CON DUMMIES ES MÁS FÁCIL

Criptomonedas

para dummies®

- Aprende a invertir en bitcoin y otras criptomonedas
- Entiende cómo funciona la tecnología blockchain
- Descubre las nuevas finanzas descentralizadas

Víctor Ronco
Carlos Callejo

Prólogo de **Álex Sicart**

Criptomonedas

para dummies®

Carlos Callejo
y Víctor Ronco

para dummies®

Edición publicada mediante acuerdo con Wiley Publishing Inc.
…For Dummies y los logos de Wiley Publishing, Inc. son marcas registradas utilizadas bajo licencia exclusiva de Wiley Publishing, Inc.

Grupo Planeta
Avda. Diagonal, 662-664
08034 - Barcelona

ISBN: 978-84-329-0592-6
Depósito legal: B. 3.637-2020

Primera edición: septiembre de 2020
Preimpresión: pleka scp
Impresión: Black Print cpi

Impreso en España - Printed in Spain
www.dummies.es
www.planetadelibros.com

Sumario

EN ESTE CAPÍTULO

- **Un recorrido por la historia del dinero**
- **El nacimiento de Bitcoin**
- **Características de la red Bitcoin**

Capítulo 1

Blockchain, Bitcoin y el origen de las criptomonedas

Las criptomonedas son, como su nombre indica, monedas encriptadas. Es decir, una forma de dinero creado sobre una elegante base tecnológica que aporta seguridad, comodidad e inmediatez, entre otros beneficios fundamentales. Es significativo e interesante hacer un breve recorrido a través de nuestra relación con el dinero desde sus formas más primitivas para llegar a entender el punto en el que estamos ahora y, con ello, tanto el potencial del *blockchain* y las criptomonedas como su aplicación financiera.

Este recorrido exprés por la historia del dinero nos llevará a descubrir la figura de Satoshi Nakamoto. Hace apenas una década, y con un seudónimo que oculta una identidad todavía hoy por desvelar, al-

guien lanza un documento que sienta las bases de una tecnología que pone patas arriba toda idea previa de relación entre clientes, instituciones, comerciantes e incluso Gobiernos. Con ello, abre la visión de un mundo completamente descentralizado que dota de mayor poder a los ciudadanos, a las personas.

En este primer capítulo iniciamos este trepidante viaje para que conozcas las bases del *blockchain,* y con ello, todo lo que viene después. Abróchate el cinturón, ¡despegamos!

El dinero a lo largo de la historia

¿Te has preguntado alguna vez qué es el dinero? Podemos definirlo como una unidad de medida, un medio de intercambio utilizado por una sociedad para el pago de todo tipo de bienes y servicios. Actualmente, el dinero se materializa en la forma física de billetes o monedas, pero ¿desde cuándo es así? O lo que es más interesante aún, ¿qué antigüedad tiene el dinero?

Aunque la forma de dinero ha ido progresando muy lentamente a lo largo de la historia, su esencia no ha cambiado. El dinero, como forma de expresar valor, se mantiene intacto. Y es que el concepto de dinero es tan antiguo como la civilización. Desde los primeros textos en forma de jeroglífico —que incluyen apuntes contables— hasta los yacimientos de civilizaciones primitivas en los que se encuentran monedas o formas más rudimentarias de acuñar valor, el dinero siempre ha estado presente. A lo largo de los últimos milenios ha evolucionado y completado algunas fases o periodos fundamentales.

- **Trueque.** Este modo de intercambio de bienes no es una forma de dinero, ya que no implica materializar el valor en una unidad de medida, pero es el origen del concepto de valor monetario como hoy lo conocemos. Hace miles de años, el hecho de cambiar un bien de primera necesidad por otro implicaba dar valor a las cosas. Por ejemplo, cambiar una piel de oso por tres conejos significaba que la piel era más valiosa; es decir, que, siglos más tarde, la piel valdría más dinero.
- **Metales preciosos.** La principal evolución en la concepción del valor se produjo cuando se pasó del valor intrínseco de las cosas —es decir, que "sirven para algo", como una piel para abrigarse— al valor abstracto, como el otorgado a un objeto, por ejemplo, una concha marina. Entre las primeras formas de

dinero encontramos caracolas, plumas, adornos o incluso la sal. Con el tiempo, los metales preciosos, principalmente la plata, el oro y el cobre, se fueron imponiendo de forma global.

