La cadena de bloques (*blockchain*) Una tecnología disruptiva con el poder de revolucionar el sector financiero

Un informe técnico de EquiSoft

Marzo 2017

EquiSoft
SOLUCIONES INNOVADORAS

Tabla de Contenidos

Otros artículos de EquiSoft:

Invasion of the Robo-Advisor: Is the Threat Real?, Febrero 2016
CRM2 and its impact on the Canadian Retail Investment Industry, Enero 2015

Introducción

La tecnología de cadena de bloques, o *blockchain*, es una que tiene que conocer.

Debido a su enorme potencial, más de 70 de las mayores instituciones financieras del mundo (como Barclays, J.P. Morgan, Royal Bank of Scotland, State Street y UBS) forman parte de un consorcio que investiga y desarrolla la tecnología de cadena de bloques. Por su parte, el equipo Global Blockchain de PwC identificó más de 700 empresas emergentes en el sector[1], mientras que la tecnología de cadena de bloques es considerada por algunos como el quinto paradigma de la computación después de la computadora central, la computadora personal, el Internet y la revolución impulsada por la tecnología móvil y las redes sociales[2].

¿No está familiarizado con la tecnología de cadena de bloques? No es el único. De hecho, de acuerdo a una encuesta del año 2016, realizada entre ejecutivos de primer nivel de algunas de las principales instituciones financieras del mundo, menos del 20% de los encuestados afirmó estar «muy familiarizado» o «extremadamente familiarizado» con esta tecnología. Dicho esto, el 56% de los encuestados reconoció su importancia[3].

¿Por qué no hay un mayor conocimiento de una tecnología que tiene el potencial de revolucionar el comercio tal como lo conocemos? Creemos que esto se debe, en parte, a que muchas industrias están concentradas todavía en aprovechar la tecnología móvil e internet para mejorar las experiencias de los clientes. Los sectores de servicios financieros y de seguros, en particular, tratan de ponerse al día a este respecto. Con toda la atención que se pone en las plataformas *front office*, los sistemas arcaicos de *back office* y *middle office* están recibiendo poca atención y es ahí donde la tecnología de cadena de bloques adquiere una mayor pertinencia. Otro factor que contribuye a la falta de conocimiento en este sector puede residir en la dificultad que tienen las personas de comprender lo que en realidad es un cambio de paradigma en la manera en que los humanos han estado realizando negocios desde siempre.

En EquiSoft, creemos que la tecnología de cadena de bloques, y sus efectos potenciales en los sectores de servicios financieros y de seguros, ameritan una mayor atención. Como tal, hemos conformado un grupo de trabajo interno para comprender mejor la tecnología de cadena de bloques y saber cómo puede ser aprovechada por nuestros clientes. Como primera iniciativa, el grupo desarrolló una introducción básica al tema, la misma que es presentada en las siguientes páginas. Estamos convencidos de que esta síntesis les permitirá tener un panorama más claro y estimulará su reflexión respecto al gran potencial revolucionario de esta tecnología.

Jonathan Georges, CIM, FCSI
Vicepresidente, Soluciones de Gestión del Patrimonio
EquiSoft

888-989-3141, ext.201
jonathan.georges@equisoft.com

1 *PwC Global FinTech Survey 2016.*
2 *Blockchain: Blueprint for a New Economy.*
3 *PwC Global FinTech Survey 2016.*

¿Qué es una cadena de bloques o *blockchain*?

«La primera generación de la revolución digital nos ofreció el internet de la información. La segunda generación —impulsada por la tecnología de cadena de bloques— nos trae ahora el internet del valor: una nueva plataforma destinada a reconfigurar el mundo empresarial y a transformar, para mejor, el viejo orden de los negocios».

