La nueva economía blockchain y criptomonedas en 100 preguntas

Ismael Santiago Moreno

nowtilus

Colección: 100 preguntas esenciales
www.100Preguntas.com
www.nowtilus.com

Título: *La nueva economía blockchain y criptomonedas en 100 preguntas*
Autor: © Ismael Santiago Moreno

Elaboración de textos: Santos Rodríguez

Diseño de cubierta: NEMO Edición y Comunicación
Imagen de portada: Composición a partir de varios símbolos de bitcoin: Bitcoin, Litecoin, Ethereum, Ripple, Iota

ISBN Papel: 978-84-1305-083-6
ISBN Impresión bajo demanda: 978-84-1305-084-3
ISBN Digital: 978-84-1305-085-0
Fecha de publicación: octubre 2019

Impreso en España
Imprime: Podiprint
Depósito legal: M-28852-2019

A mi mujer Isabel y a mis hijos Ismael y Adriana.
Gracias por vuestra paciencia y apoyo.

Índice

II. Criptografía, cypherpunks, premios nobel visionarios y un tal Satoshi.
La historia de la nueva economía blockchain

III. Taxonomía de los criptoactivos

Prólogo

Debo comenzar reconociendo que prologar esta obra supone para mí una gran satisfacción y agradecimiento, y he comenzado esta labor con ganas e ilusión. Esto ha sido así por varias razones. Por un lado, porque un cometido de este tipo supone una muestra de confianza y afecto, sentimientos ambos muy gratificantes. Por otro lado, quien me ha pedido que prologue este libro es un compañero que, por su profesionalidad y amistad hacia mí, como poco, se merece este pequeño esfuerzo por mi parte.

Entrando a considerar la obra, cabe destacar la importancia y utilidad que tiene un texto de este tipo en uno de los momentos en que la economía y la empresa están pasando por una auténtica revolución tecnológica. Esta revolución tecnológica ha hecho que aparezcan nuevos riesgos y, a su vez, muchas oportunidades en todos los ámbitos. La empresa se ha vuelto más dinámica y flexible buscando una adaptación al nuevo entorno que aún hoy se está construyendo.

Hemos pasado de un modelo de negocio tradicional a un modelo de negocio innovador, donde la tecnología ha creado muchas oportunidades. Entre las tecnologías más disruptivas podemos destacar la inteligencia artificial, el internet de las cosas, la fabricación digital, la robótica, la *blockchain*, los vehículos aéreos no tripulados y la realidad virtual y aumentada, entre otras. Las

tecnologías apuntadas han dado paso a nuevos modelos de negocio que están cambiando la economía, nuestras expectativas y nuestro comportamiento. Este proceso responde a una dinámica clara, a una estructura que se ha dado a lo largo de todas las olas tecnológicas y que sigue un proceso que: (1) empieza con un avance científico, (2) que se materializa en una nueva tecnología, (3) que llega al mundo de los negocios (4) y que cambia la organización económica o social.

Hemos pasado de depender de un mercado nacional a un mercado internacional. Hemos pasado de una empresa donde la fuente de valor estaba en los activos tangibles a una empresa donde los activos intangibles han tomado una gran importancia. En este contexto, además de oportunidades, también existen riesgos, como la falta de seguridad tecnológica, de información, etc.; riesgo que se intentan cubrir con la ciberseguridad. Además, también existe una gran diferencia entre la velocidad a la que avanzan los cambios tecnológicos y el conocimiento de estos cambios por parte de los responsables empresariales, que son los que tienen que tomar las decisiones. Este desequilibrio entre avance tecnológico y conocimiento y formación, unido algunas veces a la publicación de textos poco entendibles y con un lenguaje excesivamente técnico de estos temas, hace que surja un riesgo importante, como es la falta de capacidad de toma de decisiones en este ámbito, lo que provoca que se tomen decisiones inadecuadas o a destiempo y que genera grandes pérdidas de oportunidades y, muchas veces, de dinero.

En este libro, se abordan las cuestiones relacionadas con todo lo relativo a la cadena de bloques, en particular, y la ciberеconomía, en general. Así, se resuelven de una forma clara y precisa muchas de las dudas que gran parte de los responsables económicos y empresariales tienen en la actualidad y se ayuda a aprovechar lo máximo posible las oportunidades vertidas por estos nuevos métodos y a reducir los riesgos, que no son pocos, que entraña todo este cambio por el que estamos pasando.

En este punto, es importante señalar el aspecto positivo del riesgo (riesgo significa posibilidad de perder y posibilidad de ganar), que en este ámbito sufrimos continuamente. Sin riesgo, no hay oportunidades. Por ello, este texto nos da un conocimiento necesario con el que tendremos una herramienta más para saber gestionar el riesgo y maximizar las oportunidades.

Mi más sincera felicitación a Ismael Santiago Moreno por el encomiable trabajo que ha realizado.

Dr. Félix Jiménez Naharro

Profesor titular de la Universidad de Sevilla y director del Máster en *Corporate Finance*, Emprendimiento y Búsqueda de Financiación de la Universidad de Sevilla

I

La evolución del dinero en el tiempo. Del trueque al bitcoin y otras criptomonedas

1

¿Cuál ha sido la evolución del dinero hasta hoy?

El dinero es un lenguaje que utilizamos para comunicar e intercambiar valor entre las personas. Usamos el dinero para realizar transacciones económicas, pero también para crear relaciones, sociedades y organizaciones. Con la invención de la red Bitcoin, se puede separar el concepto del dinero de la idea del Estado nación como emisor monetario soberano. Hemos evolucionado de la moneda basada en instituciones a la moneda basada en redes informáticas.

Para que el dinero sea considerado como una herramienta adecuada para efectuar intercambios de valor, debe cumplir con todas y cada una de estas ocho características:

- Confiable
- Durable
- Escaso
- Fácil almacenamiento y transporte
- Fácil de identificar

La funcionalidad del dinero. Fuente: Ismael Santiago.

En un sistema económico moderno, para que un bien pueda ser calificado como dinero, se deben satisfacer tres funciones principales:

- Medio de intercambio y pago. El dinero debe ser un bien ligero y fácil de almacenar y de transportar que evite las ineficiencias de un sistema del trueque. Para ello, el bien en cuestión es requerido con el solo propósito de usarlo para ser intercambiado por otras cosas, es decir, un medio de intercambio generalmente aceptado para ser utilizado en las transacciones.
- Unidad de cuenta. El dinero es un sistema de registro contable. La unidad de cuenta significa que es la unidad de medida que se utiliza en una economía para fijar los precios.
- Reserva de valor. Cuando un bien es adquirido con el objetivo de conservar el valor comercial para un futuro intercambio, entonces se dice que es utilizado como un depósito de valor. Cualquier activo que mantenga su poder adquisitivo a lo largo de tiempo servirá como depósito de valor.

A continuación, vamos a recoger las argumentaciones que tienen los críticos de las criptomonedas como dinero y sobre las funcionalidades que debe cumplir este, pese a que no lo hace.

El bitcoin se define como dinero, pero, para sus críticos, está muy lejos de cumplir todas las condiciones necesarias para ser

Bitcoin es el *internet del dinero*. Fuente: Benjamín Nelan en Pixabay

envías una transacción a la red, todo participante la trata de igual manera.

Cualquier día, y Dios no lo quiera, podría darse el caso extremo de que llegáramos a un cajero automático para sacar dinero y el banco se negara a hacerlo, porque no estaría obligado a ello, como pasó en su día en Argentina, Chipre, Grecia o Venezuela, entre otros casos. El por qué lo encontramos en la arquitectura propia que tiene actualmente el dinero, que es deuda y donde no se tiene el control sobre este, ya que toda interacción está mediada y controlada por una tercera parte que tiene control absoluto sobre este dinero.

Bitcoin no se basa en la deuda como el actual sistema económico imperante sino en la libre disponibilidad y propiedad de uno tiene de sus criptomonedas, sin fronteras y sin limitaciones transnacionales.

En las tres olas descritas encontramos un denominador común, la importancia creciente del software y su impacto en los diversos sectores económicos.

En la economía actual, las principales empresas son de software, independientemente del sector al que se dediquen o presten servicios. Ejemplos de ello lo encontramos en: Netflix, como el mayor servicio de video por número de suscriptores del mercado; Amazon, donde su capacidad principal es su motor de software para vender virtualmente de todo on line; Apple (con iTunes),

Transferir bitcoins es tan sencillo como enviar un email. Fuente: Mohamed Hassan en Pixabay

importante que nunca se divulgue a nadie la clave privada y que permanezca en secreto con su propietario, ya que, si alguien lo supiera, podría acceder a los fondos y robarnos nuestro dinero. La mayoría de las aplicaciones Bitcoin aseguran mantener la clave privada protegida bajo una contraseña cifrada.

Es importante aclarar que los bitcóins que recibamos no representan ningún archivo de nuestro ordenador, ningún metal o papel, sino que, en realidad, de lo que se trata es de un valor que nuestra dirección puede tener, de la misma manera que nuestra cuenta bancaria no representa dinero que está literalmente ahí, sino que es un valor que un banco le da a nuestra cuenta. Las direcciones de Bitcoin funcionan de la misma manera. A cada dirección le corresponde un valor que puede disminuir o aumentar según las transacciones que lleguemos a realizar. Aquí es cuando entra en funcionamiento la red entre iguales o P2P (*peer to peer*), donde los nodos interconectados se encargan de vigilar y de registrar el nuevo valor de la dirección difundiendo la información de dicha transacción por toda la red, quedando respaldada de forma veraz e inmutable gracias a un complejo sistema de seguridad criptográfica. Un ejemplo explicativo sencillo de cómo funciona esta operativa sería el siguiente: Ismael es hermano de Adriana. Este dispone en su monedero electrónico de 0,4 bitcóins y decide enviar a su hermana Adriana 0,1 bitcóins. Ismael emplea su clave privada para autentificarse y anunciar a la red una nueva transacción. Después de esto, la red Bitcoin toma nota de esta transacción

Bitcoin es el nuevo oro digital, con una oferta máxima limitada a 21 millones de unidades y «mineros» que los generan con su poder computacional.
Fuente: Mohamed Hassan en Pixabay.

Satoshi Nakamoto eligió el modelo de los metales preciosos para bitcoin los encontramos en lo que ya hemos dicho: el oro sigue funcionando y lo ha hecho durante milenios y, además, este metal precioso cumple los requisitos de una buena moneda: fácil almacenamiento, durabilidad, portabilidad, homogeneidad, difícil falsificación, divisibilidad, fungibilidad, amplia distribución geográfica y la baja proporción existente entre su producción anual y las existencias.

No obstante, el oro tampoco es perfecto como medio de intercambio y preservación del valor: su resguardo es caro y arriesgado, es relativamente sencillo de falsificar, no puede ser transportado electrónicamente, es difícil transportar grandes cantidades de forma segura, la cantidad de oro en una moneda puede ser alterada y las pequeñas unidades no son convenientes para el intercambio cotidiano.