Aunque haya habido muchas formas primitivas de dinero en varias civilizaciones del planeta —ya sea mediante piedras o metales preciosos—, todas cumplen unas características comunes: son fáciles de transportar, resistentes, se pueden fraccionar, son difíciles de obtener y, por sus cualidades estéticas, las reconocen en distintas culturas.

- **Moneda.** Con la progresiva implantación del uso del oro y la plata como intercambio de valor en Medio Oriente, China y la India, hacia el año 600 a. C. se comenzaron a acuñar las primeras monedas como unidad con un peso fijo y un valor concreto. De este modo, se consiguió fijar un estándar, garantizar la cantidad de material que contenía cada moneda y reforzar el poder de la institución que avalaba la emisión de esa divisa.

  Siglos más tarde, comenzaron a utilizarse aleaciones de distintos metales para acuñar monedas, con lo que cada una de estas ya no estaba respaldada por el valor de la moneda en sí. Por ejemplo, el metal con el que está hecha una moneda de un euro hoy vale mucho menos de un euro, pero como sociedad le reconocemos el valor porque está respaldado por el Banco Central Europeo. Fue un hecho tremendamente significativo, ya que traspasaba el valor del dinero de su forma física al organismo o país que lo acreditaba. Esto dio pie a formas de dinero futuras, como los billetes, y fue el origen del sistema fiduciario o, dicho de otro modo, el sistema monetario como lo conocemos hoy.

- **Dinero bancario.** Con la madurez del sistema monetario, y como complemento al dinero físico, hacia el siglo XV surgió en el norte de Italia una idea: la oportunidad de custodiar el dinero en entidades a las que se entregaría la confianza para guardar el dinero, a cambio de un documento que acreditase que ese cliente tenía efectivamente la cantidad depositada. Todos esos apuntes y balances de los clientes quedaban registrados en las cuentas de las instituciones, facilitando así la custodia de dinero, el crédito, el comercio y el traspaso de grandes sumas. Era el origen del sistema bancario como hoy lo conocemos.

  En una primera etapa, el cliente tenía que pagar a la institución financiera por la custodia del dinero. Más adelante, pasó a ser el banco el que pagaba un interés mínimo a sus clientes a cambio de utilizar el dinero de estos para conceder crédito a nuevos

clientes. Esto es lo que se conoce como coeficiente de caja, y el no haberlo respetado sería una de las razones tras la crisis económica desencadenada en 2008.

El "coeficiente de caja" es la porción de depósitos que un banco debe mantener intactos en sus propias arcas respecto al porcentaje de dinero que puede utilizar para conceder préstamos e inversiones a sus clientes.

- **Dinero electrónico.** ¿Habías pensado alguna vez en que la mayoría del dinero que hoy utilizamos o el que tú tienes ahorrado no existe en realidad? Son apuntes contables reconocidos por instituciones financieras que acreditan que ese dinero es tuyo, pero es dinero que nunca será materializado en forma de monedas o billetes. De hecho, se estima que menos del 5 % del dinero es efectivo. El resto responde a todo el dinero no impreso que fluye mediante apuntes, pagos y transferencias electrónicas. La tecnología propició esta gran evolución en la concepción del dinero, que también se materializa en el conocido como *plastic money,* que hace referencia a este dinero electrónico en forma de tarjeta de crédito. El dinero electrónico nació en 1949 de la mano de Diners Club como una forma de cheque para que sus clientes pudieran cenar a crédito en ciertos establecimientos. Tras ello, nacerían Visa, American Express y el resto de marcas que hoy conocemos. Su aparición facilitaría los pagos y democratizaría la compra a crédito.

- Tras esto, la evolución a la que aparentemente apuntamos es a una *cashless society*. Es decir, nos dirigimos a una sociedad sin dinero en efectivo donde cualquier intercambio de valor monetario entre dos partes quedará registrado digitalmente. Esta transición, ¿será hacia una divisa digital emitida por Gobiernos centrales? ¿Tomarán las criptomonedas el relevo al dinero impreso? Está por ver, pero hay muchos proyectos trabajando en ello.