Don Tapscott, director ejecutivo del Tapscott Group y exitoso autor de *Wikinomics, The Digital Economy y Blockchain Revolution*

La tecnología de cadena de bloques o *blockchain* fue introducida por primera vez en un artículo técnico publicado en el año 2008 bajo el seudónimo de Satoshi Nakamoto, y es mejor conocida hoy en día como la plataforma base de la criptomoneda Bitcoin. Aunque los términos *blockchain* y Bitcoin son usados a menudo como sinónimos, es importante destacar que Bitcoin es tan solo una de las infinitas aplicaciones de la tecnología de cadena de bloques.

La cadena de bloques puede ser definida como un **libro contable público descentralizado diseñado para registrar las transacciones en un entorno protegido**. En otras palabras, es un tipo de base de datos usado para registrar las transacciones, que es copiado en todas las computadoras que conforman la red específica.

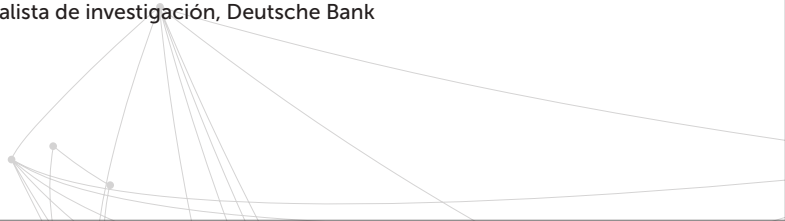
Para comprender con exactitud lo que eso significa, resulta muy útil tener en cuenta las deficiencias de los procesos de transacción existentes. Para ilustrar cómo se realiza una transacción típica en la actualidad, tomemos el ejemplo de John, quien desea comprar una camisa en la tienda de Jane. Debido a que John no tiene suficiente dinero en efectivo para pagar la camisa, y a que John y Jane no se conocen, se necesita que una tercera parte de confianza (como un banco o una compañía de tarjeta de crédito) garantice que John tiene la capacidad de pagar por la camisa para poder completar la transacción y llevarse la camisa a casa. Para ello, John pasa su tarjeta de débito o de crédito por el terminal de la tienda de Jane, la compra es aprobada y John sale con su nueva camisa. Bastante simple, ¿verdad? Bueno, no es tan simple como parece.

En promedio, cinco instituciones deben estar implicadas en una transacción de rutina como la que ocurre entre John y Jane: el banco de John, el banco de Jane, el proveedor de servicios comerciales de Jane, las entidades procesadoras de tarjetas y, en ciertos casos, la compañía de tarjeta de crédito (p.ej. Visa o MasterCard). Con todos estos participantes implicados en la transacción, puede pasar hasta una semana antes de que Jane reciba el dinero de la venta. Además, existen diversos puntos a lo largo del proceso donde puede ocurrir un fraude o un robo. Por obvias razones, este proceso es dispendioso e ineficaz.

¿Y si hubiera una mejor manera de efectuar la transacción entre John y Jane? La tecnología de cadena de bloques elimina la necesidad de intermediarios de confianza y permite que John pague directamente a Jane, de una manera más económica, rápida y segura.

«La cadena de bloques o *blockchain* representa un desarrollo netamente disruptivo que provoca el temor de los bancos respecto a esta tecnología, porque en la teoría pura de la cadena de bloques, muchos de los procesos de un banco tradicional pasarían a ser obsoletos».

Thomas F. Dapp, analista de investigación, Deutsche Bank



¿Cómo funciona la cadena de bloques?

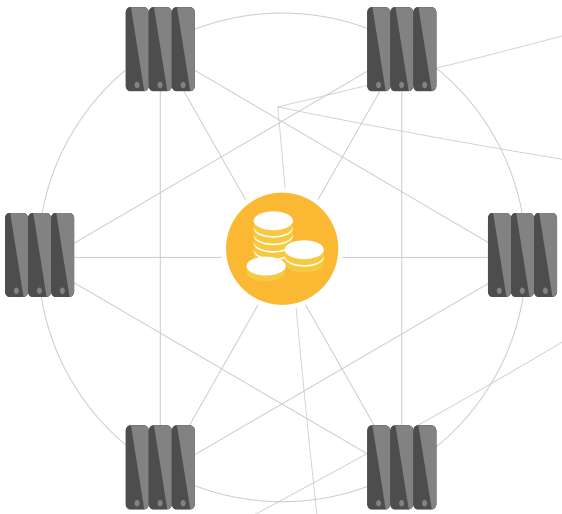
En cualquier sistema de transacciones debe existir un libro contable en el que figura el saldo de cuenta de todos los participantes. En la actualidad, estos libros son aislados y cerrados al público y, en esa condición, se requiere la presencia de terceras partes de confianza (p.ej. gobiernos, bancos, compañías fiduciarias, contables, notarios y papel moneda) para facilitar y aprobar las transacciones.

