones se basará en unos “mineros” no parece la forma más práctica de iniciar un proceso de masificación de *blockchain*.

Julio López M.

Me permito disentir porque para masificar el uso de una tecnología sus usuarios no tienen que conocerla a fondo. Estamos utilizando los teléfonos celulares y la transmisión de voz sobre IP es un tratado en “chino” para todos los usuarios. Hay una responsabilidad de los técnicos. Indudablemente, sí debe existir alguien que lo entienda para provecho de las organizaciones, así que el gremio es el que tiene tal responsabilidad de entenderlo y aplicarlo bien, no los usuarios ni la gente del común, quienes lo que necesitan es ver resultados. Es necesario aclarar el uso y ese es uno de los objetivos de este foro y lo que persigue Acis con la revista.

Rafael H. Gamboa B.

Existe un tema neurálgico, y es la realidad humana para generar cultura mediante el uso y la implementación de la tecnología. Claramente, el normal de los mortales no tiene ni idea sobre cómo funciona Internet o el mismo sistema financiero, y funcionan porque confiamos. La confianza es un asunto preponderante en algo o en alguien, llámese Estado, Banca Central o tecnología. Otro elemento que motiva el uso de una tecnología es el grado de satisfacción que genera. Y para la masifi-

cación es necesario generar cultura, aprender de las lecciones anteriores. El tema de la burbuja de finales del siglo 20, nos dejó enseñanzas bien importantes y quedó clara una premisa fundamental: cualquier desarrollo generado debe generar ingreso, debe ser un asunto económico que genere un valor agregado para la empresa y los usuarios. Debe ser atractiva y ahí es donde empieza el valor de los emprendedores, que entiendan y utilicen esta nueva tecnología para volverla atractiva y de esa forma generen demanda. De lo contrario, es muy difícil y la tecnología desaparecerá como en algún momento sucedió con *WiMax* que dejó de existir, porque no era funcional y sí demasiado costosa. Cultura y satisfacción son dos de los conceptos más influyentes.

Mauricio Pinzón G.

Para uno entender algo se dice que es necesario dictar clase al respecto. Una anécdota para ilustrar la idea: en un escenario de ingenieros, recién armado este tema, preguntaba si sabían que era un árbol de *Merkle* y me sorprendí porque menos del 5% de la audiencia lo identificaba y descubrí que yo tampoco lo había entendido bien. Otro ejemplo, en el momento que nosotros firmamos el acuerdo con la firma R3, que tiene una plataforma tecnológica denominada *Corda* y que entra dentro de la sombrilla de *blockchain*, desconocíamos que en esta arquitectura las copias de las bases de datos no se sincronizan usando la idea de la cadena de bloques y *proof-of-work*, sino usando el concepto de *notarías*. Incluso las copias en cada nodo no son idénticas por razones de privacidad y eficiencia. En resumen, hay diferentes propuestas acerca del alcance de la privacidad, los roles y las for-

mas de hacer consenso en el mundo de la descentralización de las bases de datos Distributed Ledger Technology (DLT) que estamos agrupando bajo el término *blockchain*. En mi opinión, es mandatorio para los ingenieros de sistemas entender el “paper Nakamoto” de *bitcoin* y la propuesta del “White paper” de Ethereum.

Jeimy J. Cano M.

¿Qué conocimiento deben tener los ingenieros para apropiarse y desarrollar nuevas opciones con blockchain? ¿Están preparados en las organizaciones para potenciar su uso?

Juan Mario Posada D.

Hace unos meses asistí a una Junta Directiva de una de las grandes empresas del país y me gustaría iniciar mi intervención formulándoles una pre-

gunta: ¿cuánto tiempo hace que hablamos de la nube? Entre 10 y 12 años. Y me sorprendió que uno de los miembros de dicha Junta, al referirnos a la seguridad en la nube interpeló: - ¿Qué tanto dista este concepto de nube de los dos *datacenters* que debo tener para que uno respalde al otro? Y la respuesta es que no es mucha la diferencia entre uno y otro. Y lo cito porque a pesar de tratarse de una tecnología que lleva ese tiempo y que se ha masificado, todavía hay muchas personas que tienen muchas inquietudes sobre cómo funciona. Y las organizaciones se han “montado en el bus” de la nube, sin conocer bien sus implicaciones. Luego si nos preguntamos si están preparadas las empresas para poner en marcha el uso de *blockchain*, probablemente la respuesta es no. Pero, no tienen que estar preparadas, seguramente van a encontrar desafíos,



riesgos, implicaciones en la adopción de *blockchain* como un modelo de negocio y de transacciones, pero no tienen que estarlo y no lo están, como tampoco estamos preparados, ni siquiera en esta mesa para afirmar en forma vehemente que entendemos completamente el concepto de *blockchain*. Lo cierto es que las compañías tendrán que afrontar lo que significa su uso, de una forma más proactiva. La realidad nos muestra que las organizaciones no actúan en estos temas de adopción de tecnologías y en los nuevos modelos en esa forma, sino que los asumen y de acuerdo con los obstáculos que van encontrando por el camino proponen distintas soluciones para seguir “montados en ese bus”.

Fabio A. Rojas R.

Las organizaciones no están preparadas para adoptar *blockchain*. En KPMG tenemos una alianza con Microsoft en torno a esta tecnología, en la que se han montado nodos en algunos países, orientados a explorar en conjunto con las empresas, ideas y casos de uso para *blockchain*. Y lo que observamos es que las compañías primero quieren resolver sus dudas sobre cómo funciona y de que trata esta tecnología. Y cuando empiezan a entender que tiene mucho más posibilidades que el *bitcoin*, les parece muy atractiva, pero surgen muchas incógnitas que no están resueltas y dificultan su adopción. Se preguntan si son necesarios nuevos socios de negocios para la adopción, cuál es el modelo de negocio en ese entorno y cuánto esfuerzo requiere el tratamiento de los riesgos asociados, por ejemplo, con la privacidad. *Blockchain* ¿podrá exceder las capacidades de la empresa? Tal vez, lo mismo que ha ocurrido con algunas organizaciones que adoptan

SAP, bien sea que subutilizan la herramienta por desconocimiento o simplemente porque la organización no tiene las capacidades para operar al nivel que ella lo exige. Estas incógnitas surgen al hablar de ese tipo de tecnologías. En resumen, quienes toman las decisiones en las organizaciones, por el desconocimiento e incertidumbre alrededor de *blockchain*, no están preparados para su adopción en este momento. Coincido en que al final si genera los beneficios y es suficientemente atractiva, de la misma manera como Internet o cualquier otra tecnología lo fueron, pues la adoptarán, pero no en este momento. Asumirán los riesgos o lo harán por moda, por la competencia, habrá casos de éxito que les ayudarán o gobiernos que la impulsen como lo ha hecho Canadá.

Julio López M.

El *blockchain* tiene un gran inhibidor en su aplicación y es la asociación con *bitcoin*. Mientras exista esa relación, mucha gente va a abstenerse de su adopción; es necesario sobrepasar tal inhibidor. Considero que *blockchain* es una tecnología base y nunca me pregunté si las organizaciones estaban preparadas o no para las bases de datos, cuando no existían muchos productos comerciales de hoy día, o si alguna vez estuvieron preparadas para los cubos u otros avances tecnológicos. Con una aplicación específica como el correo electrónico, nos preguntábamos si había preparación en las compañías para su puesta en marcha y nos costó mucho trabajo su introducción, algo que hoy vemos tan intuitivo. Así que la pregunta no me inquieta. Por otro lado, *blockchain* está en un desarrollo muy incipiente, y todavía no hemos visto todas las aristas ni las ventajas ni los usos que contempla,

hecho que va a limitar su aplicación en las organizaciones. Un concepto técnico y tecnologías en proceso de desarrollo, dificultan su apropiación y por ende su aplicación.

Rafael H. Gamboa B.

Frente a la pregunta, otra pregunta: ¿estaban preparadas las empresas para Internet y el correo electrónico, en los años 90? La respuesta es no, la adaptación e interiorización de Internet, fue el resultado de un proceso que generó cultura y satisfacción de los intereses de las empresas y los usuarios. Con relación a *blockchain*, la respuesta, en la misma línea es un no contundente, porque las empresas no saben a ciencia cierta para qué sirve. Las compañías se “arriesgarán” a *blockchain*, cuando valoren los eventuales riesgos, toda vez que si genera interés y satisfacción a la empresa y a los usuarios, además de una reducción de costos, sin duda la adoptarán en su actividad. Hoy por hoy los abogados, administradores y quienes participamos en una organización tenemos que ser trilingües, para entender: (i) el negocio y producir ganancia, (ii) la tecnología y (iii) una parte transversal que soporta los dos anteriores (tecnología y negocio) y son los aspectos legales.

Mauricio Pinzón G.

Tengo 57 años y varias tías que me llevan algunos más. Nunca les pregunté a ellas si estaban preparadas para usar WhatsApp y crearon un grupo y “charlan” entre ellas sin preguntarse cómo funciona. Este asunto está relacionado con la pregunta: *¿Están preparados en las organizaciones para potenciar su uso?* Uno no pregunta sobre la preparación. Uno muestra el caso de uso y muestra el beneficio de la

tecnología para la organización. Hace poco tuve la oportunidad de ver tres bancos brasileños compartiendo la base de datos de los clientes, todos con la misma copia, pero son los clientes quienes deciden qué banco puede leer sus datos personales. Es un ejercicio bonito porque unifica las diferentes bases de datos personales y empodera al cliente sobre la propiedad de éstos. Este es un caso de uso interesante para referirse al *blockchain*, en la medida que se trata de organizaciones que en lugar de competir, construyen colectivamente esta base de datos unificada para ganancia de todas las partes. En resumen, lo que hay que mostrar a la organización es el beneficio de *blockchain*, tal como mis tías vieron las bondades del grupo en WhatsApp.

Jeimy J. Cano M.