En los últimos años se han producido otras innovaciones relevantes dentro del sistema financiero, como las plataformas de pago nativamente digitales, siendo PayPal la más conocida, o la reciente efervescencia del sector *fintech*, que está redefiniendo la relación entre instituciones financieras y usuarios. Pese a estos puntos, a lo largo de la historia no ha cambiado la necesidad de una unidad de cambio reconocida para intercambiarla por las cosas a las que le damos valor, algo que hemos hecho mediante el dinero. Sí ha cambiado su forma, las instituciones que lo emiten, los organismos que lo regulan y los sistemas para transferirlo. Precisamente esto lleva a plantearse de

EL PATRÓN ORO, EL DÓLAR Y EL SISTEMA FIDUCIARIO

El patrón oro fue un sistema monetario popular durante el siglo XIX en el que los billetes se podían cambiar por oro y, a su vez, el oro por billetes, siempre a un tipo de cambio fijo. El sistema desapareció al acabar la Primera Guerra Mundial, cuando varias economías mundiales necesitaron imprimir más dinero fiduciario, haciendo insostenible el respaldo de todo ese dinero en oro. En los acuerdos de Bretton Woods de 1944 se fijó el dólar estadounidense como divisa para respaldar el patrón oro, que podía seguir respaldando su valor con reservas de oro propias. Además, se decidiría la creación del Banco Mundial y el Fondo Monetario Internacional. En 1971 se quebró finalmente ese acuerdo, pero se mantuvo el dólar como divisa internacional de referencia y principal moneda fiduciaria o *fiat*, a la cual, aun sin contar con valor intrínseco, se le otorga un valor legal propio, no el valor que hoy le damos al dólar y al dinero.

nuevo una serie de preguntas: ¿qué respalda el valor del dinero actual, en forma de dólar, euro u otra divisa? ¿Cuál es la función de las instituciones que regulan la emisión de dinero? ¿Qué papel juegan las entidades financieras que gestionan el dinero de los ciudadanos?

El origen de Bitcoin... ¿En una antigua civilización perdida en el Pacífico?

El *blockchain* se presenta hoy como una gran innovación que, gracias a una brillante tecnología, resuelve la forma de intercambiar valor. Sin embargo, según apuntan varios historiadores e investigadores, parece que tiene una curiosa conexión con una ancestral forma monetaria llamada Rai, unas piedras gigantes en forma de ballena utilizadas hace centenares de años en la diminuta isla de Yap, en la Micronesia. La mayoría de ellas ¡pesaban toneladas! Aquella piedra provenía de otra isla que estaba a centenares de kilómetros, dotando a las piedras de más valor.

Esa cualidad de "grandes piedras" es lo que las relaciona con Bitcoin. Ambas formas de moneda representan un sistema de contabilidad público que aporta transparencia sobre las transacciones y permite

ver quién envía y recibe el dinero, así como la seguridad de que son inamovibles. Además, todo ello se realiza sin necesidad de que haya un intermediario o entidad bancaria que garantice ese traspaso de dinero. Las piedras se intercambiaban por algo de valor, y, entre todos los habitantes, se transmitía de forma oral quién era el nuevo propietario de dicha piedra, haciéndose así copias de ese registro contable público e inmutable.

Criptografía y dinero digital

Antes de entrar en la misteriosa figura de alguien conocido como Satoshi Nakamoto y la creación del *blockchain*, hay que hablar del dinero digital y su relación con la criptografía como precedente de las criptomonedas.

Por un lado, es necesario cubrir la figura y el trabajo de David Chaum, considerado el padre de la criptografía y el inventor del dinero digital. Este criptógrafo, matemático, informático y teórico estadounidense, nacido en 1955, se doctoró en Informática y Administración de Empresas por la Universidad de Berkeley, California, y organizó las primeras conferencias mundiales sobre criptografía, conocidas como CRYPTO. En ellas, presentaría trabajos imprescindibles, como su artículo de 1981 "Correo electrónico de rastro oculto, direcciones de regreso y seudónimos digitales", que sentó las bases del anonimato de comunicaciones entre usuarios, o "Sistemas informáticos establecidos, mantenidos y confiables por grupos mutuamente sospechosos", el primer precedente conocido de varios de los principios del *blockchain*. Esto permitiría avanzar con la creación de un sistema de pagos digitales que, entre otras innovaciones, incluiría la idea de firma ciega.