Muchas veces, se suele decir que bitcoin posee unas cualidades similares al oro, ya que no es emitido por un banco central o un Gobierno. Este es posible por la red de ordenadores que la forman, donde encontramos miles de mineros que hacen de ella una moneda completamente segura y descentralizada. Por otro lado, bitcoin es un activo digital criptográfico que busca resolver los problemas de la moneda fiduciaria y, a la vez, quizás las del oro. Muchas personas consideran que los precios de los bitcóins o el

Bitcoin surge como respuesta a la grave crisis económica del 2008.
Fuente: Gerd Altmann en Pixabay

Los Gobiernos deben reconocer su papel en una nueva gobernanza y en la gestión de la tecnología de cadena de bloques y saber cómo afectará esto a su histórico papel en las regulaciones financieras y en las fijaciones de las políticas monetarias. Los Estados han ejercido su monopolio sobre el dinero durante milenios, pero podría darse la situación histórica de que el dinero no fuera exclusivamente emitido por una autoridad central, sino que, en su lugar, fuera también creado por una red global de entre iguales que se va distribuyendo, como es el caso de los más de 4000 criptoactivos disponibles en el criptomercado.

La regulación difiere de la gobernabilidad. La gobernanza tiene que ver con la gestión colaborativa y los incentivos para actuar sobre intereses comunes, mientras que la regulación busca el control del comportamiento mediante la imposición y el empleo de medios coactivos. La experiencia sugiere que los Gobiernos deberían abordar la regulación de las tecnologías de descentralización, como lo son los criptoactivos, con cautela, actuando de manera colaborativa con otros sectores de la sociedad, en lugar de ser la mano dura de la ley que impide la innovación y la libertad de hacer, construir y producir riqueza, como nos enseñó Adam Smith.

Bitcoin es deflacionista y no permite que los bancos generen nuevo dinero mediante la reserva fraccionaria. Fuente: OpenClipart-Vectors en Pixabay

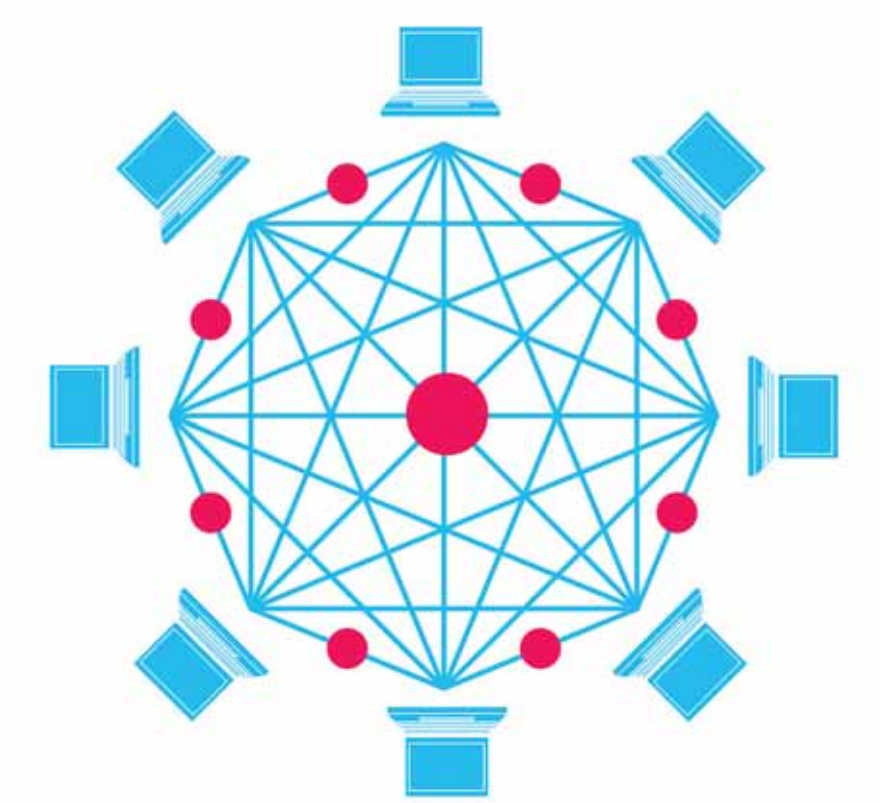
para protegerse de la inflación, disponiendo para ello de las siguientes características:

- *Sin fronteras*. Ya no es necesario el Estado como intermediario que dota de confianza al sistema económico, ya que las matemáticas, expresadas a través de código de software, se encargan de proveer la confianza entre los usuarios, eliminando por completo la participación de intermediarios humanos y considerando que todos los datos que transitan por una blockchain son verificables públicamente en tiempo real.
- *Global*. La red funciona estando distribuida en nodos localizados alrededor del mundo que contienen una réplica exacta de la blockchain, preservando de esta manera una misma verdad que no puede ser modificada arbitrariamente por ninguno de los nodos sin que haya un consenso generalizado.
- Abierta: se basan en software de código abierto, donde cualquier persona puede participar en la red sin pedir ningún tipo de autorización, descargando una copia parcial o total de la blockchain.
- *Neutral*. Cada usuario de la red sigue las reglas de consenso neutralmente y, si no las sigue, sencillamente termina siendo expulsado. Blockchain no sirve a los propósitos de ningún Estado, organización o institución.

Democratizando la «confianza» gracias a blockchain.
Fuente: InspiredImages en Pixabay

persona. Así como el internet transformó radicalmente las comunicaciones, blockchain cambiará la forma en que nuestra sociedad se organiza. La cadena de bloques impone la confianza, la verdad, la honestidad y la transparencia. Blockchain redefine las creencias comúnmente aceptadas en torno a la confianza. Lo que está en el corazón de la cadena de bloques es alcanzar el consenso, pero esta lo hace de una forma descentralizada, rompiendo el viejo paradigma del consenso centralizado. Blockchain es una base de datos pública, transparente, distribuida y replicada entre todos los usuarios de la red que almacena y mueve todo tipo de datos, incluyendo activos (dinero, acciones, música, títulos de valor, certificados) sin jurisdicciones ni fronteras geográficas y que funciona de manera instantánea. La cadena de bloque contiene un sistema contable cuyos asientos o transacciones, codificados a través de un algoritmo criptográfico, se encuentran almacenados en una estructura secuencial de bloques ordenada cronológicamente. Estos datos contenidos en los bloques son incorruptibles y no pueden ser modificados sin el consenso de todos los usuarios de la red (llamados nodos).

El protocolo de blockchain permite que dos individuos realicen transacciones entre ellos a través de internet. Por ejemplo, cuando se transfiere digitalmente el valor de una cuenta a otra en una cadena de bloques, se está confiando en el sistema blockchain



La nueva economía blockchain se basa en la descentralización.
Fuente: Tumisu en Pixabay.

registran, continua y secuencialmente, transacciones en un bloque público. Cada bloque sucesivo contiene un hash (una huella dactilar única) del código anterior, por lo que se utiliza la criptografía (a través de códigos hash) para asegurar la autenticación de la fuente de la transacción y eliminar la necesidad de un intermediario central. La combinación de la tecnología de criptografía y de la tecnología de contabilidad distribuida de la cadena de bloques garantiza la seguridad de la red. Blockchain solo provee una forma segura y flexible de organizar la información que, al combinarse con un algoritmo de consenso, da como resultado un sistema descentralizado.

En estos momentos, existen varias alternativas para los mecanismos o algoritmos de consenso, de las que destacaremos dos: prueba de trabajo (PoW) y prueba de participación (PoS).

Con respecto a la prueba de trabajo (PoW), en la blockchain, este algoritmo se usa para confirmar transacciones y producir nuevos bloques en la cadena. En la prueba de trabajo, los mineros

Conceptos que engloban la N.E.B. Fuente: de Mary Pahlke en Pixabay.

El principio de la abundancia se expresa de una forma más precisa del siguiente modo: en una red, cuantas más oportunidades se aprovechen, más rápido aparecerán oportunidades nuevas. En la economía interconectada, cualquier cosa que se puede hacer se puede hacer en abundancia, lo cual se traduce en generación de valor y en la apertura de sistemas cerrados. Tradicionalmente, en la economía, el valor procede de la escasez: oro, diamantes, Ferraris, etc. Por lo general, cuando las cosas son abundantes, estas pierden valor. Pero la lógica de la red da un giro a todo esto haciendo que, en la economía interconectada, el valor proceda de la abundancia. Como el ejemplo de la imprenta de Gutenberg, con la que, generalizando la producción de libros e incrementándose la disponibilidad de estos mediante copias económicas, aumentaba el valor intangible de las relaciones y la multiplicación de estas. Las relaciones se disparan en valor a medida que se incrementen las partes implicadas.

Ley de Moore

En 1965, Gordon Moore, cofundador de Intel, afirmó que el número de transistores por unidad de superficie en circuitos integrados se duplicaba cada año y que la tendencia continuaría durante las siguientes dos décadas. Este redefinió su ley y amplió el período a veinticuatro meses. El cumplimiento de esta ley se ha

II

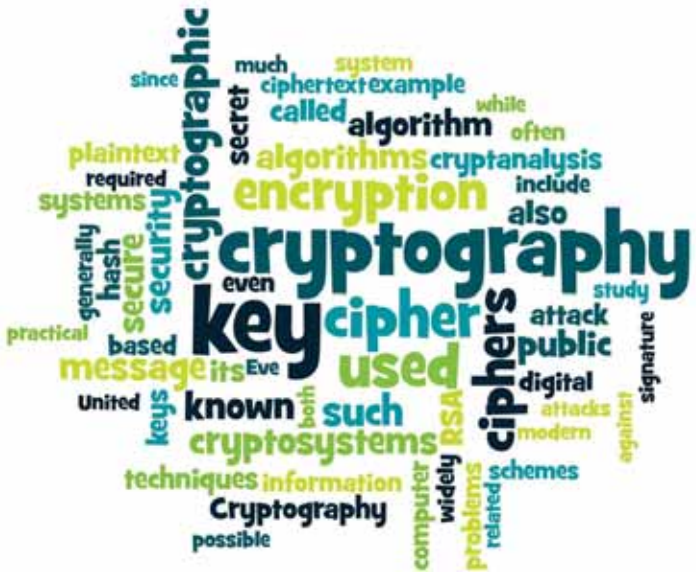
Criptografía, cypherpunks, premios nobel visionarios y un tal Satoshi. La historia de la nueva economía blockchain

11

¿La nueva economía blockchain depende de la criptografía?

La criptografía es un método para mantener la información segura y secreta transformando un mensaje legible en otro ilegible. A este procedimiento se le denomina *cifrado*, mientras que a la recomposición del mensaje en un formato legible se le llama *descifrado*.

En criptografía, existen dos conceptos clave: el cifrado y la llave. El cifrado es el conjunto de reglas que emplearíamos para codificar la información; respecto a la llave, esta nos indica cómo se deben ordenar las reglas del cifrado. Aunque muchas personas pueden tener acceso al mensaje cifrado, si no disponen de la llave, no podrán leerlo.



La criptografía es el núcleo tecnológico de la nueva economía blockchain. Fuente: tumbledore en Pixabay.

La clave privada, en definitiva, no es más que un número aleatorio tan grande que es estadísticamente imposible generar otro igual. A partir de este número, se calcula la clave pública usando el algoritmo de encriptación ECDSA (Elliptic Curve Digital Signature Algorithm). Este algoritmo proporciona la misma o mayor seguridad que el resto de algoritmos de clave pública, pero es más eficiente, rápido y escalable. Se utiliza en las blockchains para obtener las claves públicas y para firmar y verificar las transacciones. En definitiva, este algoritmo nos permitirá obtener una clave pública a partir de una clave privada. Con ambas claves, ya podremos firmar transacciones y verificar luego las firmas.