La pregunta anterior nos reveló diferentes opciones sobre la tecnología blockchain. Las organizaciones van a asumir los riesgos. El elemento clave de dicha pregunta se cifra en mostrar el caso de uso, ejemplo para que las organizaciones comiencen a “tocar” con elementos concretos cómo funciona para materializarla en un caso concreto. Después de contextualizar el tema del blockchain, vamos a las criptomonedas como la aplicación más visible en la tecnología que hoy nos ocupa. ¿Las criptomonedas representan realmente una disrupción tecnológica o una disrupción social? ¿Son las criptomonedas una nueva forma de activos que debemos regular y desarrollar?

Fabio Rojas R.

Primero que todo estoy de acuerdo en que las criptomonedas, especialmente *bitcoin*, son inhibidores y a la vez im-

pulsos, por algún lado hay que empezar. No es posible comenzar a hablar de *blockchain* y al mismo tiempo sobre 250 aplicaciones, porque eso generaría mayor confusión. Es necesario comenzar por alguna aplicación y el *bitcoin* ha despertado el interés y así como tiene su lado preocupante, también tiene el lado que motiva a los Gobiernos, a las organizaciones y a escenarios como este para empezar a hablar del asunto. No me parece negativo que se aborde desde la óptica del *bitcoin*. Considero que es un disruptor desde el punto de vista social y tecnológico. *Bitcoin*, sustentado en *blockchain*, puede contribuir de manera importante a mejorar la confianza perdida desde los problemas financieros de 2008; *blockchain* pone actores como las matemáticas, la criptografía, la informática, de la mano de otros como la confianza y transparencia, haciendo que éstos últimos, se conviertan en un actor (no de reparto) no sólo deseable, sino indispensable (protagónico).

La tecnología *blockchain* y el *bitcoin* requieren de la confianza para lograr la participación efectiva de los involucrados; desde ese punto de vista es realmente disruptiva, porque hace que el comportamiento transparente de la sociedad empiece a ser un condicionante para participar del modelo y no simplemente algo que está descrito o implícito, pero que con facilidad es posible que se pierda o se sobrepase. Desde el punto de vista de las tecnologías que están por detrás de *bitcoin* no necesariamente me parece que son disruptivas, hablar de *PKI*, *hash* y computación distribuida no es precisamente una novedad hoy en día, pero la forma en que están organizadas para operar sobre la base del consenso, sí me parece una idea totalmente disruptiva.

Juan Mario Posada D.

Las criptomonedas representan una disrupción social y tecnológica y lo afirmo de manera contundente. Lamentablemente y como hemos venido mencionando, las criptomonedas tienen que empezar a luchar contra su mala reputación. Entre mayo y julio de este año tuvimos los casos de publicidad negativa más grande de las criptomonedas con los casos de *Wanna Cry* y *Pethya*, los cuales afectaron todos los sectores de la industria y todos los países, y lo que uno siempre encontraba en los titulares de las noticias era que la extorsión para recuperar los datos oscilaba entre 100 y 300 dólares representados en *bitcoins*. La lectura de una persona del común es que el *bitcoin* es usado por los delincuentes. Y esto genera una disrupción social en el sentido de que para muchos será necesario entender bien qué son las criptomonedas y qué usos se les puede dar. Y para entender sus usos positivos juegan el entendimiento y la aplicación de las tecnologías. La masificación de estos asuntos que hoy se asocian con el crimen, la suplantación de identidad, con la *darkweb* y tantas otras posibilidades. Desde esa perspectiva es necesario que el mundo entero entienda cuáles son los usos y no me refiero a los ingenieros y técnicos que saben cómo operan las criptomonedas, sino al potencial consumidor para las transacciones del día a día.

Julio López M.

Así como en el momento de hablar de *blockchain* les pedía que separáramos ese tema del *bitcoin*, en esta pregunta sobre las criptomonedas, también deberíamos hacerlo y así separar las *criptocurrencias* de sus tecnologías de base. Independientemente de la tecnología debemos entender lo que

significa *bitcoin*, preguntarnos si eso genera o es una disrupción. Se trata de un título valor, no es un activo; desde el punto de vista legal quiere decir que yo tengo un título digital y las personas le asocian un valor. Dicho título valor tiene una característica especial y es que no tiene ningún respaldo, además de no saber quién lo emite. Una de las principales características de su uso es el anonimato: todas las transacciones son anónimas. No existe ningún control. Es un título cuyo valor se basa en la especulación. ¿Qué define si el *bitcoin* sube o baja de precio? Lo que la gente esté dispuesta a pagar. Y, adicionalmente, los *bitcoins* se generan y se multiplican en unos nodos que llaman “mineros”, pero nadie puede decir en dónde están ubicados ni a quién le corresponden, ni por qué razón en el momento de una transacción de centavos de *bitcoin* se genera un *bitcoin* completo para el “minero” que la está generando y que encontró la llave antes que los demás. Hay unos pocos a quienes les venden la idea de que ellos pueden ser “mineros” con máquinas de dos mil dólares, con el argumento de que con eso son como los mineros del viejo oeste en California. El anonimato en su uso y su generación hace que la lectura del uso del *bitcoin*, (no sólo por la gente de la calle, sino por la gente técnica, experta, por el sector financiero), es que se presta para actividades delincuenciales. Cuando se observa que la moneda preferida con la que se transan drogas ilegales, armas, con la que se pagan secuestros (*ransomware*) es el *bitcoin*, quienes teníamos alguna duda al respecto, confirmamos su carácter delictivo. El hecho de que su valor se basa en especulación genera todavía más temor; aun cuando sabemos cómo se define el valor de la acción de una empresa,

nos encontramos con valores de acciones que han sido manipuladas por ochenta veces su valor, para timar a los pequeños inversionistas con o sin participación de intermediarios financieros, en donde la queja final es preguntar por la presencia de la Superintendencia Financiera, en términos de protección. Como técnicos insisto en que tenemos una responsabilidad en el sentido de aclararles a los inversionistas cómo se manipula el precio del *bitcoin* y de qué depende. Las burbujas nombradas pueden repetirse en el entorno del *bitcoin*. En este momento existen 900 o más *criptocurrencies* y en la red probablemente un número mayor y dentro de muy poco tiempo podrán existir nueve mil. Si no tenemos control sobre el mundo real por parte de la Superintendencia Financiera, ¿cómo será en la virtualidad? Me sorprenden los auditores y concedores de riesgos promocionando el *bitcoin*. Desde esta perspectiva, advierto sobre el riesgo y la necesidad de ilustrar a las personas sobre los peligros que corren sus inversiones en *criptocurrencies*. Hay quienes han calificado las criptomonedas como un sistema Ponzi, una pirámide; soy un convencido de tal situación y espero que alguno de los presentes me haga ver lo contrario. La principal disrupción en este entorno, son las monedas digitales, pero no las basadas en especulación ni en la falta de control. Estoy seguro de que en el país hoy en día se transa diez veces más el dinero electrónico que en físico, en papel. Pronto vamos a concluir que no necesitamos el dinero en papel, pero sí la entidad central que controle cuánto dinero está circulando por el medio para no hacerle daño a una sociedad, generando papeles virtuales que no tienen ningún respaldo y no corresponden con un de-

sarrollo social. De ahí surge otra inquietud en la que sí está la disrupción con las *criptocurrencias* y es en la generación de valor. ¿Cómo se genera valor en la sociedad? Inicialmente se generaba por trueque, mediante el intercambio, y dependiendo del entorno, se establecían las condiciones de dicho intercambio. Luego surgió la moneda de cambio y llegó el oro, establecido como la manera de generar valor y se trataba de encontrar esos metales preciosos. Más tarde vino el papel moneda para guardar el oro y no manipularlo. Hoy en día nos preguntamos ¿le estamos reconociendo generación de valor a un computador que encuentra una llave de encriptación? Como otro tema asociado a considerar, señalo que no debería existir temor por decir “tengo un determinado número de *bitcoins*” e incluirlos en la declaración de renta y, al final del año, indicar la venta y la ganancia de los mismos. No debería existir problema. ¿Se declaran los valores en *criptocurrencias*?

Rafael H. Gamboa B.

Definitivamente, cada vez que surge un nuevo entorno tecnológico se genera una disrupción tecnológica por la potencialidad que producen los diferentes tipos de opciones; y en lo social, por la expectativa, la emoción que genera de enriquecimiento rápido, de tener algo novedoso y vanguardista. Y no nos detenemos a pensar en el real valor económico que tiene ni en un asunto neurálgico como la confianza. Cuando hablamos de criptomonedas, como ya se ha mencionado, claramente comenzaron con “el pie izquierdo”. El mundo conoció la potencialidad de las criptomonedas, como consecuencia de la página *web silkroad*, para comercializar drogas, armas, pornografía, dándole un empujón al anoni-

mato que siempre se busca en Internet. El *bitcoin* tiene valor porque tiene demanda. Se han mencionado elementos que generan valor, confianza y control como el sistema financiero. ¿Por qué confiamos en que una transacción virtual de determinado valor, es cierta en el pantallazo que la soporta? Es porque alguien está regulando el sistema financiero, la Banca Central o la Superfinanciera. Esta última entidad ha señalado que los *bitcoins* no son una moneda real, porque no cuenta con respaldo, no tiene poder liberatorio. La define como un *commodity*, un bien que puede transarse sin equivalencia a un billete o a una transacción electrónica. ¿Cuál es el respaldo real de una *bitcoin*? Una demanda creciente generada por la sociedad. En tal sentido no se trata de adoptarlas ni tampoco de desecharlas. Existe un aspecto jurídico que no se puede desconocer, lo que buscan las normas es establecer un marco de confianza, si ocurriera una burbuja y no hay control por parte del ente estatal, la responsabilidad se le atribuiría al Estado. Es necesario un marco jurídico, para preservar la salud del sector financiero colombiano y para garantizar la seguridad de todos los ciudadanos del país.

Mauricio Pinzón G.