La tecnología de cadena de bloques es un software gratuito y de código abierto distribuido a nivel mundial que elimina la necesidad de terceras partes de confianza al hacer que una red de computadoras mantenga un libro contable común vía el internet. Este libro contable común es público y es distribuido en su totalidad a través de una red de «nodos», cada uno de los cuales tienen una copia completa del libro contable o de la cadena de bloques.

En una de cadena de bloques, todos los detalles de una nueva transacción son registrados, marcados con la hora y verificados por agentes denominados «mineros», quienes compiten por ser los primeros en resolver problemas matemáticos complejos y poder publicar el siguiente bloque de transacciones en el libro contable (o la cadena del historial de transacciones). Los mineros son personas que utilizan complejos sistemas informáticos para resolver problemas matemáticos y reciben un tipo de remuneración financiera por sus esfuerzos. Cuando el bloque de transacciones es subido por el minero que fue el primero en resolver el cálculo, todos los nodos de la red validan automáticamente el libro contable y todas las transacciones que se encuentren en él. Por lo general, la mayoría de los nodos (51 por ciento) deben aceptar que el bloque es válido para que éste pase a formar parte de la cadena de bloques de transacciones o *blockchain*. Los bloques de transacciones son usualmente publicados en el libro contable compartido a intervalos de diez minutos.

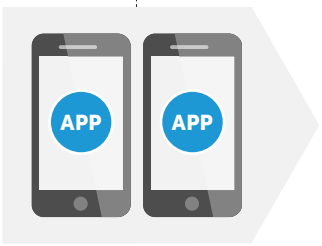
«No es difícil estar fascinada por algo tan transformativo».

Carolyn Wilkins,
vicegobernadora sénior,
Bank of Canada

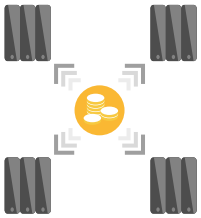


VOLVAMOS A NUESTRO EJEMPLO DE JOHN Y JANE, PERO USANDO ESTA VEZ LA TECNOLOGÍA DE CADENA DE BLOQUES PARA PROCESAR LA TRANSACCIÓN.

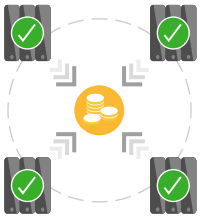
JOHN usa una aplicación de billetera electrónica (como una aplicación de banca móvil) en su teléfono inteligente, ingresando la clave pública de Jane obtenida al escanear un código QR del teléfono de ésta o por un correo electrónico enviado por ella y que contiene una dirección de pago cifrada.



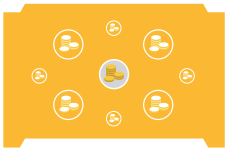
La aplicación informa a los « mineros » alrededor del mundo de que John desea efectuar una transacción específica con Jane.



Los mineros validan que John tiene suficiente dinero en su billetera electrónica para realizar el pago.

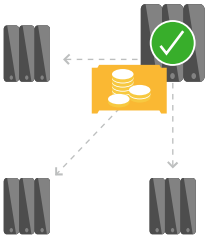


La transacción de John es agrupada junto con muchas otras transacciones solicitadas en un periodo de diez minutos, y el bloque de transacciones pendientes es enviado para su verificación.