Con todo esto lo único que ya nos faltaría es la dirección Bitcoin, que es totalmente pública y que sirve para que podamos recibir transacciones. Esta dirección no es más que nuestra clave pública *hasheada*. La criptografía juega un rol importante en las criptomonedas, entre las funciones más importantes destacamos el *hashing* y la firma digital. El hashing es un método criptográfico para modificar importantes cantidades de información en otra mucha menor que es difícil de imitar. Es el componente principal de la tecnología blockchain. Recuerda, el hashing es la huella dactilar de un mensaje o documento.

Otro de los matices que hacen especialmente conveniente a este tipo de algoritmos para blockchain es que, si cambiamos un solo dato del documento, todo el hash entero cambia. Esto es crucial en la concatenación de los bloques de la cadena, ya que un bloque tiene como dato el hash del contenido del bloque anterior

Los cypherpunks establecieron las bases de la red Bitcoin.
Fuente: Gerd Altmann en Pixabay.

dactilar digital, para que nos entendamos). A diferencia de Bitcoin, b-money nunca llegó a funcionar.

Nick Szabo creó Bit Gold, que consistía en un sistema de intercambio de valor que disponía de un novedoso sistema de consenso de red inspirado en la teoría de juegos y que evitaba la posibilidad de realizar el doble gasto con el mismo dinero en la red gracias a la resolución de un problema matemático.

Hal Finney colaboró notablemente en el desarrollo de un sistema de pruebas de trabajo reutilizables totalmente funcional antes de Bitcoin, además de su activa participación en los primeros días de Bitcoin, para lo que fue uno de los más activos interlocutores de Nakamoto y uno de los primeros en descargarse y utilizar la primera versión del cliente de Bitcoin.

En resumen, la privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad en una sociedad abierta requiere de sistemas anónimos para efectuar transacciones. Un sistema anónimo ofrece la capacidad a los individuos para revelar su identidad solo cuando lo deseen. Así mismo, la privacidad en una sociedad abierta requiere de la criptografía. Encriptar es indicar que se desea la privacidad. Los cypherpunks se dedican a construir sistemas anónimos y defienden su privacidad con criptografía.

La privacidad fue una de las principales preocupaciones de Satoshi Nakamoto en el desarrollo de la red Bitcoin. Fuente: OpenClipart-Vectors en Pixabay.

muy similar a lo que propone Bitcoin. Este conjunto de cosas lo hacen ser un claro candidato a la autoría de Bitcoin.

Craig Wright

El afán de este científico computacional y empresario australiano por declarar en público que él era Satoshi Nakamoto, sin demostrar pruebas sólidas de ello, le restan credibilidad a sus afirmaciones, pues, además, este tipo de actitudes se contradicen con la ideología cypherpunk de la que fue originaria esta criptomoneda. Un hacker que supuestamente logró infiltrarse en las cuentas de correo de Wright demostró que, en ellas, se afirmaba que Satoshi Nakamoto era, en realidad, un seudónimo conjunto, donde también se incluía al analista computacional forense Dave Kleiman.

Dorian Nakamoto

En 2014, la revista *Newsweek* publicó un artículo en el que lo apuntaba como el creador de Bitcoin basándose en las conclusiones derivadas de una entrevista con la periodista Leah McGrath Goodman y en ciertas pruebas no muy concluyentes, donde el sospechoso afirmó dudosamente haber trabajado en el proyecto Bitcoin. Aunque Dorian sea el candidato más conocido, quizás también sea el menos probable

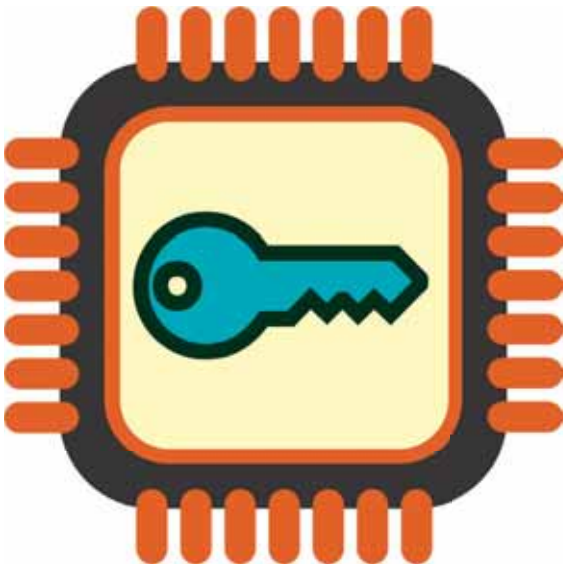
En agosto de 2008, el dominio *bitcoin.org* fue registrado y, en octubre de ese mismo año, se dio a conocer el primer trabajo de Satoshi Nakamoto. Se trataba de un *White Paper* (libro blanco) que fue publicado en metzdowd.com y que tenía por título

Un *ataque del 51% podría faslsear la cadena de bloques.* Fuente: Aaron Olson en Pixabay.

en la arquitectura de los criptoactivos. Sin embargo, se pueden realizar cambios en el proceso de generación de bloques y de confirmación de las transacciones para solucionar el problema, por ejemplo, implementado el método de consenso de prueba de participación por el de prueba de trabajo. Esto quiere decir que la probabilidad de generar un bloque no se ve ahora afectada por el poder de cómputo disponible, sino por el número de criptoactivos con los que cuente el minero. En esta situación, para generar el 51% o más de las criptomonedas, el minero debe disponer de al menos esa cantidad, lo que dificultaría, por ello, el ataque.

Un ejemplo del ataque del 51% lo sufrió la criptomoneda Ethereum Classic (ETC), la cual se desarrolló desde el 5 al 7 de enero de 2019 con el robo de 219000 ETC a través del doble gasto de las criptomonedas. La cadena se reorganizó varias veces, al igual que su sistema de prueba de trabajo (PoW), para paliar la situación, pero fue insuficiente para proteger la criptomoneda, ya que el problema radicaba en que tenía un poder de computación muy bajo (*hashrate*), esto provocó que fuera una presa fácil para un ataque de esta naturaleza. Los atacantes llegaron a concentrar más del 58% del poder de computación total de la red. Recordemos que un ataque del 51% implica controlar más del 50% del poder de procesamiento de una cadena de bloques para poder cambiar el historial de las transacciones o evitar que se confirmen las mismas.

En el caso de la red Ethereum Classic (ETC), la modificación se consiguió a partir de que el atacante obtuviera la mayor cantidad de poder de procesamiento durante la ejecución de la prueba



La llave pública y la privada dan funcionalidad a lo monederos de criptomonedas. Fuente: de OpenClipart-Vectors en Pixabay.

verificar que esa firma es la auténtica. El sistema debe seguir los siguientes pasos para lograr completar ese proceso:

1. Por parte de Adriana, se toman los datos de la transacción y se utiliza el algoritmo SHA-256 (que es el empleado en Bitcoin) para cifrarlos en un hash (huella digital de un documento o información) de sesenta y cuatro caracteres.
2. El hash obtenido se firma con la llave privada de Adriana, dando como resultado dos números conocidos, y con un peso variable de entre setenta y un y setenta y tres bytes. Para que nos entendamos, esa es la firma digital.
3. Entonces, se envían a Ismael los datos de la transacción, la clave pública de Adriana y la firma digital.
4. Empleando la llave pública de Adriana, el sistema por parte de Ismael podrá descifrar la firma digital para poder obtener el hash de sesenta y cuatro caracteres correspondiente a los datos de la transacción, que previamente Adriana había cifrado con SHA-256 y combinado con su llave privada.
5. Como los datos de la transacción también fueron recibidos por Ismael, el sistema repite el proceso de cifrarlos con SHA-256 para conseguir el hash correspondiente.
6. Se verifica que los hashes de los pasos 4 y 5 sean idénticos. Si no lo son, esto indicaría que alguien modificó los datos o la clave pública. Por tanto, la transacción se invalidaría, ya que fue cambiada durante su tránsito o no corresponde al propietario de los fondos.

III.

Taxonomía de los criptoactivos

21

¿Las aplicaciones descentralizadas originan criptoactivos?

Las Dapps o aplicaciones descentralizadas se perfilan como un nuevo y alternativo modelo de la web que conocemos, siendo los criptoactivos un ejemplo de estas. Criptomonedas como Bitcoin han demostrado que son económicamente viables y tecnológicamente factibles.

El internet de la información está dominado en la actualidad por grandes plataformas tecnológicas multinacionales cuyas aplicaciones actúan oligopolísticamente en la red de manera centralizadora, tales como Google, Amazon, eBay, Airbnb, Twitter, Dropbox, Facebook, Apple, Uber o WhatsApp. Pero esta realidad podría cambiar en los próximos años gracias a tecnologías disruptivas descentralizadas como blockchain.

Las Dapps o aplicaciones descentralizadas son plataformas de software desarrolladas en código abierto e implementadas en una cadena de bloques descentralizada (no dependen de una entidad central), que funcionan según un protocolo o algoritmo de validación de bloques (prueba de trabajo o prueba de

Conjunto representativo de tokens digitales del criptomercado. Fuente: Ismael Santiago

Token de utilidad: estos tokens no están diseñados como inversión, sino que proporcionan a los usuarios acceso futuro a un producto o servicio. Este tipo de tokens permite a sus dueños acceder a diferentes servicios que ofrece una plataforma basada en una cadena de bloques. Se usan para dinamizar la microeconomía de un ecosistema blockchain, facilitando así el financiamiento de los proyectos mediante una oferta inicial de moneda o ICO.

Token de seguridad: estos tokens representan capital o deuda de la puesta en marcha de un proyecto empresarial, dando a sus propietarios el derecho de reclamar sus intereses de inversión. Puede ser el derecho a participar en una entidad legal para aportar capital, para obtener ganancias o para ser acreedor o prestamista.

En resumen, los tokens son un elemento esencial para la nueva economía blockchain (NEB). La principal diferencia entre estos dos términos, como hemos explicado detalladamente antes, es que, mientras que las criptomonedas funcionan en una cadena de bloques propia e independiente, los tokens son creados sobre blockchains ya existentes, además de que no son minables.

Altcoins son criptomonedas que se construyen mediante el código fuente de bitcoin. Fuente: WorldSpectrum en Pixabay.

propias criptomonedas. Las altcoins pretenden aprovechar el éxito de bitcoin. Las razones por las cuales las personas invierten en criptomonedas alternativas a bitcoin son las siguientes: creen realmente que las nuevas criptomonedas poseen una solución efectiva para un determinado problema existente; ciertos inversores creen que determinas criptomonedas alternativas podrán cosechar un éxito similar a bitcoin, la cual llegó a rozar su máximo valor (de 20 000 dólares por unidad) y también se piensa que algunas criptomonedas pueden ser minadas de forma más sencilla y rentable que bitcoin actualmente.