Me despojo del “gorro” de ingeniero para hablar como empleado de banco central. El dinero impreso o papel moneda, no es ni el 10% de la masa monetaria del país, el resto es digital desde finales de los años ochenta, cuando se usaba el término “desmaterializar”. En aquel entonces todos los papeles que representaban valor como títulos y efectivo fueron digitalizados. El dinero, respaldado por un país o un banco central ya es digital. Con respecto a si las criptomonedas representan real-



mente una disrupción tecnológica o una disrupción social, yo diría que si estuviéramos en la época de las cavernas y preguntaran si la sal es un asunto disruptivo en términos sociales y de avance, la respuesta es sí, en los dos aspectos. Tecnológicamente descubrimos la sal y socialmente adquirimos confianza en que la sal tenía valor más allá de sus propiedades físicas. No es posible comer sal ni oro ni papel moneda, como tampoco criptomonedas, pero son tecnologías que sirven para representar valor y alrededor de las cuales se genera confianza. Por ejemplo, un papel moneda lo cargamos en la billetera por la confianza que despierta en nosotros quién respalda ese papel. Si tengo un millón de pesos colombianos y debo escoger entre comprar francos suizos, oro, criptomonedas o bolívares ¿cuál sería mi preferencia? Hoy, a pesar de la existencia de los países, bancos y reguladores (ejemplo: Superfinanciera), existen personas que guardan su dinero o sus

joyas debajo del colchón y lo hacen pensando por fuera de este conjunto de actores. Mi respuesta es sí, las criptomonedas son una disrupción social y tecnológica, tanto como cualquier otra tecnología de representación de valor. Y, sobre si las criptomonedas son una nueva forma de activos que debemos regular y desarrollar, es como si en el momento que apareció el oro, las tribus trataran de regular la confianza que todas le tenían a este metal. Las criptomonedas nacieron después del año 2008, luego de la crisis en que muchas personas perdieran dinero y por ende confianza en gobiernos y en bancos. Esa confianza busca otros campos. Eventualmente, cada país regulará solamente lo que pueda controlar.

Luis Eduardo Daza G.

*Socio-Oficial de Cumplimiento
SurBTC*

*Profesor de la Universidad Javeriana
Exconsultor de la oficina UNODC de
las Naciones Unidas*

Aunque profesionalmente tengo varias “camisetas puestas”, hoy estoy como socio y oficial de cumplimiento de SurBTC, una compañía chilena que ofrece su plataforma tecnológica para comprar y vender (Exchange) *Bitcoin* y *Ethereum*, la cual abrió operaciones en Chile, Perú y Colombia y está abriendo espacio en Argentina. También he sido banquero, regulador, subdirector de la UIAF y consultor de Naciones Unidas en temas de antilavado y de riesgo. Con este preámbulo responderé las siguientes preguntas: ¿las criptomonedas representan realmente una disrupción tecnológica o una disrupción social? ¿Son las criptomonedas una nueva forma de activos que debemos regular y desarrollar? La respuesta es que corresponden a los dos tipos de disrupción y para entenderlo hago referencia a dos fuentes muy serias: la primera es el Manual de Oslo publicado por la OCDE y Eurostat en el que se definen cuatro tipos de innovación relacionadas con producto, proceso, organizativa y de mercadotecnia. Claramente, lo que está pasando con la tecnología *blockchain* y especialmente *bitcoin* cumple con las características de innovación que define dicho manual. *Bitcoin* es un ejemplo de algo innovador. La segunda fuente sería para afirmar que es disrupción tecnológica y social es Clayton Christensen, una de las autoridades en el tema de innovación. Según Christensen, la innovación puede ser disruptiva, incremental o evolutiva; la incremental mejora algo que ya existe con tecnología, y la evolutiva busca llegar a algún nuevo mercado o producto, mejorando las condiciones de algo actual. La disruptiva es aquella en la que existe algo realmente novedoso que surge lentamente y luego crece muy rápido. Y es ahí donde precisamente encajan *bit-*

coin y la tecnología *blockchain*. En otras palabras, según Christensen, es algo que comienza con pocos jugadores en el mercado y el componente tecnológico es lo que lo caracteriza.

Además, tiene la ventaja de crecer muy rápidamente y posicionarse al mismo ritmo. Además, existe también un caso de estudio realizado por unos estudiantes del MBA de la Universidad Javeriana que confirma que *bitcoin* es una innovación disruptiva, que también sirve de referencia. Aún no es público, pero muy pronto se podrá consultar. Además, disrupción social es aquella que busca resolver un problema social, como la escasez o calidad del agua, problemas de alimentación, contaminación, la calidad de vida de las personas, el transporte, entre otros asuntos. Y también *blockchain* y *bitcoin* encajan en una forma de innovación social, con varios ejemplos a citar. Uno muy claro es la identificación en algunos países africanos, en donde no tienen una identificación o pasaporte como nosotros y se ha utilizado la tecnología *blockchain* para el reconocimiento y registro inmodificable de las personas, entre otros ejemplos. Teniendo en cuenta esto y la tecnología *blockchain* a través de *bitcoin*, el reto como innovación social para Colombia ha sido el acceso a internet y el nivel de acceso al sistema financiero formal (bancarización). Según algunos datos conocidos, Asobancaria señala que aproximadamente un 72% de la población colombiana está bancarizada; medida como aquella persona que ha usado un producto financiero durante los últimos tres meses. El otro aspecto es el nivel de Internet. Según datos de Mintic, el país tiene un nivel de penetración aproximada del 52%. Por lo tanto, estos indicadores inciden direc-

tamente en desarrollo de proyectos de innovación social que propongan soluciones a problemas de la base de la pirámide. Y algo claramente disruptivo en el tema de *bitcoin* es la inclusión financiera. ¿Cuántas personas en Colombia tienen una tarjeta de crédito? Y la mayor forma de comprar a través de Internet es con tarjeta de crédito. En Latinoamérica se ha dado una gran exclusión a este mundo de compras digitales, porque las personas que no tienen tarjeta de crédito, no pueden acceder. En consecuencia, *bitcoin* ofrece una alternativa para hacerlo. Es una tecnología en la que, por medio de un teléfono y una conexión a la red, podría tener esa inclusión financiera. Por otro lado, en este momento existen mil 281 criptomonedas, un mercado que hoy vale 209 billones de dólares y si en media hora se hiciera una consulta, llegarían seguramente a mil 500. En cuanto a la regulación, lo que propongo es que debería darse en varias etapas. Hay que regular, autorregular o desregular en algunos casos en los que hay concentración, para que la tecnología de la que estamos hablando funcione. Existen ejemplos en algunos países como Estonia, con proyectos de Gobierno que permitieron adoptar la tecnología *blockchain* y las compañías pueden registrarse y es posible pagar impuestos. Estonia forma parte de la economía denominada D5 o “Digital five”; son cinco países que se pusieron de acuerdo para desarrollar proyectos de Gobierno en esa dirección. Existe también una regulación moderada, con la libertad para la tecnología y el desarrollo de negocios sometidos a un seguimiento y después de dos años, las autoridades entran a regular. En Colombia se debe regular no la tecnología, pero sí algunos actores. Hay 10 Superintendencias en el

país en las que se supone que existe una regulación para ciertas actividades económicas y empresariales, algunas de ellas mucho más fuertes que otras. La Superfinanciera es la más representativa en ese sentido.

Jeimy J. Cano M.

Es evidente que los contextos social y tecnológico están fusionados y aparecerán mayores retos para las personas, la tecnología y las empresas. El mercado de bitcoins cuesta billones de dólares en este momento. En otra dirección, ¿qué conocimiento deben tener los ingenieros para apropiarse y desarrollar nuevas opciones con blockchain?

Juan Mario Posada D.

Uno de los grandes desafíos que tenemos los ingenieros es la adaptabilidad, en el sentido de que cuando tenemos un perfil técnico nos acostumbramos a operar en ciertas condiciones y cuando llega una disrupción fuerte como la que están trayendo *blockchain* y las criptomonedas, tendemos a enfocarnos mucho en los defectos y dejamos de ver sus virtudes. Ya decíamos que estas nuevas tecnologías traen inmediatez, ayudan a fortalecer la confianza, la seguridad, la globalización y definitivamente si los ingenieros no nos adaptamos en conocimiento y en la disposición para el cambio, difícilmente vamos a lograr ser esos actores o mediadores entre la tecnología y la sociedad, papel fundamental que tenemos cuando contamos con el privilegio de disponer de ciertos conocimientos técnicos que nos ayudan a entender mejor los cambios tecnológicos de los últimos años. La tecnología por su dinámica nos mantiene en un permanente desafío. Naturalmente, debemos conocer la tecnología que

respalda los modelos de *blockchain* y las criptomonedas para lograr el enlace entre éstas y la sociedad, para favorecer las condiciones bajo las cuales se adoptan las nuevas formas de hacer negocios. De lo contrario, nuestro papel será inocuo, en la medida en que vamos a pasar desapercibidos. La resistencia al cambio lo único que hace es entorpecer lo inevitable que, en este caso es un gran volumen de negocios sujetos a los principios que ofrecen estas nuevas tecnologías.

Jeimy J. Cano M.

¿En las universidades se están proporcionando los conocimientos necesarios sobre estas tecnologías?

Juan Mario Posada D.

El desafío en las universidades es proporcionar las bases desde el punto de vista técnico, ético y moral. No creo que todas las universidades lo estén haciendo pero, sin duda, una de las características de la Academia es abordar algunas de estas tecnologías mucho antes de que se masifiquen. El reto es aterrizarlo al mundo de los negocios para que los estudiantes comprendan los efectos de apropiación de nuevas tecnologías. Desde luego la Academia juega un papel muy importante que deberá fortalecer. Pero también depende de la disposición que como ingenieros tengamos para abordar estas nuevas condiciones globales de los negocios y de la interacción social. No es una responsabilidad única de la Academia, cada uno como individuo tiene la obligación de conocer, aprender y adaptarse a las nuevas condiciones del mercado, con las criptomonedas y la tecnología *blockchain* como herramienta de inmediatez, seguridad, confianza y facilidad para los negocios y la solución de muchas ne-

cesidades de la sociedad. Y es una responsabilidad también de los individuos y del Estado asumir estos nuevos desafíos.