Dentro de los diez primeros minutos del inicio de la transacción, **JANE** recibe el pago por la compra de John (en comparación con una semana en nuestro ejemplo anterior).

El minero ganador recibe una recompensa financiera (p.ej. Bitcoins recientemente emitidos) y el nuevo bloque es añadido al frente de la cadena de bloques.



Cuando un minero resuelve el problema matemático, lo anuncia al resto de la red.

Todos los mineros alrededor del mundo compiten por el derecho de publicar el bloque de transacciones en el registro compartido, resolviendo un complejo cálculo criptográfico.

En este ejemplo básico, los términos del acuerdo entre John y Jane para la compra de la camisa son claros y directos. Sin embargo, el tipo de detalles que pueden ser incluidos en las transacciones son ilimitados. Esto quiere decir que una simple transacción puede ser no solamente realizada eficazmente en una cadena de bloques, sino que los términos de un contrato complejo (p.ej. hipotecas, contratos de opciones y futuros, contratos laborales, contratos de seguros, etc.) también pueden ser manejados mediante una cadena de bloques. Un «contrato inteligente» en una cadena de bloques conserva los términos del contrato e incluso los ejecuta automáticamente mediante, por ejemplo, flujos de dinero automatizados. Estos contratos inteligentes eliminan la necesidad de intermediarios entre las partes, garantizan su cumplimiento automático y reducen significativamente la burocracia. De hecho, Capgemini estima que los contratos inteligentes serán implementados en aplicaciones prácticas de uso general antes del 2020, y que esto puede representar ahorros de 16 mil millones de dólares americanos anuales[4] para los consumidores ($500 USD para el consumidor promedio) en costos de banca y seguros.

4 Digital Transformation Institute de Capgemini, *Smart Contracts in Financial Services: Getting from Hype to Reality.*

¿Qué tan segura es la cadena de bloques?

Considerando el carácter público y compartido de la cadena de bloques, es natural que surjan preguntas respecto a la seguridad de las transacciones en este tipo de red. En realidad, la cadena de bloques es mucho más segura que las redes de transacción existentes.

En primer lugar, aunque el libro contable y todas sus transacciones son públicos, las personas que participan en la cadena de bloques mantienen el anonimato, por intermedio de claves cifradas públicas y privadas. Esto significa que incluso si todos conocen todas las transacciones y el saldo de todos los participantes en la cadena de bloques, no existe ninguna manera de relacionar las transacciones con las personas específicas.

En segundo lugar, debido a que cada nodo individual de la red posee un registro actualizado del libro contable, para modificar las transacciones en la cadena de bloques un pirata informático tendría que piratear por lo menos el 51 por ciento de los nodos mineros a nivel mundial (porque si no hay consenso, un bloque de transacciones no puede ser incluido en la cadena) en un tiempo de diez minutos (que es la frecuencia con que un nuevo bloque de transacciones es validado y agregado a la cadena). Por ello, se estima que se necesitaría combinar 200 de las más grandes súper computadoras del mundo para poder piratear el sistema[5].

«El comercio basado en la cadena de bloques es mucho más seguro que el sistema actual. El carácter distribuido de la red que verifica la integridad de las transacciones y los saldos asociados hace que sea matemáticamente imposible atacar con éxito el sistema».

Judd Bagley,
director de comunicaciones,
Overstock.com

5 *Future Bank Today.*

Aplicaciones de la cadena de bloques en los sectores de servicios financieros y de seguros

«La tecnología de cadena de bloques no sólo cambiará la forma de efectuar los pagos, también cambiará todo el ámbito de la negociación y la liquidación».

Oliver Bussmann,
jefe de información, UBS

«La tecnología de cadena de bloques redefine no solamente la manera como opera el sector de valores, sino también el modo de operación de toda la economía financiera mundial».