Sin embargo, no todas las altcoins consiguen cumplir con sus propósitos ni el de sus inversores cuando lanzan su mecanismo propio de captación de financiación, denominado ICO, basado en el crowdfunding en el que un proyecto basado en blockchain, nuestra altcoin, vende una serie de criptomonedas propias del proyecto a los primeros usuarios a cambio de otras criptomonedas ya asentadas y conocidas en el mercado (bitcoin, ethers, por ejemplo). Para que nos entendamos, el funcionamiento de una ICO es muy similar a una IPO (oferta pública de ventas de acciones, en español) en los mercados bursátiles, donde las empresas salen al mercado a captar capitales de inversores interesados en tener una parte de esas compañías. En el caso de una ICO, no se venden acciones, sino criptoactivos, lo cual también sirve para financiar el crecimiento de la plataforma de blockchain. Otra diferencia que podemos encontrar entre una ICO y una IPO es que, en

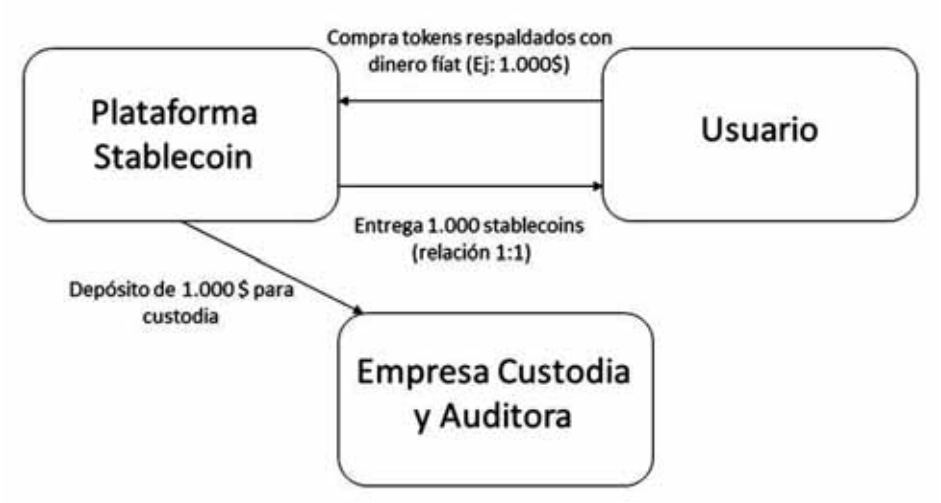
Stablecoins y Facebook serán protagonistas de la batalla a *librar* en el criptomercado. Fuente: Ismael Santiago

Libra estará apoyada por una reserva real y podrá cambiarse por otras monedas reales basado en una tasa estable de cambio. La Asociación de Libra ha fijado el valor de la moneda en un dólar estadounidense por unidad, pudiendo fluctuar dentro de una banda estrecha.

Libra se diseñó para ser una criptomoneda digital estable, completamente respaldada por una reserva de activos reales (la Reserva de Libra) y por una red competitiva de plataformas de cambio que compren y vendan Libra. Esto significa que cualquiera que posea Libra tendrá un alto grado de seguridad de poder convertir su moneda digital en moneda fiat local con base en una tasa de cambio, tal como cuando, al viajar, cambia una divisa por otra.

Para hacer realidad la misión de Libra, una moneda y una infraestructura financiera de naturaleza sencilla y global que empodere a miles de millones de personas, Blockchain de Libra y la Reserva de Libra requieren de una entidad de gobernanza conformada por miembros diversos e independientes. Esta entidad de gobierno es la Asociación Libra, una organización de miembros independiente y sin fines de lucro, con oficinas generales en Ginebra, Suiza. Inicialmente contó con 28 grandes empresas entre las que se incluyen Uber, Spotify, Vodafone, Visa, Martercard, eBay, Coinbase o PayPal.

La Asociación Libra es también la entidad que administrará la Reserva de Libra y que, por ende, permitirá alcanzar estabilidad y crecimiento a la economía de Libra. La asociación es la única parte habilitada para crear (acuñar) y destruir (quemar) Libra. Esta



Esquema de funcionamiento de un stablecoin anclada al dólar estadounidense

sirve de garantía a los tokens digitales. Además, puede generar un problema de liquidez, porque se necesiten grandes cantidades de capital como respaldo si se aspira a acuñar suficientes tokens para conseguir una adopción masiva.

Dentro de esta clasificación, se incluyen Tether, TrueUSD, Gemini Dollar, Paxos Standard y USD Coin.

A continuación, procedemos a describir el funcionamiento de cada una de estas.

Tether: Tether (USDT) es la moneda estable de mayor capitalización del mercado, además de ser el ejemplo más conocido. El proyecto fue fundado en noviembre de 2014 y tiene dos tokens: USDT y EURT, análogos al dólar y al euro. Las criptomonedas están conectadas con la casa de cambio Bitfinex. Para estos dos tokens digitales citados, se ha empleado el estándar ERC20 de la blockchain de Ethereum.

Este proyecto empresarial ha sido objeto de cuestionamientos al no ofrecer información clara sobre la entidad auditora y de custodia de las reservas de monedas fíat que sirven de garantía a los tokens digitales emitidos; incluso algunos de sus críticos han llegado a manifestar que no hay suficientes garantías. La emisión, entre noviembre de 2017 y enero de 2018, de casi 1800 millones de USDT sin que se hayan auditado sus reservas generó dudas sobre su validez. En mayo de 2019, de acuerdo con una declaración jurada presentada ante el Tribunal Supremo del Estado de Nueva York, solo el 74 por ciento de las tenencias de Tether

IV

Los modelos de negocio de las criptomonedas

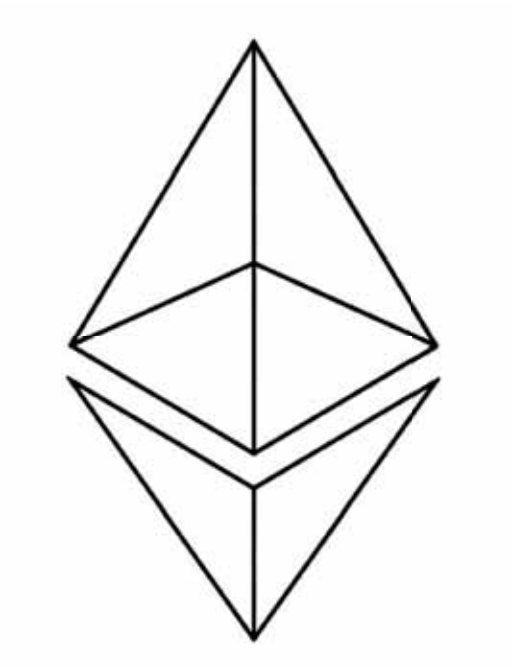
31

¿Bitcoin competirá contra el euro y al dólar estadounidense?

En 2009, fue presentado Bitcoin por primera vez como un software de código abierto por un programador anónimo, o un grupo de programadores, bajo el seudónimo de Satoshi Nakamoto. Posteriormente, su desarrollo fue liderado por otros expertos del equipo inicial, denominado Bitcoin Core.

El propósito de Satoshi Nakamoto al crear Bitcoin fue la independencia de una red de pagos descentralizada frente a cualquier autoridad central. La red de Bitcoin procesa los pagos de manera casi instantánea. Normalmente, se necesitan aproximadamente diez minutos de media para que alguien del otro lado del mundo reciba los bitcóins, mientras que las transferencias bancarias normales pueden demorarse varios días.

Actualmente, las entidades financieras conocen prácticamente todo sobre sus clientes: direcciones, números de teléfono, hábitos de consumo, historial de créditos e ingresos, etc. Todo es muy diferente con bitcoin, ya que la billetera no tiene que estar vinculada a ninguna información de identificación personal. En el caso



El ether es el primer altcoin y la segunda criptomoneda en capitalización de mercado. Fuente: lbokel en Pixabay

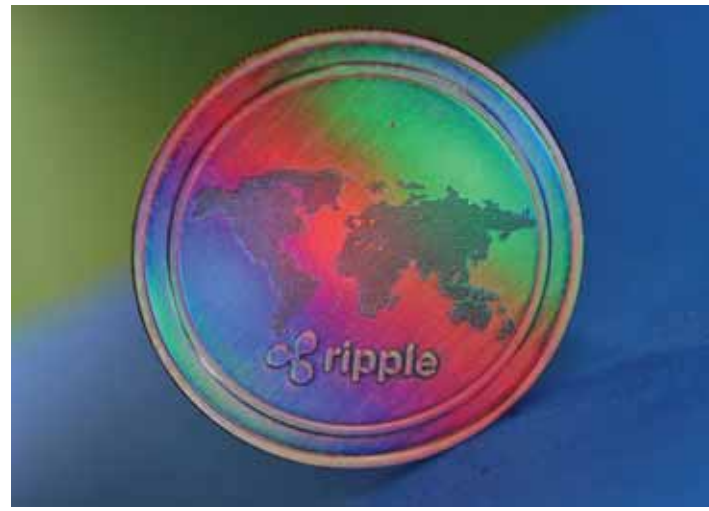
su red, además de ser un modo inversión para aquellas personas interesadas en su tecnología y evolución. Sus principales características son:

- Descentralización. No hay autoridad central que las controle.
- Anonimato. Ya que las direcciones para enviarlas y recibirlas son series numéricas aleatorias.
- Rapidez y seguridad para realizar transacciones directas, superando con ello al dinero fiat.

Ether es la criptomoneda de Ethereum, el combustible que impulsa esta plataforma de aplicaciones distribuidas. Ether es el incentivo que asegura que los desarrolladores escriban aplicaciones de calidad y que la red permanezca saludable y segura.

La oferta total de ethers y su tasa de emisión fue decidida en la preventa de 2014. La emisión está limitada a dieciocho millones de ethers por año (una tasa del 25% de la oferta inicial). Aunque se espera que esta varíe, ya que Ethereum tenía decidido cambiar su esquema de minado de prueba de trabajo (PoW) a prueba de participación (PoS) bajo la denominación Casper. La fecha de lanzamiento ha sido pospuesta varias veces.

En Ethereum, la recompensa por bloque, al principio, fue de cinco ethers por bloque, pero, con la introducción de una versión mejorada denominada Byzantium, se vio reducido a tres ethers por bloque. En el futuro, la recompensa dependerá directamente



Ripple permite realizar transacciones transfronterizas más rápidas y económicas que *SWIFT.* Fuente: Miloslav Hamřík en Pixabay.

descentralizada denominada Distributed Ledger Technology (DLT).

Ripple pretende agilizar el sector financiero de pagos transfronterizos, donde las cosas se han mantenido relativamente estables durante muchos años. En una época actual basada en la digitalización y la instantaneidad de la prestación de los servicios, donde podemos realizar innumerables actividades con nuestros *smartphones*, no podemos realizar con ellos transferencias internacionales de forma rápida y económica.

Por ejemplo, si alguien ha intentado recibir o enviar una transferencia a otro país, se habrá dado cuenta de las enormes comisiones que obtienen los intermediarios financieros, ya sean bancos o el propio servicio PayPal, sin olvidarnos de la problemática que supone el intentar sacar nuestros fondos bancarios en algunos países. Estas prácticas bancarias les han reportado durante muchos años enormes beneficios, con el respectivo sufrimiento aparejado de sus clientes. Esta circunstancia podría cambiar con Ripple, que promete transacciones internacionales instantáneas y a un coste extremadamente bajo.