Fabio A. Rojas R.

Desde el punto de vista técnico y de conocimiento, no hay de qué preocuparse. Hace unos años conseguir ingenieros especializados en SAP era muy difícil, ahora eso es relativamente sencillo. Con el boom de *Data Analytics* se encuentran programas muy importantes en diferentes universidades. Por ejemplo, en la Universidad Javeriana –entidad en donde soy profesora– tenemos programas de *Data Analytics* para contadores. A medida que este tipo de tecnologías demuestran valor, importancia y uso, los conocimientos y la Academia parecen sincronizarse para atender la formación de los ingenieros. Tengo fe en que ese conocimiento se podrá asumir con responsabilidad para facilitar el uso de la tecnología *blockchain* y las criptomonedas. Para mí el reto es el de siempre, cómo lograr que los ingenieros se integren en el modelo de negocios y se conviertan en un puente que facilite el entendimiento y uso de la tecnología para los diferentes involucrados y no solamente para selectos grupos “gurú” en temas tecnológicos. No es lo mismo escribir en Internet www.google.com, que digitar cadenas de más de 30 caracteres que empiezan por 1 o 3, como en *blockchain*. Lo que sí veo es la falta de unión entre el mundo técnico y el lenguaje del negocio, del inversor, del regulador, del abogado y del usuario, ahí es donde está el reto principal.

Julio López M.

En estos aspectos podemos tener un consenso. Técnica y conceptualmente *blockchain* es un desarrollo de las es-

estructuras de almacenamiento de datos distribuidos y son conceptos de base que la universidad proporciona. Quiero resaltar mejor la ética y la responsabilidad social del ingeniero de sistemas específicamente. Tenemos una gran responsabilidad frente al uso de la tecnología y en lo relacionado con las *criptocurrencias*, todavía mayor. Entre más complejas sean las tecnologías, somos los ingenieros quienes tenemos que traducir a las personas del común y en esa dirección somos tendencia. Debemos ser conscientes de todos los riesgos asociados a las *criptocurrencias*, así como de todos los beneficios del *blockchain* como tecnología y tenemos la responsabilidad de mostrar estos riesgos a la sociedad. En las múltiples oportunidades que he tenido de asistir a conferencias sobre estos temas no he encontrado ningún conferencista que se refiera a los riesgos asociados a las famosas billeteras digitales de las *criptocurrencias*. La gente está colocando buena parte de su capital en esos espacios virtuales y me pregunto si conocen los riesgos a los que está expuesta una *cryptobilletera*. Si han contemplado después de su muerte ¿quién la va a heredar? Y ¿cómo se establece un juicio si ese dinero se quiere distribuir entre los miembros de su familia? Esos riesgos nosotros los ingenieros los conocemos y debemos plantearlos. Quiero destacar los temas de ética y responsabilidad social, ya que todo lo que se hable al respecto, será poco. Siempre habrá nuevos retos para los muchachos y nuevos focos de corrupción, de dinero fácil y esos principios hay que establecerlos. Por otro lado, el papel de la Academia me sorprende, en la medida en que no he visto que en el sector estén trabajando estos asuntos. He observado movimiento de los “pro-

fetas” de las *criptocurrencias*, pero poco del sector académico, de la misma manera que en los temas de irrupción digital y las estrategias frente a los nuevos desarrollos, tampoco se han abordado y debería hacerlo, toda vez que tienen un impacto grande en la sociedad. A nivel de investigación el aporte debería ser amplio y esta es una de las grandes carencias, tanto en el ámbito educativo como de la sociedad. Con relación a la regulación es necesario que los gobiernos del mundo se ocupen en la declaración de las *criptocurrencias* como un título valor, en procura de crear el marco jurídico de protección y control para sus inversionistas. Es necesario generar los mecanismos de control y seguridad para evitar el impacto que podría producirse por un descalabro financiero. Si reconocemos que las *criptocurrencias* están siendo utilizadas en actividades ilegales, todos los ciudadanos deberíamos estar de acuerdo en su regulación para generar el control respectivo.

Mauricio Pinzón G.

Como ciudadano, primero quiero aclarar que si uno tiene *bitcoins* debe declararlos. Como ingeniero y sobre el conocimiento que deben tener los ingenieros para apropiarse y desarrollar nuevas opciones creo que existen roles claros al respecto. Uno es el del ingeniero que analiza el caso de negocio y determina si los actores se beneficiarían del uso de esta tecnología. Lo podemos llamar “analista del negocio”. Este primero define quiénes y cómo van a interactuar en este caso de negocio usando *blockchain*. El segundo rol lo podemos llamar “arquitecto de soluciones”, este rol ve el caso de negocio, entiende la tecnología que lo puede apoyar por debajo, y define la

arquitectura. Finalmente, está el desarrollador que va a utilizar las librerías existentes y define y prueba objetos y flujos. La decisión de usar *blockchain* es del analista de negocio. La decisión de si se usa la arquitectura o servicio de *Ethereum*, *RSK*, *R3/Corda*, *IBM/Hyperledger*, *JPMorgan/Quorum*, etc., o si se toma el código abierto de alguna plataforma y se monta de manera autónoma es del arquitecto de soluciones. EL desarrollador tendrá que conocer a partir de esto las librerías que usan estas plataformas en *Golang*, *Kotlin*, *Solidity*, *Java*, etc.

Rafael H. Gamboa B.

Aunque no soy ingeniero de sistemas, voy a referirme a la pregunta sobre el conocimiento que deben tener estos profesionales y para hacerlo retomo lo planteado sobre la obligación de entender los riesgos, salir de su zona tecnológica de confort. En tal sentido, el ingeniero de sistemas debe participar en el negocio, más allá de la tecnología. Ahí está el reto para servir de puente entre las normas arcaicas que tenemos, frente al riesgo que existe al implementar nuevas tecnologías.

Luis Eduardo Daza G.

Aunque tampoco soy ingeniero, los comentarios expuestos aplican en dos niveles. Por una parte, algunos de estos profesionales deben conocer el tema del *blockchain* y otros acercarse con mucha mayor profundidad, en una forma más técnica. En cuanto a los temas fundamentales, sugeriría tres aspectos: el primero, es entender que esta tecnología está involucrada con la posibilidad de intercambiar bienes y servicios y afecta, o por lo menos cuestiona, la propiedad intelectual; esto invita a una reflexión de cómo esta tecnología viene cambiando estos dos

temas. En segunda instancia, se trata de una tecnología distributiva y es la mejor representación de la economía colaborativa y de negocios colaborativos basados en un ecosistema de múltiples emprendimientos alrededor de dicha tecnología. En tercer lugar, uno de los grandes retos es la divulgación de *blockchain*, intrínsecamente atada a *bitcoin*, con un enfoque de riesgo, porque efectivamente se ha abusado en algunos temas de intercambio de valor o como una forma alternativa y novedosa de pago. Como la humanidad, la tecnología se usa para lo bueno, que es la gran mayoría, y para lo malo, que es la minoría. Finalmente, los tres principales actores deben acercarse a una mejor comprensión de la tecnología; los negocios públicos, privados; los gobiernos y la academia. Una muestra de esa aproximación es el caso de una ciudad en Suiza que acepta el pago de sus impuestos a través de *bitcoin* y la tecnología *blockchain*. Al respecto, recomiendo el Informe de la Oficina para la Ciencia del Reino Unido (Distributed Ledger Technology: beyond blockchain) que en siete capítulos explica con claridad la tecnología distributiva para *blockchain*. Por su parte, la academia aún no se ve con una apropiación clara. Principalmente, el tema ha llegado a través de las iniciativas privadas y grupos de emprendedores o ecosistemas innovadores. No se ve la tecnología *blockchain* en programas de formación de pregrado, se ve más en posgrado que es donde está la realidad de los profesionales dirigiendo negocios o empresas. Tampoco hay una buena cantidad de proyectos de investigación. En Colombia, el tema ha tenido una muy buena acogida y en el sector financiero, por ejemplo, hay iniciativas como Colombia Fintech y

otras que desarrollan acciones de divulgación con el Ministerio de TIC o el Banco de la República; la DIAN, por su parte, emitió un pronunciamiento en el sentido de que quien obtenga recursos en asuntos de minería de *bitcoin* lo debe declarar como propiedad. La Superfinanciera también se ha pronunciado en varias oportunidades para sus vigilados en forma restrictiva y otras, como la Superintendencia de Sociedades, lo ha hecho en forma preventiva.

Jeimy J. Cano M.

Después del análisis hecho sobre diferentes aspectos relacionados con la tecnología blockchain y las criptomonedas, les pido a cada uno de los participantes formular una conclusión para finalizar el debate.

Juan Mario Posada D.

Quiero destacar el papel del ingeniero como puente entre la tecnología y la sociedad, siempre con una responsabilidad ética y moral, sin satanizar en este caso las tecnologías de *blockchain* y las criptomonedas. Desde luego, existen los riesgos y deben ser conocidos. Como consultor en riesgos he procurado transmitir la gestión de los riesgos enfocado a lograr el equilibrio entre los beneficios de las nuevas tecnologías y los riesgos que traen consigo. Definitivamente, me parece relevante el papel de aquellos que tenemos un perfil técnico para que los negocios entiendan las nuevas tecnologías y la sociedad también.

Fabio Rojas R.

Soy muy entusiasta frente a estos nuevos desarrollos de *blockchain* y las criptomonedas. Casos como *Ethereum* o el mismo *bitcoin* demuestran el potencial que existe. El dinero en pa-

pel está llegando al fin de su ciclo, como todo y como en todo existen riesgos; no creo que *bitcoin* sea una pirámide, existen pirámides que tratan de aprovecharse del término *bitcoin*, pero eso es muy diferente y tengo la convicción de que *blockchain* está en los comienzos de la evolución de la moneda. Nosotros los ingenieros debemos entender, comprender y transmitir que este tipo de tecnologías presentan muchas alternativas para nuevos modelos de negocio y de interacción. Los mismos Estados y los reguladores tendrán que modificar sus bases con prácticas diferentes para ejercer el control y la regulación. Estas tecnologías nos llevan a modificar, a explotar lo bueno y aprovechar los valiosos aportes. Mi visión es más optimista sobre la tecnología *blockchain* y las criptomonedas. Escenarios como este de ACIS contribuyen a la construcción sobre los nuevos desarrollos tecnológicos.