Bob Greifeld,
director ejecutivo, NASDAQ

Las aplicaciones de la tecnología de cadena de bloques, las cuales son obvias y bien documentadas, están centradas en el concepto de facilitar las operaciones de intercambio de dinero y la actualización de los antiguos sistemas heredados de transacción y de liquidación. Sin embargo, la tecnología de cadena de bloques ofrece a las firmas de servicios financieros y a las empresas de seguros otras e innumerables oportunidades para optimizar sus procesos y mejorar sus servicios.

Por ejemplo, la prevención del lavado de dinero y del financiamiento del terrorismo es algo sumamente costoso para las firmas financieras. De hecho, se estima que solamente el gasto mundial por las iniciativas de cumplimiento con las medidas de lucha contra el lavado de dinero ascendió a 10 mil millones de dólares americanos en el 2014[6]. Además, las exigencias de las políticas «conozca a su cliente» (KYC – *Know Your Client*) tienden a retrasar las transacciones y acarrean la duplicación sustancial de los esfuerzos de las distintas firmas. Un libro contable descentralizado basado en la cadena de bloques no solamente eliminará la duplicación de esfuerzos para completar las verificaciones KYC, sino que también permitirá que las actualizaciones de los detalles del cliente sean distribuidas a todas las instituciones casi en tiempo real. Asimismo, el libro contable descentralizado proporcionará un registro histórico de todos los documentos y actividades de cumplimiento de todos los clientes.

De la misma manera, en el sector de los seguros, los contratos inteligentes en una cadena de bloques pueden ofrecer a los consumidores y a los aseguradores los medios para gestionar los reclamos de manera transparente y eficaz. Los detalles de un contrato de seguros pueden ser almacenados en una cadena de bloques, y la plataforma también puede ser usada para validar los reclamos (reduciendo de esta manera la frecuencia de los reclamos fraudulentos) e incluso para activar los pagos automáticamente cuando se reúnan y validen las condiciones necesarias. Como resultado, se obtendrían procesos simplificados y una mejor experiencia del cliente.

6 KPMG, *Global Anti-Money Laundering Survey 2014*, KPMG, enero del 2014.

Los desafíos

Si bien la tecnología de cadena de bloques tiene el potencial de impulsar un cambio de paradigma en la forma como se hacen los negocios en el mundo, ésta no deja de tener desafíos. A continuación, indicamos algunos de los principales retos asociados con la adopción de esta joven tecnología.

ACEPTACIÓN

Debido a que la cadena de bloques es una tecnología tan sin precedentes, lograr su comprensión y aceptación por parte de los desarrolladores de sistemas, los usuarios y los operadores constituye todo un reto. Como la cadena de bloques representa una manera de pensar muy alejada de la manera como se hacen las cosas en la actualidad, los recursos y habilidades de TI en esta área podrían ser difíciles de conseguir, debido a que salen del conjunto de habilidades tradicionales de TI.

COSTO

Pese a que la tecnología de cadena de bloques puede ofrecer a las organizaciones ahorros increíbles en los costos, los altos costos iniciales pueden representar un factor disuasivo. Pasar de un sistema centralizado a una red descentralizada requiere cambios significativos o el reemplazo completo de la estructura heredada.

ASPECTOS REGLAMENTARIOS

Las divisas mundiales en la actualidad son por lo general creadas y reguladas por los gobiernos nacionales. Las criptomonedas, gestionadas por cadenas de bloques, pueden tener dificultades para lograr su adopción generalizada por las instituciones financieras existentes, si las preguntas acerca de su estatus normativo no son contestadas.

CONSUMO DE ENERGÍA

La tecnología de cadena de bloques necesita una cantidad importante de energía para mantenerse activa. Miren por ejemplo la cadena de bloques Bitcoin. Los mineros de la red proponen 450 mil billones de soluciones por segundo para validar las transacciones[7]. A medida que se añaden nuevas cadenas de bloques, las exigencias en cuanto a la capacidad informática de procesamiento pueden crecer exponencialmente.