Actualmente, los bancos e instituciones financieras utilizan un servicio propuesto por la organización llamada Society for Worldwide Interbank Financial Telecommunication (SWIFT) para poder realizar las transacciones transfronterizas de forma segura, que, para entendernos, es una red de mensajería que transmite órdenes de pagos de forma segura entre bancos. Con cerca de 10000 miembros, SWIFT hace posible el envío de veinticuatro millones de mensajes por su red diariamente. Y, además, en ningún momento SWIFT gestiona el dinero físico o mantiene cuentas. Se

V

Los fundamentos tecnológicos de la nueva economía blockchain

41

¿En qué consiste blockchain y cuáles son sus propiedades?

Actualmente, estamos acostumbrados a compartir información a través de internet. Pero, cuando se trata de transferir valor (derechos de propiedad, dinero o propiedad intelectual), habitualmente recurrimos a tradicionales entidades centralizadas, como lo son la banca y el Estado. La tecnología blockchain ofrece la sólida posibilidad de eliminar a estos intermediarios, y lo hace al registrar transacciones y al establecer identidades y contratos.

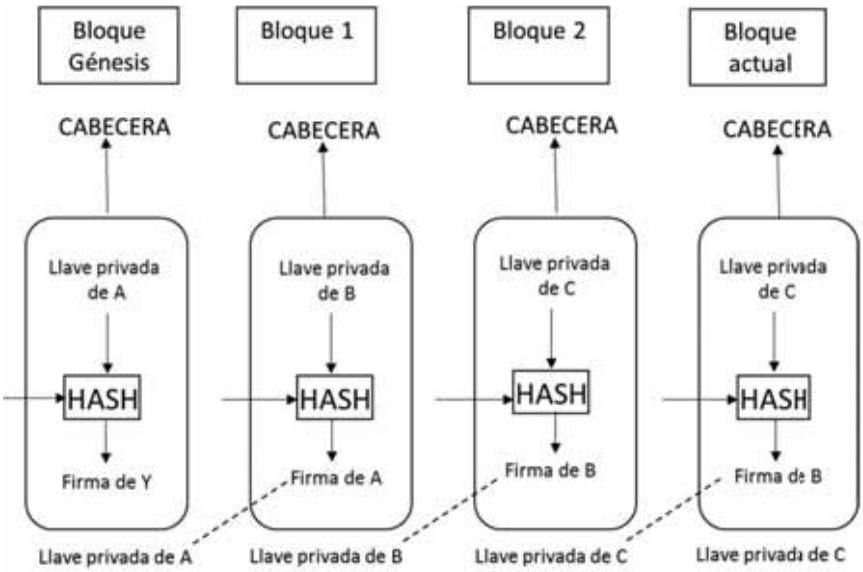
Una blockchain es una base de datos basada en la tecnología de contabilidad distribuida y que está protegida criptográficamente, organizada en bloques de transacciones relacionados entre sí matemáticamente utilizando la criptografía y que se halla distribuida entre diferentes participantes, lo que significa que una copia de la misma estructura de información es alojada y mantenida por muchos dispositivos que no están sujetos a ningún control central. Esta base de datos soporta una lista creciente de registros ordenados llamados bloques. Cada bloque tiene una marca de tiempo y un vínculo con el bloque que le antecede. Resumiendo,

Propiedades de la cadena de bloques. Fuente: Darwin Laganzon de Pixabay.

exitosos, tenemos a Bitcoin y Ethereum, entre otros. El beneficio de la nueva estructura económica descentralizada que promete la nueva economía blockchain lo encontramos en los protocolos, los cuales serán los encargados de canalizar el internet del valor.

Descentralización: se trata de un sistema que permite que usuarios que no confían (ni tienen por qué) plenamente entre ellos puedan mantener un consenso sobre la existencia, el estado y la evolución de una serie de elementos compartidos. El consenso es precisamente la clave de un sistema blockchain porque es el fundamento que permite que todos los participantes en el mismo puedan confiar en la información que se encuentra grabada en él. Este sistema basado en la confianza y el consenso se crea a partir de una red global de ordenadores que administran una enorme base de datos. Cada vez que se alcanza un consenso, una transacción se registra en un bloque, que es un espacio de almacenamiento. La cadena de bloques realiza un seguimiento de estas transacciones que pueden verificarse posteriormente como realizadas. La cadena de bloques puede estar abierta a la participación de cualquiera que lo desee (blockchain pública) o bien limitada a solo ciertos usuarios (blockchain privada), aunque siempre sin la necesidad de que exista una entidad central que supervise o valide los procesos que se lleven a cabo.

Contabilidad pública distribuida: la tecnología de la cadena de bloques es un registro público y distribuido de transacciones, con una marca de tiempo que permite el seguimiento de dichas transacciones procesadas en su red, donde cada usuario verifica la validez de cada una de estas, lo que evita el doble gasto. Los registros de



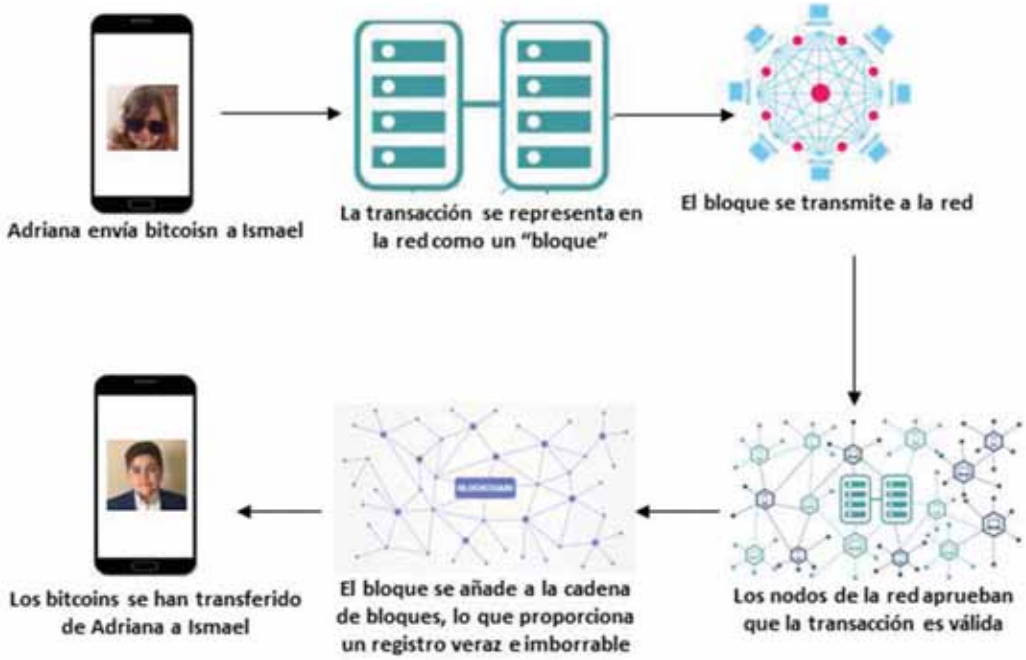
ESTRUCTURA DE BLOCKCHAIN

agrupados en pares y generan un nuevo hash que, a su vez, se agrupa con otro y se repite el proceso hasta alcanzar un único bloque, la raíz del árbol, que se denomina apuntador hash raíz (*root hash*) y se registra en la dirección del bloque actual (*block hash*) con el fin de disminuir el espacio ocupado por cada bloque. El nonce, por su parte, se refiera a un valor que solamente puede ser usado una vez. Este número único o nonce es un número aleatorio emitido por los mineros mediante la prueba de trabajo (PoW) que sirve para autenticar el bloque actual y evitar que la información sea reutilizada o modificada.

43

¿Con cuántos tipos de blockchain nos podemos encontrar?

Podemos clasificar los distintos tipos de blockchain en función del acceso a los datos o a los permisos; principalmente son públicas y privadas. Las blockchain públicas son aquellas en las que no hay restricciones para participar, tanto en la lectura como en la escritura de sus datos. La blockchain es pública si cualquier usuario puede participar en ella libremente, de ahí que se la llame también



CÓMO FUNCIONA BLOCKCHAIN

Un nodo es un ordenador conectado a la red que emplea un programa informático para almacenar y distribuir una copia actualizada, en tiempo real, de la blockchain. Las transacciones se realizan desde monederos electrónicos o *wallets*, los cuales consisten en archivos encriptados que funcionan de forma similar a una cuenta bancaria. Un monedero electrónico es un conjunto de clave pública y privada controladas por un software. La clave pública es una cadena alfanumérica de treinta y cuatro caracteres de longitud que componen lo que se conoce como un hash criptográfico. Esta es la dirección de Bitcoin, que hace las veces de número de cuenta. De esta forma, para que un usuario envíe bitcóins a otro y los reciba, previamente debe haberle dado la clave pública.

La clave privada es una cadena de sesenta y cuatro caracteres de longitud que prueba que eres el dueño de la clave pública. Además, es necesaria para decirle a la red que estas enviando bitcóins a otro monedero. Esta clave sirve para autorizar transacciones desde el monedero electrónico, para lo que se emplea en todo este proceso la criptografía asimétrica.

Un bloque es un conjunto de transacciones confirmadas. Cada bloque es una parte de la cadena con los siguientes elementos básicos: un código alfanumérico que enlaza con el bloque anterior, un conjunto de transacciones y otro código alfanumérico que

VI

Ejemplos del impacto de la nueva economía blockchain en diversos sectores económicos

51

¿Cuándo hace la unión la fuerza para el sector bancario gracias a blockchain?

La digitalización de la banca es uno de los principales retos de este sector financiero, que busca nuevas formas de rentabilidad en un entorno histórico de bajos tipos de interés. La banca busca aplicaciones tecnológicas con las que lograr que sus procesos sean más ágiles, más eficientes y también más económicos. El sector bancario ha invertido y sigue invirtiendo importantes sumas de dinero en tecnologías que pueden afectar disruptivamente a su actual modelo de negocio. Una de ellas es, sin duda, la tecnología de cadena de bloques (fundamentalmente privada), que promete mejorar considerablemente los actuales procedimientos de la banca mediante la desintermediación y el ahorro de numerosos costes operacionales.

En los últimos años, el comportamiento en los mercados del sector bancario ha experimentado importantes cambios en un entorno de extrema incertidumbre, con una importante presión regulatoria y con unas muy bajas rentabilidades obtenidas,

La contribución de blockchain a la seguridad aérea está siendo incuestionable en el sector de las aerolíneas. Fuente: Robert Waghorn en Pixabay.

de usos de blockchain y tecnologías emergentes en el ecosistema de los viajes y de la aviación para así disponer de información vital para descubrir la falla de cualquier siniestro y evitar con ello nuevos accidentes. Se analizan, por ejemplo, los datos de entrada y salida del ventilador del motor del avión: el lugar donde fue instalado, la persona que lo instaló, la fecha de emisión e instalación y la hora en que se realizó esta actividad.