Julio López M.

Como reflexión final insisto en la separación de la tecnología *blockchain* y las *criptocurrencias*, porque se mezcla una tecnología con una aplicación que actúa como inhibidor hacia el uso de un desarrollo con un amplio alcance en los negocios. Coincido en enfatizar en la responsabilidad social que tenemos los ingenieros de sistemas en mostrarle a la sociedad los nuevos desarrollos con sus beneficios, riesgos y aspectos negativos. También debemos considerar la responsabilidad del gremio en esta órbita.

Mauricio Pinzón G.

En mi opinión y con todo respeto, concuerdo con Julio. Es arriesgado mezclar el tema tecnológico de *blockchain* con el marco legal y financiero de las

criptomonedas, porque se corre el riesgo de confundir al lector.

Rafael H. Gamboa B.

Desde el punto de vista jurídico, la tecnología está para servir a la sociedad y al mayor número de personas, ese precisamente es el fundamento de las normativas y las entidades de control. El interés general, prima sobre el interés particular. Nuestra experiencia nos muestra que, por lo general, los abogados le temen a los aspectos tecnológicos, por lo que descargan estos temas en el área de informática, lo que lleva a que los ingenieros de sistemas se vean envueltos en una serie de responsabilidades que no tienen que ver con su rol dentro de una organización y los ponen a revisar cláusulas y otros temas de carácter jurídico. De ahí la necesidad de que exista en las organi-

zaciones un equipo multidisciplinario, que permita la mejor implementación de la tecnología, buscando maximizar utilidades de la organización, dentro del marco legal que mitigue eventuales responsabilidades.

Luis Eduardo Daza G.

El tema que nos ocupa hoy plantea retos y oportunidades que se ajustan perfectamente al nombre de la sección de la revista “Cara y Sello”. Se trata de observar los diferentes enfoques que contempla la tecnología *blockchain* entre beneficios, riesgos, oportunidades y la manera de aclarar su alcance. Para finalizar recomiendo leer los artículos publicados al respecto, por distintas personas que ofrecen conocimiento sobre esta nueva tecnología y sus aplicaciones. 🌐

Sara Gallardo M. Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro “Lo que cuesta el abuso del poder”. Ha sido corresponsal de la revista Infochannel de México y de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador; investigadora en publicaciones culturales; gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res); corresponsal de la revista IN de Lanchile; editora en Alfaomega Colombiana S.A. y es editora de esta revista.

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 (Preuk-schat, 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 número 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” (Preuk-schat, 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 una plataforma 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-

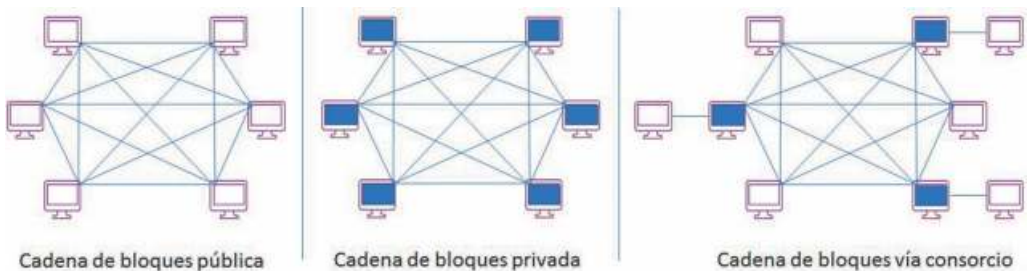


Figura 1. Tipos de cadenas de bloque (Tomada de: Lin y Liao, 2017, p.655)

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 propuestas 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 (EuroS&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-](https://oilprice.com/Energy/Crude-Oil/How-Many-Barrels-Of-Oil-Are-Needed-To-Mine-One-Bitcoin.html)
- 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-.

Blockchain, una mirada a la descentralización de las transacciones y de la información

Resumen

Las nuevas tecnologías de la información pueden generar valor a las empresas e industrias en una forma disruptiva y, dependiendo de su envergadura y proyección de crecimiento, también cambiar el mundo y la forma de conectarlo. *Blockchain* es una de ellas e incide en el modelo actual de negocios, en industrias como la financiera y de bienes raíces, generando una mejora en los servicios para brindar mayor valor a los clientes.

Este artículo busca explorar las bases del funcionamiento de la tecnología *blockchain*, sus principales características y las primeras aplicaciones, además de reflexionar hacia dónde se dirige y el impacto que podría generar.

Palabras claves

Blockchain, *bitcoin*, descentralización, base de datos, distribuida.

Rafael Bettín Díaz

Introducción

Dada la constante evolución de la tecnología y teniendo en cuenta que en promedio cada diez años surge el siguiente gran paradigma tecnológico, vale la pena estar a la vanguardia de los acontecimientos más recientes en

este campo. Desde los años 70 hemos pasado de las tarjetas perforadas al uso actual de la nanotecnología y los dispositivos móviles inteligentes, sumados a los desarrollos que produjo la aparición de Internet y ahora *blockchain* o bloque de cadenas.

De acuerdo con Swan (2015), *blockchain*, en su forma más precaria, "se comporta como el libro mayor en donde se almacenan todas las transacciones que se han ejecutado" [traducción del autor]. Su funcionamiento es como una base de datos que en una forma descentralizada permite almacenar transacciones e información de valor [traducción del autor] (Gates, 2017, Chapter I), todo esto bajo el concepto de libro mayor distribuido o DLT¹ por sus siglas en inglés. Cada transacción en este gran libro mayor se verifica por consenso de la mayoría de los participantes de la red y, una vez introducida la información, ésta no puede ser borrada, modificada o alterada [traducción del autor] (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2015, p. 1).

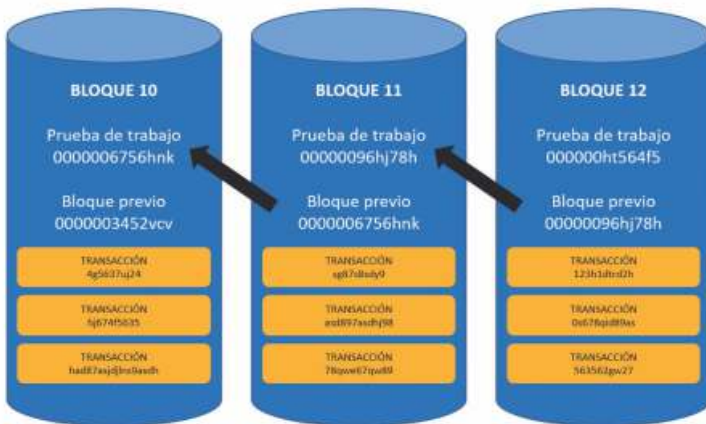
Para entender de una forma práctica los conceptos alrededor de *blockchain*, haremos referencia a una de las múltiples aplicaciones que esta tecnología puede tener, como lo es *bitcoin*, la moneda digital dada a conocer en un artículo titulado "Bitcoin: Un sistema

de efectivo electrónico Peer-to-Peer" (2008), de Satoshi Nakamoto, cuya identidad sigue siendo desconocida. *Bitcoin* permite a las personas realizar transacciones financieras directamente, sin una autoridad intermediaria y en cualquier otra moneda digital o efectivo electrónico en el mercado, fundamentadas en la tecnología *blockchain*.

Inicialmente, Satoshi describió una versión *peer-to-peer* de efectivo electrónico que permitiría los pagos en línea directamente de una parte a otra, sin tener que pasar a través del concepto de una institución financiera y cuyo almacenamiento de las transacciones se realizaría a través de cadenas de bloques; con cada bloque reciente o transacción, conectado o añadido a un bloque precedente y el bloque anterior a otro bloque precedente; en ese orden se forma una cadena de bloques o transacciones autenticadas y validadas mediante una firma digital. (Ver imagen 1)

¹ Distributed Ledger Technology

Imagen 1 : Almacenamiento de información y transacciones en *blockchain*



Fuente: Creación del autor.

Todo el sistema de *blockchain* por ser descentralizado y distribuido está construido en la confianza y la transparencia debido a que la identidad de los participantes es desconocida y la única autenticación se realiza a través de claves digitales, mediante la ejecución de varios algoritmos matemáticos [traducción del autor] (Icahn, 2017, p. 10).

Actualmente, la importancia de esta tecnología recae en las diferentes aplicaciones que, gracias a las investigaciones realizadas alrededor de ella, se han podido desarrollar, ampliando de manera significativa su alcance, rompiendo paradigmas y de una forma disruptiva incursionando en diferentes procesos que funcionan de manera centralizada, entre ellos los servicios bancarios, los bienes raíces y los procesos asociados a la cadena de abastecimiento.

Blockchain: ¿cómo funciona?

Una de las formas más fáciles para explicar el funcionamiento de *blockchain* es a través de una transacción financiera, simulando una transferencia des-

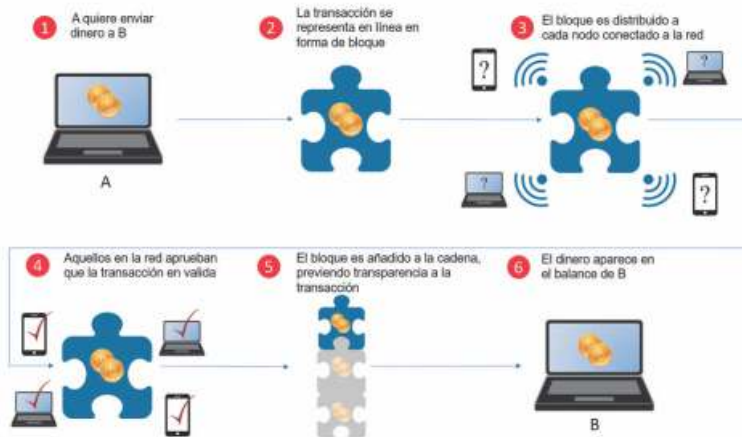
de el origen A, hasta el destino B, como se muestra en la Imagen 1.