NORMALIZACIÓN

Para que la cadena de bloques pueda acelerar eficazmente los procesos comerciales, mejorar el mantenimiento de registros, perfeccionar la detección de fraudes y mucho más, es necesario un cierto nivel de normalización global a través de las instituciones. Desafortunadamente, esto es algo más fácil de decir que de hacer. Las costumbres, los regímenes reglamentarios y los procesos políticos de los países pueden retrasar los esfuerzos de normalización.

«[La cadena de bloques] es una tecnología maravillosa y estoy convencido de que será disruptiva. Pero creo que tenemos mucho trabajo por hacer».

Peter Cherecwich, presidente de servicios globales de fondos, Northern Trust

7 Deloitte, *Insights*, « Blockchain technology: 9 benefits and 7 challenges ».

Hacia una normalización a nivel mundial

«La tecnología del libro contable descentralizado tiene el potencial de cambiar los servicios financieros de una manera muy profunda, similar al cambio producido por el internet en los medios de comunicación y en el entretenimiento».

r3cev.com

«...Ethereum está también llamando la atención de los gigantes de las finanzas y de la tecnología, como JPMorgan Chase, Microsoft e IBM...».

The New York Times

«Desde la aparición de la web, ninguna otra tecnología ha traído consigo la promesa de una revolución tan amplia y fundamental como la que nos propone la tecnología de cadena de bloques».

Hyperledger.org

En la actualidad, se están llevando a cabo varios esfuerzos que tienen el objetivo de contribuir a la normalización de la tecnología del libro contable descentralizado.

R3 es una compañía tecnológica que lidera un consorcio de 70 de las más grandes instituciones financieras del mundo, con la finalidad de investigar y desarrollar la tecnología del libro contable descentralizado en el sistema financiero. Hasta la fecha, sus esfuerzos resultaron en una plataforma descentralizada de código abierto llamada Corda, diseñada para registrar los eventos financieros y ejecutar la lógica del contrato inteligente.

La Fundación Ethereum es una organización suiza sin fines de lucro que desarrolló una plataforma descentralizada que ejecuta contratos inteligentes en una cadena de bloques personalizada. Esta plataforma, financiada originalmente por una «crowdsale» (venta al público) en el año 2014, hace posible que los desarrolladores creen mercados, mantengan registros de las deudas, trasladen fondos y mucho más.

Interledger es un proyecto colaborativo de código abierto que tiene el objetivo de desarrollar un sistema universal de pagos que permita efectuar pagos entre los participantes, independientemente del medio usado por el receptor del pago y por el pagador. El proyecto es conducido por el Consorcio World Wide Web (W3C), la principal organización internacional de normalización para la red informática mundial.

El proyecto Hyperledger es un esfuerzo colaborativo de código abierto creado para promover el avance de las tecnologías de cadenas de bloques en las diversas industrias. En esta colaboración mundial participan líderes de las finanzas, la banca, el internet de las cosas, las cadenas de suministro, la manufactura y la tecnología. El proyecto apunta a conglomerar una cantidad de iniciativas independientes y disímiles de desarrollo de estándares, proporcionando un marco de trabajo que sustente los distintos componentes de la tecnología del libro contable descentralizado para usos diversos.