La consultora de negocios y tecnología Capco realizó un informe para la Asociación Internacional de Transporte Aéreo (IATA), el cual mostraba que la cadena de bloques puede hacer que la industria sea más rápida y rentable, mejorar la experiencia del cliente y el valor de la industria. En otro estudio realizado por la firma internacional Accenture, se mostraban los beneficios de implementar la tecnología blockchain en la aviación comercial, como los que se consiguen en el almacenamiento e intercambio de datos, para así alcanzar la mayor integridad de los procesos, que son fundamentales para mejorar la seguridad del vuelo, el servicio y la experiencia del usuario, además para de abaratar los costes. Para esta firma, la tecnología de cadena de bloques puede terminar integrándose en todos los sectores de la industria de viajes y sus entidades intervinientes, desde el alquiler de automóviles o la inmigración hasta los hoteles y las agencias de viaje en línea, pues, en algún momento, todos necesitan información sobre el pasajero y tienen diferentes exigencias que pueden ser satisfechas plenamente implementando esta tecnología

Logotipo de Olivacoin.
Fuente: Ismael Santiago.

ahora, eran mercados de margen, como Estados Unidos, Reino Unido, Alemania u Holanda. Esta situación ha llevado al sector a una situación económica límite donde más del 90% de los ingresos de explotación que genera equivalen a la compra de aceituna y otros costes de aprovisionamiento, con lo que un gran número de pequeñas empresas olivareras y almazaras productoras se plantean el cerrar si no cambian las actuales circunstancias.

Este es el motivo principal del nacimiento y desarrollo del proyecto de Olivacoin como plataforma digital descentralizada basado en la diferenciación de la trazabilidad veraz del aceite de oliva. Olivacoin pretende convertirse en un mercado digital para la compraventa de aceite de oliva a granel a nivel B2B para los operadores del sector, que permitirá una mayor agilidad, rentabilidad, liquidez y desintermediación gracias a la integración que sufrirá la cadena de suministro del sector gracias a esta tecnología, disponiendo además de una blockchain propia y de una tecnología basada en internet de las cosas (IoT), concretada en un sistema experimental analítico de trazabilidad para el aceite de oliva que permitiría comprobar en destino la calidad.

Lo que impulsó el desarrollo de Olivacoin fue encontrar una alternativa innovadora a la desaparición del Mercado de Futuros del Aceite de Oliva (MFAO), que se produjo principalmente por las estrictas exigencias de adaptación y requerimientos normativos y económicos demandados por la reglamentación comunitaria y

Valoración Financiera del Sector del Aceite de Oliva

Balance de situación	Sector Aceite
Inmovilizado	**1,296,961,224.59 €**
Inmovilizado inmaterial	242,145,587.65 €
Inmovilizado material	240,159,087.96 €
Otros activos fijos	814,656,548.98 €
Activo circulante	**1,230,854,751.42 €**
Existencias	359,606,422.83 €
Deudores	437,774,718.91 €
Otros activos líquidos	433,473,609.68 €
Total activo	**2,527,815,976.01 €**
Fondos propios	**600,169,860.47 €**
Capital suscrito	634,924,654.03 €
Otros fondos propios	- 34,754,793.56 €
Pasivo fijo	**811,759,630.27 €**
Pasivo no corriente	752,999,940.02 €
Otros pasivos no corrientes	58,759,690.25 €
Provisiones	- €
Pasivo líquido	**1,115,886,485.26 €**
Deudas financieras	232,674,138.92 €
Acreedores comerciales	243,354,604.56 €
Otros pasivos líquidos	639,857,741.78 €
Total pasivo y capital pro	2,527,815,976.00 €

Cuenta de Pérdidas y Ganancias	Sector Aceite
Ingresos de explotación	3,961,694,081.56 €
Importe neto Cifra de Ventas	3,961,085,204.61 €
Otros Ingresos Explot	- €
TRPPI	608,876.95 €
Consumo de mercaderías y de materias	3,651,550,622.31 €
Gasto de Personal	90,523,349.30 €
Otros gastos de explotación	214,518,899.21 €
EBITDA	**4,492,333.80 €**
CAT	44,009,883.78 €
BAIT	**- 38,908,673.03 €**
Ingresos financieros	29,395,324.66 €
Gastos financieros	154,233,667.66 €
Resultado financiero	**- 124,838,343.00 €**
Result. ordinarios antes Impuestos	**- 163,747,016.03 €**
Impuestos sobre sociedades	
Resultado Actividades Ordinarias	**- 163,747,016.03 €**
Ingresos extraordinarios	- €
Gastos extraordinarios	- €
Resultados actividades extraordinarias	
Resultado del Ejercicio	**- 163,747,016.03 €**

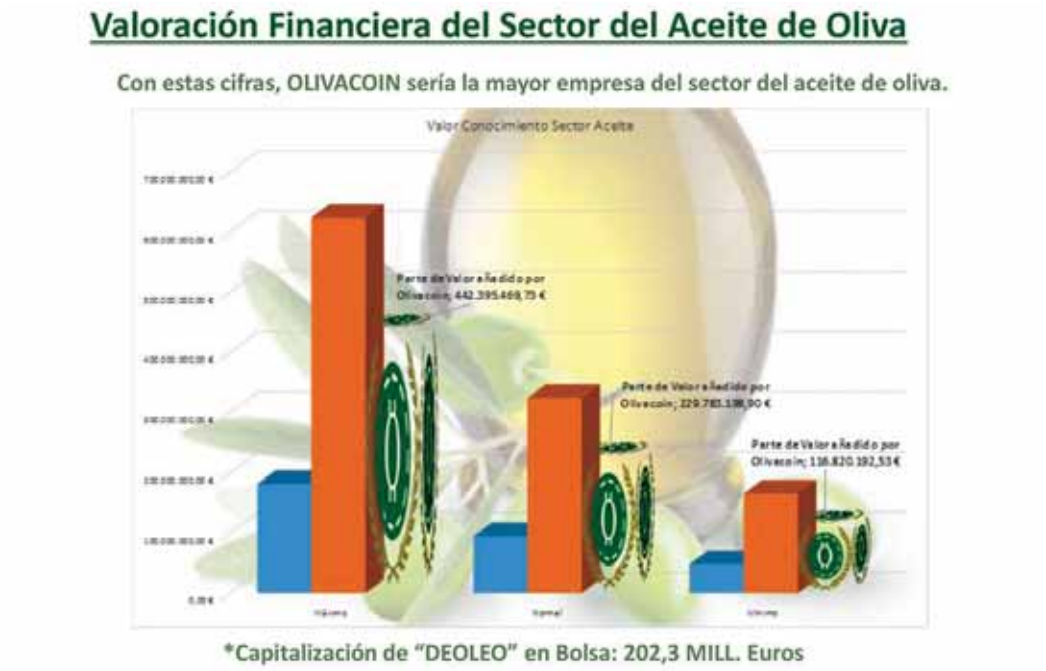
Escenarios de valoración económica del sector del aceite de oliva y de la tecnología Olivacoin. Fuente: Elaboración propia.

Valoración Financiera del Sector del Aceite de Oliva

	Riesgo	Valor Sector Aceite	Escenario con Olivacoin
	0.25%	101,423,935,437.44 €	8,113,914,835.00 €
	1.25%	20,283,849,543.76 €	1,622,707,963.50 €
	2.25%	11,267,661,833.34 €	901,412,946.67 €
Máximo	3.25%	7,799,521,677.02 €	623,961,734.16 €
	4.25%	5,963,198,251.31 €	477,055,860.11 €
	5.25%	4,826,252,501.42 €	386,100,200.11 €
Elegido	**6.25%**	**4,053,003,989.35 €**	**324,240,319.15 €**
	7.25%	3,492,973,430.62 €	279,437,874.45 €
	8.25%	3,068,639,731.41 €	245,491,178.51 €
	9.25%	2,736,003,257.32 €	218,880,260.59 €
	10.25%	2,468,234,006.25 €	197,458,720.50 €
	11.25%	2,248,040,746.20 €	179,843,259.70 €
Mínimo	12.25%	2,063,777,710.34 €	165,102,216.83 €
	13.25%	1,907,314,291.64 €	152,585,143.33 €

	Escenario sin OlivaCoin	Escenario con OlivaCoin	Valor añadido por Olivacoin
	2,359,995,990.73 €	8,113,914,835.00 €	5,753,918,844.26 €
	472,009,134.25 €	1,622,707,963.50 €	1,150,698,829.26 €
	262,240,668.26 €	901,412,946.67 €	639,172,278.40 €
Máximo	181,566,264.43 €	623,961,734.16 €	442,395,469.73 €
Normal	**94,457,120.25 €**	**324,240,319.15 €**	229,783,198.90 €
Mínimo	48,282,024.30 €	165,102,216.83 €	116,820,192.53 €
	44,657,368.46 €	152,585,143.33 €	107,927,774.87 €

Escenarios de valoración económica de los intangibles del sector del aceite de oliva y de Olivacoin. Fuente: Elaboración propia.



Represantación gráfica de los escenarios optimista, neutral y pesimista de la valoración económica de los intangibles del sector del aceite de oliva y de la tecnología Olivacoin. Fuente: Elaboración propia.

aprovisionamiento en relación con las ventas provocaría un aumento en el valor del conocimiento de 229 783 198 euros.

Gran parte de este aumento en el valor se debería fundamentalmente a las prestaciones propias que ofrece la tecnología de cadena de bloques de Olivacoin: desintermediación, integración de los agentes de la cadena de suministro del aceite de oliva, reducción considerable de costes (tanto financieros como no financieros), veracidad de unos datos incorruptibles, mejora de la confianza entre los agentes intervinientes gracias a la tecnología de la cadena de bloques y las muy diversas aplicaciones de los contratos inteligentes (confianza descentralizada garantizada, transparencia, cámara de compensación, autoejecución y autoliquidación en tiempo real, etc.). Esto llevó a una conclusión que trajo consigo muchos titulares de prensa tanto nacionales como internacionales: Olivacoin uberizaría el sector (término empleado por la empresa UBER) y se podría llegar a convertir en la mayor empresa del sector del aceite de oliva gracias a la tecnología blockchain, ya que su posible valor de 229 783 198 euros superaría la capitalización de mercado de la mayor empresa cotizada del sector por aquel entonces: Deoleo.

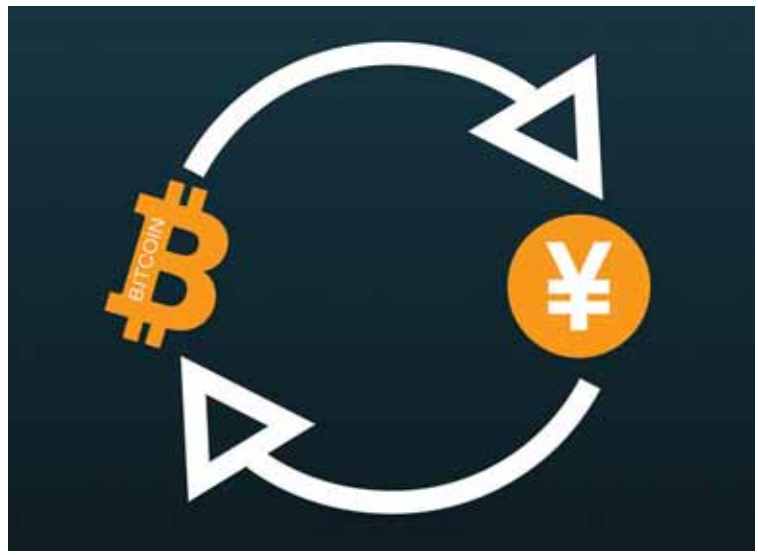
VII

Las nuevas b-finanzas y su regulación

61

¿Forzarán las nuevas empresas fintech un cambio radical en la banca que conocemos?