Una vez que la transacción es creada por el sujeto A (1), se representa en línea como un bloque junto con muchas otras transacciones realizadas en el mismo período de tiempo (2); En este punto, con el fin de verificar la validez del certificado de esta transacción, se utilizan diferentes algoritmos matemáticos (funciones hash²) para cifrar la firma digital empleada para enviar la transacción. Este bloque creado, ahora se está transmitiendo a toda la red de nodos conectados (3) y todos los nodos conectados a la red *blockchain* verifican si la transacción es válida o no; este proceso se conoce como prueba de trabajo³ y puede tardar hasta 10 minutos, aproximadamente. Una vez que la transacción es validada y

² Las funciones hash: estas funciones son un algoritmo matemático que "toma algunos datos de entrada y crea algunos datos de salida" [traducción del autor] (Sean, 2016), Esto significa que una función hash se llevará a una entrada de cualquier longitud y tendrá una salida de longitud fija.

³ Prueba de trabajo: Se permite que cada nodo *blockchain* conectado a mantener transacciones segura y alcanzar un acuerdo resistente a la manipulación [traducción del autor] (Icahn, 2017, p. 18).

Imagen 2: Transacción financiera utilizando la tecnología *blockchain*



Fuente: (Crosby et al., 2015, p. 10)

aprobada por todos los nodos conectados (4), el bloque es finalmente añadido a la cadena (5); todo este proceso de 1 a 5 se conoce como minería⁴. Al final, el sujeto B puede ver la transacción reflejada en su balance (6).

Características de *blockchain*

Durante el desarrollo de este artículo hemos mencionado algunas de las características de esta tecnología, cómo funciona y algunos de sus usos potenciales. Ahora vamos a enfatizar en ciertos beneficios y oportunidades como la descentralización de la información y la trazabilidad en las transacciones, según Gates (2017) y Swan (2015). Adicionalmente, revisaremos algunos de los riesgos asociados, debido al manejo de redes públicas y otros aspectos relacionados con la seguridad.

Beneficios y oportunidades de la tecnología

- La transparencia es una de las mejoras más significativas de *blockchain*.
 - No hay intermediarios involucrados en el proceso.
 - Utiliza una red descentralizada.
 - Crea confianza entre los participantes de la red que, aunque nunca se han visto, pueden realizar transacciones entre sí.
 - La seguridad es proporcionada a través de la trazabilidad.
 - Todos los datos introducidos en *blockchain* son inmutables, inalterables o inmodificables.
 - *Blockchain* puede ser fácilmente auditable.
 - Ofrece múltiples usos, casi cualquier tipo de activos se pueden grabar en ella.
- La tecnología es bastante asequible, sin necesidad de grandes inversiones ni infraestructuras complejas. Ya hay plataformas basadas en *blockchain* como *Ethereum*⁵ que nos permiten crear aplicaciones descentralizadas (Dapps⁶).
 - *Costo reducido*, toda vez que con un solo libro es posible mantener registros de las transacciones realizadas.
 - Como es distribuida ayuda a aumentar la velocidad de la transacción. Esto se debe a que elimina los intermediarios y todo el mundo puede auditar y verificar la información registrada en ella.

Riesgos asociados a la tecnología

- Por lo general, las redes *blockchain* son públicas y están envueltas en falta de seguridad; significa que todo el mundo será capaz de ver las transacciones y el balance de todos los participantes de la red. Vale la pena resaltar que también hay *blockchains* privadas, que poco a poco han ido tomando más auge en los mercados.
- Las claves públicas y privadas⁷ en *blockchain* proporcionan al usuario la capacidad de realizar cualquier clase de transacción, dependiendo del tipo de red *blockchain* utilizada. Al perder una de las dos claves (pública o privada) se pierde todo y no hay manera de recuperar la información.

⁴ Minería: Se refiere a añadir nuevos bloques de registros (transacciones) en la contabilidad pública de *Blockchain*.

⁵ "Es una plataforma *Blockchain* que es pública y tiene una funcionalidad de transacciones programables" [traducción del autor].

⁶ "Ejemplos de las aplicaciones que se ejecutan en una red P2P de los ordenadores en lugar de un único equipo".

⁷ Es como el nombre de usuario y contraseñas que la mayoría de la gente utiliza como identificadores en cualquier otra aplicación.

A pesar de que la descentralización es algo por lo que sobresale esta tecnología, también puede ser una de las razones para que su adopción tome más tiempo, debido a que ninguna organización tiene control sobre *blockchain*.

- La red *blockchain* todavía tiene problemas de escalabilidad, debido a los tiempos empleados en minería y validación de las transacciones; el proceso puede ser más lento que con otras aplicaciones transaccionales centralizadas.
- Aún existe poca confianza por parte de la gente para utilizar este tipo de tecnologías en las que la información, dependiendo del tipo de *blockchain* implementada, puede ser pública.
- La regulación de los gobiernos y de las instituciones bancarias puede ser un problema al cual se enfrentará *blockchain* a lo largo del camino.
- La integración con los sistemas existentes y heredados es uno de los puntos críticos de esta tecnología, especialmente para las instituciones bancarias, debido al costo de la migración y la sustitución de los sistemas.

Aplicaciones en diferentes industrias

En servicios financieros

La principal área de estudio para los negocios y empresas alrededor de *blockchain*, es la combinación de los servicios financieros tradicionales con esta nueva tecnología. Para ello, la Red de Información Interbancaria (RII) de los más prestigiosos bancos a nivel mundial ha unido esfuerzos con el fin de investigar los posibles usos de esta tecnología y la forma de crear una red

global que permita realizar transacciones entre sus clientes y sus mismas entidades filiales. Ahora, los bancos con sucursales a nivel regional podrán realizar movimientos financieros entre éstas sin tener que retransmitir esos fondos a través de un intermediario” [traducción del autor] (Swan, 2015, p. 11).

En recaudación de fondos

Con el uso de tecnologías como *blockchain*, el modelo de negocios actual para los servicios de recolección de fondos de inversión (*crowdfunding*) cambiaría completamente; antes se necesitaba un servicio centralizado como *Kickstarter* o *Indiegogo* para permitir una campaña de *crowdfunding*, Ahora, con *blockchain* se elimina la necesidad de un tercero intermediario.

También se habilita la posibilidad de que los *startups* recauden fondos mediante la creación de sus propias monedas digitales y vendan "acciones criptográficas" a los inversionistas interesados. Estos últimos, en este tipo de campañas, mediante *blockchain*, reciben un *token*⁸ que representa las acciones de la empresa en la que han invertido [traducción del autor] (Swan, 2015, p. 12).

Con los contratos inteligentes⁹

Muchas de las industrias que utilizan la tecnología *blockchain* van a hacer uso

8 Unidad de valor emitida por una entidad privada (BBVA, 2017).

9 De acuerdo con los contratos de Smart Alliance - En colaboración con Deloitte, Nick Szabo describió un contrato inteligente, como un conjunto de promesas digitales, incluidos los protocolos y condiciones, que las partes estuvieron de acuerdo para llevar a cabo esas promesas [traducción del autor] (2016).

de contratos inteligentes y podrán intercambiar algo de valor en forma automática. Si se cumplen las condiciones de un contrato, los pagos o el intercambio de valor son realizados de acuerdo con sus términos. Del mismo modo, si no se cumplen las condiciones del contrato, los pagos pueden ser retenidos [traducción del autor] (Swan, 2015, Chapter VIII). Actualmente, empresas como Walmart en Estados Unidos, tienen este modelo como piloto para la compra de carne de cerdo desde Asia y gestionar la operación con sus proveedores.

Con Internet de las cosas¹⁰ (IOT)

IoT se está convirtiendo rápidamente en una tecnología popular para el consumidor y las empresas. Una gran mayoría de las plataformas de IoT se basa en un modelo centralizado, en el que como agente o *hub* controla la interacción entre los dispositivos. Sin embargo, este enfoque es poco práctico para muchos escenarios en los que los dispositivos necesitan intercambiar datos entre sí de forma autónoma.

Este requisito específico ha llevado a esfuerzos hacia IoT con plataformas descentralizadas. La tecnología *blockchain* facilita la implementación de estas plataformas descentralizadas para el intercambio de datos seguros y sobre todo para la confianza de la información, así como para el mantenimiento de registros. Este tipo de arquitectura, *blockchain* sirve como el libro mayor y mantiene un registro confiable de todos los mensajes intercambiados entre los dispositivos inteligentes en una topología IoT descentralizada [traducción del autor] (Crosby et al., 2015, p. 17).

En la cadena de suministro

En una implementación *blockchain*, un contrato inteligente puede desencadenar la transferencia de valores automáticos basados en condiciones. Basta imaginar un rastreador GPS¹¹ en un barco que desencadena un pago realizado en un instante a través de *blockchain*, una vez que la ubicación GPS de la nave demuestra que el buque ha llegado al destino del comprador [traducción del autor] (Hua & Notland, 2016, pp. 22, 23). En la industria de la cadena de suministro, las aplicaciones de *blockchain* están generando nuevos modelos para su mejora y automatización, permitiendo a los diferentes actores conocer toda la información de los diferentes productos, desde su cultivo hasta la entrega al cliente final, pasando por los diferentes procesos de transformación, lo que permite una fácil identificación y generación del certificado de origen de los mismos, sobre todo si hablamos del mercado de alimentos orgánicos.

El futuro de *blockchain*

“La tecnología más probable que cambie la próxima década de los negocios no es la web social, los grandes datos, la nube, la robótica, o incluso la inteligencia artificial. Es la blockchain ...” (Tapscott & Tapscott, 2016).