Conclusiones

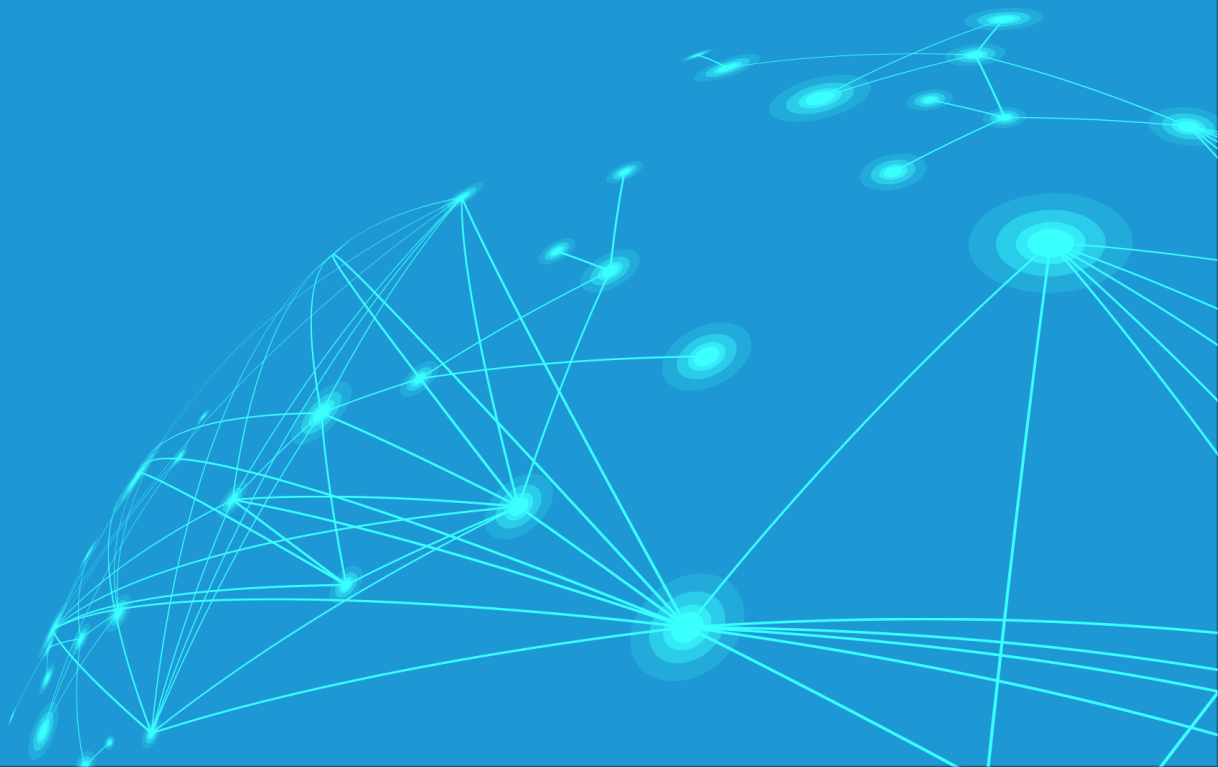
Hoy en día, la cadena de bloques es una tecnología emergente que tiene ciertos desafíos importantes en el futuro. Sin embargo, si es bien encauzada, la cadena de bloques tiene el potencial de causar una disrupción total en los modelos de negocios tradicionales y hacer obsoletos ciertos líderes actuales de la industria, en un lapso de cinco a diez años. Esa es precisamente la razón por la cual los líderes mundiales de la industria y las firmas emergentes están invirtiendo billones de dólares en la investigación, el desarrollo y la prueba de aplicaciones basadas en la tecnología de libro contable descentralizado.

Entonces, el grupo de trabajo de EquiSoft sobre las cadenas de bloques continuará siguiendo atentamente la evolución de esta estupenda tecnología para ayudar a nuestros clientes a adaptarse al posible cambio de paradigma en la manera en que se hacen negocios.

Independientemente de cuándo, o incluso de si alguna vez, la tecnología de cadena de bloques pase a ser de uso general, es algo que merece nuestra atención. Después de todo, ¿acaso la computadora personal, el internet y las redes sociales, hoy en día de uso corriente, no fueron alguna vez tecnologías emergentes que tenían un futuro incierto?

«Siempre sobreestimamos el cambio que ocurrirá en los próximos dos años y subestimamos el cambio que ocurrirá en los próximos diez».

Bill Gates



Equisoft se especializa en el diseño y desarrollo de soluciones de negocios digitales en las áreas de servicios financieros y de seguros.
Para obtener más información acerca nuestros productos y servicios, visite nuestro sitio web: www.equisoft.com.

CANADA | ESTADOS UNIDOS | CHILE | AFRICA DEL SUR | INDIA