La evolución de la innovación tecnológica y su respectivo impacto en la economía y en la sociedad hace que aparezcan diariamente nuevos conceptos que son difíciles de entender y términos como criptomonedas, token, blockchain o *fintech*, entre otros. Si nos centramos en este último término citado, nos damos cuenta de que es un concepto actualmente muy en boga en el sector financiero —y estimamos que lo seguirá siendo en los próximos años—. El término *fintech* se explica como la contracción de las palabras inglesas *finance* y *technology* (en español, 'sector tecnofinanciero' o 'tecnofinanzas'). El sector tecnofinanciero es considerado una nueva industria financiera que aplica la tecnología para mejorar las actividades financieras. Este sector corresponde a aquel segmento de empresas cuya actividad económica está basada en la tecnología y que ofrece productos o servicios financieros alternativos y al margen de las grandes entidades bancarias tradicionales. Este tipo de empresas, orientado al sector financiero se caracteriza por desempeñar su actividad de forma muy ágil, eficiente, instantánea



Los exchanges permiten el intercambio de criptoactivos de forma transparente. Fuente: Parveender Lamba en Pixabay.

general, como lo hacen las ICO. Como los lanzamientos se hacen desde casas de cambio o exchanges, quienes deseen invertir en los proyectos deben identificarse y cumplir con los procedimientos de conocimiento de cliente o Know Your Customer (KYC) y de prevención de blanqueo de capitales o Anti-Money Laundering (AML) que cumplen estas plataformas. A partir del depósito de criptoactivos, el sistema de financiación se activa por parte de los inversionistas mediante sus carteras, las cuales están habilitadas en la plataforma. Desde sus cuentas en la casa de cambio, los aportantes autorizan el empleo de los fondos para la adquisición de los tokens del proyecto empresarial que se vaya a lanzar.

El desarrollo de las IEO es muy similar a las ICO, con la salvedad de que son tuteladas por una *exchange* o casa de cambio. De todas maneras, el proceso genera una serie de cambios en el desarrollo del proyecto que marca algunas diferenciaciones con respecto a lo que son las ICO. En las ICO, los desarrolladores administran los fondos, a diferencia de lo que pasa con las IEO, donde los fondos que se obtienen para financiar el proyecto empresarial son gestionados por la casa de cambio. Sobre la responsabilidad de la casa de cambio recae la evaluación de la viabilidad y la seriedad del proyecto; es ella la que decide apoyar el lanzamiento si considera que cumple con una serie de estándares que eviten los fraudes y que garanticen su desarrollo.

Las IEO sirven como mecanismo de seguridad ante las posibles estafas de criptomonedas, ya que son ejecutadas por las propias casas de cambio. Estas ofertas ayudan a mermar la incapacidad de algunos inversionistas para evaluar la calidad de las ICO y a

El blanqueo de capitales es uno de los principales problemas que encontramos en el criptomercado. Fuente: Gerd Altmann en Pixabay.

beneficiario final incluiría: con respecto a la persona física que abre la cuenta, nombre y cargo; con respecto a la persona jurídica, nombre y dirección; con respecto a los beneficiarios finales, nombre (y título de la persona o las personas que la controlan), fecha de nacimiento, dirección, número de seguridad social o número de pasaporte y país de emisión o número de identificación similar. En el caso de que no se tomaran las medidas adecuadas, las consecuencias difieren entre Estados Unidos y Europa. En Estados Unidos, su incumplimiento generaría grandes problemas. Concretamente, las sanciones en ese país norteamericano pueden llegar a multas de un millón de dólares y hasta treinta años de cárcel. En Europa, las sanciones máximas son de cinco millones de euros o del 10% de la facturación anual total de la organización. Aunque las leyes AML y KYC entraron en vigor hace años, las leyes sobre el beneficiario final son más recientes. En Estados Unidos, la norma final de CDD de FinCEN, que también cubre el beneficiario final, entró en vigor el 11 de mayo de 2018. En Europa, la cuarta directiva AML entró en vigor el 26 de junio de 2017 y contiene disposiciones sobre el beneficiario final.

VIII

Guía para invertir con éxito en el criptomercado

71

¿Dónde y cómo se pueden adquirir criptomonedas?

Nos vamos a centrar principalmente en dónde y cómo se pueden adquirir las dos principales criptomonedas que hay en el criptomercado; nos referimos al bitcoin y al ether de Ethereum. Antes de nada, necesitamos disponer de un monedero electrónico o *wallet* para poder almacenar las criptomonedas que vayamos a adquirir. Estos monederos tienen una variedad de formas que ofrecen distintas posibilidades de seguridad, acceso y almacenamiento. En el caso de bitcoin, los tipos principales que encontramos son: en línea, de escritorio, *hardware*, móvil y papel.

El concepto de *almacenar* no es literal en el ámbito de los criptoactivos, ya que, nos referimos a un *software* que permite la disponibilidad de un conjunto de llaves (pública y privada), del que la privada permite acceder a una dirección de Bitcoin y poder ejecutar, transferir y gastar los fondos. Esas llaves digitales se necesitan para llevar a cabo transacciones y, si el usuario pierde o le roban la llave privada, en esencia, pierde el acceso a sus bitcóins. En las transacciones con bitcoins, es fundamental mantener la

El autor dando ejemplo y comprando criptomonedas en un cajero Bitcoin.
Fuente: Ismael Santiago.

llave privada (comparable a un pin de cajero automático) como un secreto protegido y solo emplearla para autorizar transacciones con esta criptomoneda. El número de opciones para poder comprar bitcóins aumenta constantemente; por ejemplo, usando los cajeros de Bitcoin. Estos ofrecen a sus usuarios una experiencia de compra más privada. Los cajeros automáticos de Bitcoin aparecen en ciudades de todo el mundo y su número está en constante crecimiento. Las máquinas cobran una comisión del tres al ocho por ciento sobre el precio normal de cambio. Todo lo que necesita hacer un usuario es insertar efectivo en el cajero automático y escanear el código QR de su billetera móvil o recibir un recibo en papel con los códigos e instrucciones sobre cómo transferir los fondos a su monedero digital.

A medida que la criptomoneda bitcoin gana en popularidad, este tipo de cajeros automáticos tienen el potencial de convertirse en una de las formas más comunes de adquirir este tipo de criptomoneda. Para poder acceder al cajero automático Bitcoin más cercano, se puede utilizar un servicio de mapas como CoinATMRadar. En diciembre de 2018, el número de cajeros automáticos Bitcoin en España ascendió a setenta y seis tras haberse incorporado 40 durante ese mes, con lo España se sitúa en el quinto lugar entre los países con más cajeros de este tipo a nivel mundial. De acuerdo a los datos del sitio Coin ATM Radar, la mayoría

IX

La cuarta revolución industrial y la nueva economía blockchain

81

¿La cuarta revolución industrial necesita incorporar blockchain para su desarrollo?

La cuarta revolución industrial conlleva la transformación del ser humano debido a la convergencia tecnológica de los sistemas biológicos, digitales y físicos. Esto derivará en transformaciones en la forma en que trabajamos, nos relacionamos y vivimos. Esta nueva revolución nos está obligando a replantearnos cómo se desarrollan los países y cómo las compañías crean valor añadido.

Revolución industrial es la denominación historiográfica de los procesos de revolución tecnológica que se producen en la Edad Contemporánea protagonizados por los cambios en la industria. La primera revolución industrial se inició en el Reino Unido en la segunda mitad del siglo XVIII y se extendió a gran parte de Europa occidental y a la América angloparlante unas décadas después. Concluyó entre 1820 y 1840. Esta primera revolución industrial permitió pasar de una economía rural basada fundamentalmente en la agricultura y el comercio a otra economía de carácter urbano, industrializada y mecanizada gracias a novedades como el motor a vapor. La segunda revolución industrial

La cuarta revolución industrial ha llegado para quedarse al igual que blockchain. Fuente: Gerd Altmann en Pixabay.

La historia muestra que, una vez que las revoluciones industriales se ponen en funcionamiento, el cambio se produce con rapidez. Los emprendedores convierten los inventos en innovaciones comerciales, estas dan lugar a nuevas compañías que crecen aceleradamente y, por último, los consumidores demandan los nuevos productos y servicios que mejoran su bienestar y calidad de vida. Como ya describiría el economista Joseph Schumpeter, la labor del emprendedor es crítica en el papel que desempeña en la innovación, pues altera ciclos económicos y determina el aumento y la disminución de la prosperidad que genera con su actividad, mediante un proceso de transformación que acompaña a todas las innovaciones y que el autor denominó «destrucción creativa». Este último concepto está ligado a la denominada «disrupción tecnológica (o cambio súbito)», que se produce cuando hay convergencia de varias tecnologías y modelos de negocio que suponen un coste diez veces inferior a las soluciones ya existentes; es decir, que lo nuevo sustituye a lo antiguo o actual cuando es diez veces más baratos y mejora, lógicamente, las prestaciones existentes. Una vez que el engranaje de este proceso comienza a funcionar, la economía, la industria y la sociedad cambian a toda velocidad.

Los conceptos de la cuarta revolución industrial ya están integrados en las formas de actuar y pensar de los emprendedores dedicados a desarrollar nuevos tipos de servicios innovadores. Sus compañías son ágiles, colaborativas y adaptables a las circunstancias cambiantes del mercado y mejoran continuamente su

El e-commerce se beneficiará de la adopción paulatina de las criptomonedas como medios de pago en internet. Fuente: Tumisu en Pixabay.

una centralización en grandes plataformas mundiales como son Amazon y Alibaba, sus dos ejemplos paradigmáticos.

El tráfico que generan estas plataformas es de tal calibre que favorece también las ventas de las tiendas en línea afiliadas. Y, a la vez, esa dinámica tan favorable les proporciona el oxígeno necesario para mantener las visitas a Amazon o Alibaba en unos niveles muy altos. En Amazon, el consumidor sabe lo que puede esperar en términos de calidad del producto, política de devoluciones, servicio de atención al cliente, precio o entrega; un patrón que genera confianza e impulsa a los clientes a volver. Esta centralización y acumulación de poder implica que Amazon es capaz de añadir comisiones de distribución medias del 15% a los artículos vendidos. Si el trato entre fabricante y consumidor fuera directo, y no a través de un intermediario como es el caso, la supresión de estas comisiones supondría ahorros multimillonarios. No obstante, el comercio electrónico actual no está aprovechando la oportunidad que internet brinda de eliminar intermediarios, al contrario. La prueba es el desorbitado poder que están acumulando empresas como Amazon, que le permite prescribir la venta de productos de todo tipo, lo que a su vez frena el desarrollo de empresas, productos y negocios que sencillamente no cumplen los «filtros» impuestos por la compañía. Se trata de ventas que algunas empresas no pueden llegar a materializar y de productos que los consumidores no tendremos oportunidad de descubrir nunca si

Blockchain permite el cambio y el crecimiento económico en los actuales modelos de negocio. Fuente: Kai Kalhh en Pixabay.

que, en definitiva, facilita el surgimiento de nuevos modelos de negocios.