La cadena de suministro puede ser uno de los procesos que en este mo-

10 Internet de las cosas (IoT por sus siglas en inglés) “Es un término utilizado para una red de dispositivos que comprenden los frigoríficos, cámaras de seguridad, automóviles, aviones, computadoras, etc. ha existido durante un tiempo bajo diferentes formas y nombres” [traducción del autor](Guartime, 2017).

11 Sistema de Posicionamiento Global.

mento tiene más flexibilidad para adoptar esta tecnología; no obstante, su aplicación está actualmente bajo investigación por parte de las grandes compañías tecnológicas que seguramente integrarán la minuciosa de toda la cadena de valor *blockchain* del proceso, donde las empresas podrán realizar transacciones entre sí con un único “libro mayor” compartido para todas las transacciones, donde el tiempo y el papeleo que están gastando se pueden reducir considerablemente. Como parte de esta evolución vendrá sus integraciones con el sistema actual, con el fin de no hacer traumático el proceso de adopción, donde la tecnología se ejecutará en una capa de tecnología diferente a las que conocemos ahora, lo cual la hace transparente para el usuario final.

Por otro lado, esta tecnología todavía tiene un largo camino por recorrer, muchos obstáculos que superar y confianza que ganar. Las entidades y los gobiernos tienen que establecer una mayor regulación para ayudar con su adopción y las empresas empiezan a avanzar hacia nuevos modelos, servicios y propuestas tecnológicas basadas en *blockchain*. También, la infraestructura alrededor dará forma al futuro de la tecnología, para reducir su costo y rápida adopción.

Para el corto tiempo que lleva en el mercado ha avanzado ampliamente en su investigación, dando lugar a *blockchain* 1.0, para el uso en monedas digitales; posteriormente, *blockchain* 2.0, surgió para los contratos inteligentes y su aplicación con IoT; y, por último, *blockchain* 3.0, el estado actual de esta tecnología para diferentes industrias, a través del desarrollo de *Dapps*. Entre los sectores que en

un futuro próximo adoptarán *blockchain* como base para sus procesos figuran: el seguimiento de los impuestos, las entidades reguladoras, las cuales tendrán la oportunidad de conocer en tiempo real los movimientos financieros de todo el mundo y con antelación su patrimonio; la votación en línea y el almacenamiento en la nube. La información se distribuye en muchos servidores conectados a la red que todavía mantiene la privacidad de la información; la identidad digital será posible mediante el seguimiento de una persona desde su nacimiento, por cada documento relacionado con ella (Icahn, 2017).

Referencias

- BBVA. (2017, July 7). BBVA | Qué es un “token” y para qué sirve. Retrieved November 15, 2017, from <https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/>
- blockchainhub.net. (n.d.). What is a dApp? Decentralized Application on the Blockchain. Retrieved October 10, 2017, from <https://blockchainhub.net/decentralized-applications-dapps/>
- Bresett, M. (2017). Ethereum: What You Need to Know about the Block Chain Based Platform.
- Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2015). Blockchain Technology Beyond Bitcoin. Sutardja Center for Entrepreneurship & Technology Technical Report, Berkeley University of California, 35.
- Gates, M. (2017). Blockchain: Ultimate guide to understanding blockchain,

- bitcoin, cryptocurrencies, smart contracts and the future of money. (First Edition).
- Guartime. (2017). Internet of Things Authentication: A Blockchain solution using SRAM Physical Unclonable Functions, 16.
- Gupta, M. (2017). Blockchain For Dummies®, IBM Limited Edition. John Wiley & Sons, Inc. Retrieved from www.wiley.com
- Hua, A. V., & Notland, J. S. (2016, December 19). Blockchain enabled Trust & Transparency in supply chains. NTNU School of Entrepreneurship, Norway. Retrieved from <http://www.the-blockchain.com/docs/Blockchain%20enabled%20Trust%20&%20Transparency%20in%20supply%20chains.pdf>
- Icahn, G. (2017). BLOCKCHAIN: The Complete Guide To Understanding Blockchain Technology. Amazon Digital Services LLC.
- Satoshi Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, 9.
- Sean. (2016, November 29). If you understand Hash Functions, youll understand Blockchains. Retrieved October 5, 2017, from <https://decentralize.today/if-you-understand-hash-functions-youll-understand-blockchains-9088307b745d>
- Smart Contracts Alliance, & Deloitte. (2016). Smart Contracts: 12 Use Cases for Business & Beyond A Technology, Legal & Regulatory Introduction. Chamber of Digital Commerce, 55.
- Swan, M. (2015). Blockchain: Blueprint for a new economy (First Edition). California, United States: OReilly Media, Inc.
- Tapscott, D., & Tapscott, A. (2016, May 10). The Impact of the Blockchain Goes Beyond Financial Services. Retrieved October 13, 2017, from <https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services> 🌐

Rafael Bettín Díaz. Ingeniero de Sistemas de Información, Especialista en Gerencia de Proyectos, Est. Maestría en Ingeniería de Procesos. Actualmente y por lo últimos 3 años me he desempeñado como Gerente de Proyectos de implementación y desarrollo de software de gestión empresarial.

Regulación de blockchain como fenómeno disruptivo

Resumen

Sin ir más allá de lo poco dicho sobre la necesidad de regulación de las nuevas tendencias tecnológicas, el presente escrito busca dar una perspectiva general de la incidencia de *blockchain* en los nuevos modelos económicos que se sirven de los datos y la información como activos vitales, primordiales e incluso exclusivos en su desarrollo.

La sociedad de la información y del conocimiento, en términos de la normatividad colombiana vigente, como lo es la Ley 1341 de 2009, implica un Estado en obligación de reconocer que el acceso y uso de las Tecnologías de la Información y las Comunicaciones (TIC), es uno de los pilares sobre los que se erige la vigente sociedad y estilo de vida de los colombianos. Pero, ¿qué pasa cuando el anterior modelo social y económico, se niega a dar paso a la nueva dinámica informática?

Blockchain pone sobre la mesa nuevamente, el manejo político y regulatorio que (no) se ha dado a los diferentes fenómenos disruptivos que se presentan en la actualidad.

Palabras Clave

Blockchain, contratos inteligentes, *Big Data*, regulación, disrupción tecnológica.

Iván Darío Marrugo J. y Andrés Felipe Contreras P.

Introducción

Los fenómenos disruptivos en el mundo han llegado para quedarse. Suena paradójico pensar que algo que en sí

mismo se traduce en mutación, cambio y dinamismo, tenga la vocación de ser una constante en nuestra actual sociedad. Desde la llegada de aplicaciones de transporte como UBER y

otros servicios de plataforma como son el *crowdfunding* y aquellos prestados por compañías como AIRBNB (hotelería) o AMAZON (mensajería), se siente como improporrible satisfacer la necesidad de aplicar y usar las tecnologías, en cualquier escenario de nuestra vida, coyuntural o no.

Lo complejo no es alcanzar tal propósito, el potencial inventivo y la iniciativa son innegables. La dificultad surge cuando se relegan otros fenómenos culturales y económicos de estirpe tradicional (taxis, hoteles, fondos de inversión, etc.).

La tecnología es entonces una herramienta que provee encantos y desencantos dependiendo del extremo en el que cada persona se encuentre. Se vuelve entonces un catalizador de sentimientos y gustos que lo ubican a un lado u otro de la brecha tecnológica.

Con la implementación de *blockchain*, la codificación de transacciones y la sistematización de las mismas, se pone la lupa sobre las entidades financieras que hasta la fecha han asumido el rol de intermediarios en el flujo de activos que hay entre las cuentas de una persona A y una persona B. Esa actividad de intermediación es la que hoy podría empezar a ser superada gracias a este tipo de tecnologías.

Aunque puede llevar a imprecisiones, una forma de describir *blockchain* sería compararla con un libro de contabilidad digital de acceso público. Se comparte entre una comunidad de usuarios, creando o agregando un registro finito e inmutable de todas las transacciones que tienen lugar. Cada transacción se sella con fecha y hora, y luego se vincula a una transacción an-

terior, creando una cadena larga o un historial de intercambios, de ahí su llamativo nombre.

Dicho en otras palabras, “el concepto de descentralización de la información, uno de los principios fundamentales de *blockchain* es Distributed Ledger Technology (DLT), esto significa que no existe un documento único, mantenido por un solo agente (un banco, una institución gubernamental, etc.), donde se registran todas las transacciones, sino que cada usuario (también llamado nodo) mantiene su propia copia del registro de transacciones. Esto conlleva ventajas significativas: al no ser necesaria la existencia de un agente central, el sistema se torna más transparente y por lo tanto más justo, además de reducirse los gastos de intermediarios y aumentar la velocidad y agilidad de las transacciones; también se gana en seguridad e incorruptibilidad del sistema, ya no hay un único documento central susceptible de ser alterado fraudulentamente, sino tantos de ellos como usuarios existan en dicho sistema, falsear una transacción significaría alterar de manera simultánea miles o millones de documentos” (Agustín Muñoz).

Las personas que se inmiscuyen en la cadena de bloques, lo hacen con la doble dimensión de agentes vigías y usuarios dentro de este conjunto de nodos que compone el sistema. La ventaja es que, el sistema, tal cual como ha sido diseñado, permite validar las características propias de confidencialidad, integridad y disponibilidad de los datos que viajan a través de él, garantizando la seguridad y privacidad de los usuarios. En este punto debe aclararse que la información relativa a la transacción, como el tiempo en

que fue realizada y los bloques con los que interactúa, son de naturaleza pública, lo que quiere decir que se puede hacer una trazabilidad de la misma desde un punto 1 a un punto 2, sin revelar el emisor y destinatario de dichos datos. Es aquí donde reside el gran valor de algo como esto, empresas, negocios y el comercio minorista podrían beneficiarse enormemente de un sistema seguro. El mayor beneficio es que, debido a su naturaleza con sello de tiempo y proceso de registro automatizado, no es necesario supervisar el intercambio directamente, o, para decirlo de otra manera, no hay necesidad de un administrador. Los usuarios de *blockchain* y la comunidad que participan en cada transacción son todos administradores. He ahí el dilema.

Lo redundante en estos temas es la falta de control y el desequilibrio que el uso de estos nuevos modelos económicos plantea.

En términos sencillos, esta gran base de datos de múltiples actores, a más de propiciar una alternativa a la gestión de transacciones, mediante intermediarios que pueden alterar la regla de las competencias en el mercado, por su sencillez, anonimato y sistema especial de seguridad, plantea nuevos desafíos de orden legal que pueden o no tener una pronta respuesta, de conformidad con el ordenamiento jurídico vigente a cada territorio.

Uno de los desafíos

Regular fenómenos globales mediante egoístas visiones locales

El blanqueo de activos, la financiación del terrorismo y otras formas de delincuencia común, son modalidades cri-

minales que en contextos virtuales cada vez cobran mayor fuerza y se alejan de la vista prestante de los entes de control y fiscalización de nuestro país.

Esto necesariamente implica que, más allá de gestar políticas públicas, sociales y económicas y de la expedición de cuerpos normativos sesgados por el afán de atender tales situaciones, es imprescindible que los funcionarios estatales en especial y los ciudadanos en general, adquieran competencias y conocimientos en estos temas para así, adoptar respuestas preventivas y reactivas de cara al mal manejo de tecnologías y sistemas como lo es por ejemplo el *blockchain*.

A su vez, esto último lleva a que se genere un cambio de mentalidad en las personas. El sesgo que se adopte podrá conducir a una sociedad abstraída de las tecnologías, en la que los consumidores son ajenos a los componentes trascendentales de las mismas; o, por el contrario, puede generar una sociedad vanguardista, auto gestora y autoprotectora de sus derechos e intereses.

En Colombia, aunque tenemos gran cantidad de leyes, existe debilidad en el proceso regulatorio. Hoy por hoy, casos como Uber han exacerbado las posturas de entes como el Ministerio de Tecnologías de la Información en contra de otras como las adoptadas por el Ministerio de Transporte; y mientras se discute si la política pública de apropiación Tic tiene mayor peso que el afán regulatorio o de proteger un tipo anacrónico de negocio, es bastante el retraso en innovación tecnológica, y ese es sin duda el caso de *blockchain*. Los nuevos productos y servicios están evolucionando con base en las

transacciones de blockchain, pero actualmente no existen regulaciones sobre cómo deben escribirse las transacciones. Aunque éstas podrían audirse y permitirían que hubiera transparencia, de acuerdo con los beneficios prometidos por *blockchain*, las industrias altamente reguladas pueden necesitar desarrollar nuevas reglas para esta tecnología. Es probable que sus transacciones de contabilidad distribuida requieran cambios en las regulaciones de la industria de información financiera, así como los procesos de auditoría. También puede ser que las regulaciones de intercambio de información deban modificarse para proteger a las empresas, así como a sus inversores y sus clientes.

Tomando como base un interesante estudio de investigación de BBVA, en lo relativo al uso de la tecnología *blockchain* en los mercados financieros, se pueden plantear al menos siete retos importantes para dilucidar en el futuro.

1. Marco legal sobre la naturaleza jurídica de *blockchains* y libros distribuidos compartidos.
2. Marco legal para el reconocimiento de *blockchain* como nodos inmutables e inviolables.
3. Regulación del Derecho al olvido en la red.
4. Marco legal sobre la validez legal de los documentos almacenados en *blockchain* como evidencia de posesión o existencia.
5. Marco legal sobre la validez legal de los instrumentos financieros emitidos en *blockchain*, incluidas las criptomonedas.

6. Regulación de fenómenos como el de la jurisdicción y aplicabilidad territorial de la Ley en Internet.

7. Reglamento sobre el uso de *blockchain* como registro regulatorio válido para el Internet de los objetos.

Reflexiones finales

El proceso de adaptación a las nuevas tecnologías requiere un cambio rotundo de mentalidad en las personas. Es conveniente prever alternativas que satisfagan las necesidades de todos los frentes que se ven afectados con estos fenómenos, sin perder de vista que esta representación de equidad no puede desconocer el innegable e inevitable “siguiente paso” hacia una sociedad digital, de la *información y del conocimiento*.

La alternativa debe ser clara. Las entidades financieras, bancarias u otros intermediarios, deben cumplir con su objeto de la forma más eficaz y segura posible. Esto necesariamente los llevará a adoptar tecnologías y diseños basados en *blockchain* para que, de esta forma, no se vean rezagados o desplazados por operaciones paralelas en las que su intervención no sea necesaria y por ende no remunerada.

La respuesta a esta mutación y a este cambio generacional, seguramente no tarde mucho. Esperamos sea la más acorde con los intereses personales y sociales, tanto de proveedores de servicios como de consumidores.

Referencias

Definición Wikipedia: https://es.wikipedia.org/wiki/Cadena_de_bloques
Consulta 22/11/17. Una cadena de

bloques o cadena articulada, conocidas en inglés como Blockchain es una base de datos distribuida, formada por cadenas de bloques diseñadas para evitar su modificación una vez que un dato ha sido publicado usando un sellado de tiempo confiable y enlazando a un bloque anterior.⁶ Por esta razón es especialmente adecuada para almacenar de forma creciente datos ordenados en el tiempo y sin posibilidad de modificación ni revisión.

“Blockchain in Financial Services: Regulatory Landscape and Future Challenges for its Commercial

Application”, 2017. Publicado en: https://www.bbva-research.com/en/publicaciones/blockchain-in-financial-services-regulatory-landscape-and-future-challenges-for-its/?utm_source=twitter&utm_medium=social&utm_campaign=bbvaresearch&utm_term=13122016s

Agustín Muñoz. C.O.O .R.FINTECH PLC en https://blogs.elconfidencial.com/mercados/tribuna-mercados/2017-05-03/blockchain-criptomonedas-poder-manos-todos_1375854/. Hipervínculo consultado el 22/11/17. 🌐

Iván Darío Marrugo J. Abogado de la Universidad de San Buenaventura. Especialista en Derecho de las Telecomunicaciones de la Universidad del Rosario. Con estudios de maestría en Derecho Administrativo en la misma Universidad. Auditor Interno Certificado en Sistemas de Gestión de Seguridad de la Información ISO 27001. Computer Hacking Forensic Investigator (CHF1) v.8 del EC-Council. Experto en Derecho de las Tecnologías; se especializa en Comercio Electrónico, Derecho Informático, Seguridad de la Información y Protección de datos personales, Tecnologías de la Información y Comunicaciones, Evidencia Digital, Computación Forense. Socio Fundador de Marrugo Rivera & Asociados - FuturLex.

Andrés Felipe Contreras P. Abogado de la Universidad Externado de Colombia y Especialista en Responsabilidad y Daño Resarcible de la misma universidad. Coordinador de Investigación en el Departamento de Derecho Informático y de las Nuevas Tecnologías y editor del Blog jurídico del Departamento. Encargado del desarrollo, producción y gestión de investigaciones, conforme a los parámetros y lineamientos de Colciencias. Cuenta con diversos estudios en Derecho Económico, Derecho de Protección al Consumidor, Derecho de Telecomunicaciones, Nuevas Tecnologías y Diseño y Administración de Ambientes Virtuales de Aprendizaje - Moodle. Actualmente es Consultor Asociado de Marrugo Rivera & Asociados - FuturLex.

Afíliese a



Afíliate a la Asociación Colombiana de Ingenieros de Sistemas y recibirás los siguientes beneficios:

- Revista Sistemas trimestralmente y un boletín informativo mensual por correo electrónico.
- Precio especial en la inscripción a eventos y cursos organizados por la Asociación.
- Además los asociados tienen derecho de asistir, sin ningún costo, todos los jueves a nuestro ciclo de conferencias.
- Le ofrecemos el servicio del correo **acis.org.co** para que redireccione al correo de su preferencia. Para realizar la solicitud deben escribir un mensaje a: administrador@acis.org.co solicitando este servicio.

Tenemos afiliaciones para profesionales o estudiantes, anímate a ser miembro de este gran gremio.

Para más información consulte:

<http://bit.ly/2jpfcdn>

Calle 93 No. 13 - 32 - Oficina 102
Teléfonos: 6161407/09 - 3015530540
cursos@acis.org.co - acis@acis.org.co
www.acis.org.co



XXXVII Salón de Informática **La 4ª Revolución Industrial y la** **Malla Digital Inteligente:** **Oportunidades para la** **Empresa Colombiana**

Del 9 al 11 de mayo de 2018

Cámara de Comercio de Bogotá - Sede Chapinero - Calle 67 # 8 - 32/44

El Foro Económico Mundial declaró a principios del 2016, que nos encontramos en el inicio de la 4ª revolución industrial, caracterizada por el surgimiento de los sistemas ciber-físicos, es decir, por la integración de computación, redes de datos y procesos físicos. En el centro de esta revolución encontramos software fundamentado en algoritmos que aplican técnicas sofisticadísimas de inteligencia artificial y aprendizaje de máquina (machine learning), que conectados con redes de datos y con las personas mismas, generan ecosistemas complejos donde las oportunidades para lograr mejores productos y servicios basados en información, son infinitas. Estos conceptos coinciden con la propuesta de malla digital inteligente realizada por el Gartner Group dentro del su planteamiento sobre tecnologías estratégicas 2017. En qué consiste y cuáles son los retos y oportunidades que el avance de estas tecnologías implica para la empresa Colombiana, son los temas fundamentales del XXXVII Salón de Informática organizado por ACIS para este año.

Codirectores:

Maria Esther Ordoñez Ordoñez y Jorge E. Camargo Mendoza



Calle 93 No. 13 - 32 - Oficina 102
Teléfonos: 6161407/09 - 3015530540
cursos@acis.org.co - acis@acis.org.co - www.acis.org.co