El estudio elaborado por IBM en más de 3000 altos ejecutivos de empresas de diferentes sectores en todo el mundo compara a aquellas organizaciones que ya están experimentando o implementando blockchain de manera activa (a las que denomina «exploradores») con aquellas que, en estos momentos, ni siquiera contemplan adoptar esta tecnología. El 33 % de las empresas ya están utilizando la tecnología blockchain o se plantean su uso en breve, y un 78 % de los que ya la están explorando lo hace como respuesta a los cambios que se producen en su sector o para desarrollar nuevos modelos de negocio. Entre las principales conclusiones del estudio destaca también el hecho de que el 100% de los denominados exploradores (es decir, aquellos que ya están experimentando o implementando blockchain) esperan que esta tecnología apoye de alguna forma su estrategia empresarial; y un 63% pretende utilizarla para conseguir una mayor transparencia en sus transacciones. Entre aquellos exploradores que afirmaron que su modelo de negocio está amenazado, más del 50% de ellos espera lanzar un modelo empresarial completamente nuevo en su sector o en cualquier otro. El 71% de aquellos que ya trabajan con blockchain de manera activa cree que las asociaciones industriales van a resultar clave en los nuevos desarrollos con esta tecnología.

Blockchain permite optimizar las funcionalidades prometidas por el internet de las cosas (IoT). Fuente: Gerd Altmann en Pixabay.

- *Reciclabilidad*: puede usarse muchas veces y para muchas cosas.
- *Innovación*: permite nuevos modelos de negocio para nuevas oportunidades.
- *Confianza*: asegura la integridad de los datos y la confiabilidad de los participantes.
- *Eficiencia*: minimiza los costes y maximiza la eficiencia.

Existen numerosos beneficios potenciales del IoT distribuido habilitado con blockchain en muchos niveles. El rediseño y la automatización de procesos en redes de igual a igual, en lugar de a través de personas o aplicaciones intermediarias centralizadas, podría traer numerosos beneficios, como ya se identificaron. Entre ellos están: la velocidad (automatización de extremo a extremo); los costos reducidos (asociados con el envío de cantidades casi infinitas de datos a instalaciones de procesamiento central gigantes; eliminación de intermediarios costosos); mayores ingresos, eficiencia o productividad (liberando el exceso de capacidad para su reutilización); mejora de la efectividad (las listas de verificación integradas y otros protocolos reducen el impacto del error humano); mayor seguridad e integridad (la confianza está diseñada en la arquitectura de la red); menor probabilidad de fallo del sistema (eliminación de cuellos de botella); la reducción del consumo de energía (energía requerida por la propia red compensada por una mayor eficiencia y menor desperdicio); mayor protección de la privacidad (el intermediario no puede anular o ignorar las reglas

X

El futuro de la economía y la sociedad en el contexto de la nueva economía blockchain

91

¿El nuevo internet del valor exigirá un nuevo sistema monetario internacional?

La irrupción del internet de la información ha cambiado radicalmente nuestras vidas. Empleamos diariamente plataformas centralizadoras de la información en nuestro quehacer diario como Google, Facebook o Amazon, las cuales monetizan la información de sus usuarios sin impunidad. Se trata de unos gigantes monopolizadores que han sido capaces de situarse a la cabeza de la economía mundial gracias a los datos. La nueva economía se construye sobre una red que nos conecta a todos; su valor más importante es lo que transmitimos a través de ella, y estas compañías lo han aprovechado para buscar su posición de liderazgo en el mercado.

Las revoluciones tardan tiempo en ser percibidas. Actualmente, nueve años después de la puesta en funcionamiento de la primera red de blockchain, hemos comprendido que lo que conocemos como cadena de bloques tiene que ver en realidad con un nuevo internet: el internet del valor. En lugar de información, en esta nueva red se transmiten títulos de propiedad de cosas, físicas o digitales. Blockchain tiene potencial para cambiar el mundo que

El Internet del valor permitirá la libre transferencia de la información y del valor económico. Fuente: Parveender Lamba en Pixabay.

como es blockchain. Este token también representa una unidad de valor que permite la gobernanza del modelo de negocio de una organización, dotando con ello de más poder a sus usuarios para interactuar con los productos y tecnología generados a la vez que facilita la distribución y el reparto de beneficios entre los socios de dicha entidad.

Los tokens digitales significan tres cosas: la representación digital del valor; que el control del token lo determinan las claves criptográficas, y que el registro de la propiedad del token radica en la cadena de bloques. La combinación de estas tres cosas da sentido a la tokenización, donde se concentra la capacidad de innovación disruptiva de blockchain. La tokenización es inherente a la representación digital del valor, siendo un proceso de conversión de los activos en tokens que se pueden almacenar, registrar e intercambiar en un sistema blockchain convirtiendo el valor almacenado de un activo tangible o intangible (una patente, una casa o un préstamo) en un token que puede manipularse a lo largo de dicho sistema de la cadena de bloques. La tokenización pretende abrir nuevos mercados autónomos en los que dotar de valor digital a productos y servicios aparentemente alejados de las nuevas tecnologías. Además, esta tiene muchas ventajas sobre los llamados mercados financieros tradicionales de capital en acciones, por ejemplo, en términos de innovación, velocidad, seguridad y responsabilidad.

La tecnología blockchain otorga nuevas *oportunidades económicas a los países en vías de desarrollo.* Fuente: stokpic en Pixabay.

no bancarizados, blockchain está generando una nueva forma de identidad financiera que no depende de la relación de una persona con un banco, sino que está enraizada en la propia reputación. En este nuevo paradigma, en lugar de pasar las pruebas de identificación tradicionales, los individuos pueden crear una identificación digital persistente y una reputación verificable y desplegarla en diferentes relaciones y transacciones. La tecnología de la cadena de bloques otorga confianza y acceso a servicios financieros para esta nueva identificación digital.

Todos los días, un inmigrante en algún lugar del primer mundo cobra su salario y se pone a la cola para enviar el 50% de su salario a su país de origen, para ayudar a su familia, que reside allí. En todo el mundo, 550 mil millones de dólares son transmitidos todos los años desde países del primer mundo en forma de remesas. Gran parte de ese dinero es enviado principalmente a cinco destinos: México, India, Filipinas, Indonesia y China. En algunos de estos lugares, estas remesas representan más del 40% de la economía local. Este importantísimo flujo de capital es gestionado por empresas como Western Union, que cobran, de media, una comisión del 9% de todas y cada una de esas transacciones a la gente más pobre y desfavorecida del planeta. ¿Qué pasaría si estos inmigrantes descubrieran que podrían enviar dinero a sus países de origen con criptomonedas como bitcoin no por un 20% ni

¿Será la deuda mundial impagable o la futura caída de un gran banco lo que provoque una nueva crisis económica? Fuente: Gerd Altmann en Pixabay

Estamos en una disyuntiva donde aún podemos decidir cómo queremos que continúe el actual siglo xxi. Podemos continuar con la senda de la centralización y la tiranía de los bancos centrales, que nos han llevado a la actual economía zombi, con unos bancos centrales y unas monedas únicas, impuestas y monopolísticas; o podemos elegir libremente la descentralización, la libertad y una democracia real de mercado escogiendo el dinero que queremos utilizar porque nos convencen sus virtudes y no porque nos obligan a utilizarla. El dinero fíat, controlado por los bancos centrales, requiere la confianza de todos los que lo utilizan. Confianza en que aquellos que lo controlan no se excederán en sus manipulaciones. Confianza en que los gobernantes cumplirán sus promesas y pagarán sus deudas (pero ya sabemos que la deuda mundial es impagable). Es muy posible que el sistema de dinero fíat, inaugurado por Nixon en 1971, termine mutando o acabe por derrumbarse definitivamente por la inasumible e impagable deuda global mundial. Hasta hace poco, las inversiones refugio se concentraban en metales preciosos como el oro y la plata; en la actualidad, podemos incluir en estas a bitcoin y a otros criptoactivos, sobre todo aquellos realmente más estables y que suelen responder al término *stablecoin*.

Glosario de primeros auxilios

Alastria blockchain: es un consorcio formado por más de setenta compañías para desarrollar el ecosistema blockchain en España. Es la primera red española multisectorial del mundo en blockchain.

Algoritmo: conjunto de pasos y métodos lógicos que, en una red informática, sus participantes deben seguir para ejecutar un comando o resolver un problema. En el ámbito blockchain se refiere a los métodos empleados por la minería para verificar transacciones. Algunos de ellos son SHA-256, CryptoNight y Scrypy.

Altura del bloque: cantidad de bloques que preceden a otro en una plataforma blockchain.

ASIC: el Circuito Integrado de Aplicación Específica (ASIC) es un chip diseñado para cumplir una tarea determinada. En el mundo de Bitcoin y las criptomonedas, es utilizado para resolver problemas de hashing y así generar nuevas criptomonedas, lo que se conoce como «minería de criptomonedas».

Ataque de 51 %: en teoría, un ataque informático que puede ser perpetrado por una entidad o grupo de minería que posee la mayoría del procesamiento de transacciones de la red blockchain (51 % o más) para prevenir que nuevas transacciones se confirmen.

Bibliografía recomendada

Mougayar, W. *La tecnología Blockchain en los negocios: perspectivas, práctica y aplicación en Internet*. Madrid: Anaya Multimedia, 2018.

En este libro trata con detalle el concepto de la cadena de bloques y su impacto en la actividad económica. Para el autor blockchain es una nueva capa tecnológica que reconfigura los protocolos sobre Internet y amenaza con sortear las antiguas estructuras heredadas y las empresas que funcionan de forma centralizada. En esencia, la cadena de bloques inyecta confianza en la red, dejando a un lado a algunos intermediarios que realizaban esa función y alterando creativamente su funcionamiento. Es una obra que ofrece un plan innovador que cubre el qué, el porqué y el cómo de la tecnología blockchain.

Saifedean, A. *El patrón Bitcoin: La alternativa descentralizada a los bancos centrales*. Barcelona: Deusto, 2018.

Para el autor de esta obra, la crisis financiera ha dejado un poso general de desconfianza en la sociedad. Todo lo que tiene que ver con el mundo financiero es visto con un recelo no siempre justificado y, en este caldo de cultivo, han nacido las llamadas criptomonedas. Partiendo de esta premisa, el

Bibliografía consultada

Alabi, K. «Digital blockchain networks appear to be following Metcalfe's Law». En: *Electronic commerce research and applications*, 2017;Vol. 24: 23-29.

Antonopoulos, A. *Internet del dinero*. Vol. 1. Madrid: Living Language, 2017.

—, *Mastering Bitcoin* (2.ª ed.). Sebastopol: O'Reilly Media Inc., 2017.

Arthur, B. Increasing returns and path dependence in the economy. Michigan: University of Michigan Press, 1994.

Botsman, R. *Who Can You Trust?* Londres: Penguin Books, 2017.

Brafman, O. y Beckstrom, R. *La araña y la estrella de mar.* Barcelona: Urano 2007.

Burniske, C. y Tatar, J. *Cryptoassets: the innovative investor's guide to Bitcoin and beyond*. Nueva York: McGraw-Hill Education, 2017.