La **firma ciega** es un protocolo de firma digital que permite a un usuario recibir un mensaje firmado por otra entidad sin que esta pueda ver el contenido del mensaje. Este sistema también permite evitar el doble gasto, es decir, que una forma de dinero digital pueda utilizarse fraudulentamente en dos ocasiones. Si no existiera este método, si hoy solo tuvieras 100 euros en tu cuenta, podrías enviar una transferencia de 100 euros a un amigo... y, antes que se confirmara la recepción del dinero, ¡comprarte unas zapatillas por valor de 100 euros!

Años más tarde, en 1990, David crearía la empresa de pagos electrónicos DigiCash, que incluía la aplicación de sus trabajos e investigaciones previas, los cuales se materializarían en la solución eCash. En 1994, y tras haber madurado el proyecto, en la primera conferencia

World Wide Web demostró que el sistema de pagos que había desarrollado permitía transacciones de dinero entre ordenadores en red de forma automatizada. Era, sin duda, uno de los grandes precedentes de las criptomonedas como hoy las conocemos.

David Chaum continúa desarrollando brillantes proyectos basados en *blockchain* que, ante todo, tienen la privacidad del individuo como piedra angular de su corriente ideológica, el *cypherpunk.* Esto lo relaciona con otra de las figuras que precedieron a Satoshi Nakamoto y que resultan fundamentales para entender Bitcoin: Timothy May.

Tymothy C. May, estadounidense nacido en 1951, fue otro brillante ingeniero informático, pensador, escritor e ideólogo, conocido activista del movimiento *cypherpunk* y creador del criptoanarquismo como corriente fundamental precedente al *blockchain*. Su primera experiencia profesional lo llevó a trabajar en Intel durante casi una década, donde aportó grandes descubrimientos para el aumento de la eficiencia de los circuitos electrónicos que producía el gigante norteamericano. Pero tomó su papel protagonista en 1988, al publicar "El manifiesto criptoanarquista", considerado un documento fundamental en materia de criptografía y privacidad. En él, defiende el derecho al anonimato y pone en tela de juicio el papel regulador de Gobiernos e instituciones de todo el mundo. Durante los años siguientes Tim seguiría lanzando publicaciones de vital importancia para entender el nacimiento y la madurez del pensamiento *crypto,* donde incluía ideas como la necesidad de sistemas criptográficos, comunidades y redes virtuales, o comunicaciones anónimas, entre otros.

El **criptoanarquismo** es una corriente que defiende la anarquía a través de la tecnología informática. Los criptoanarquistas emplean *software* criptográfico para garantizar la confidencialidad y seguridad al enviar y recibir información a través de redes informáticas, en un esfuerzo por proteger la privacidad, la libertad de expresión y la libertad económica. Mediante el uso de este *software* basado en comunicación entre pares (*peer-to-peer*), la asociación entre la identidad de un determinado usuario u organización y el seudónimo que utiliza es difícil de trazar, a menos que el usuario revele esa asociación. Es difícil decir qué leyes del país serán ignoradas, ya que incluso se desconoce la ubicación del participante. Sin embargo, en teoría, los participantes pueden crear voluntariamente nuevas leyes utilizando contratos inteligentes o, si el usuario es un seudónimo, depender de la reputación en línea.

Por lo que has ido leyendo en estas últimas líneas, te habrás dado cuenta de que la tecnología *blockchain*, Bitcoin y todo lo que viene de-

trás, es el cruce de una corriente tecnológica y de otra ideológica. Las dos son pilares imprescindibles para entender la criptoeconomía.

El origen de Bitcoin: Satoshi Nakamoto

Treinta y uno de octubre de 2008: firmado con el nombre de Satoshi Nakamoto, en una lista de correo de criptografía se publica un documento llamado "Bitcoin: A Peer-to-Peer Electronic Cash System". El rompedor documento no se limitaba a describir la creación de una criptomoneda, el bitcóin, sino que también detallaba la tecnología en la que se iba a apoyar para operar y un protocolo con una política para regular la creación y distribución de esa moneda. Es decir, prácticamente el documento estaba diseñando una política monetaria propia.

Las **redes *peer-to-peer*** o P2P son redes de ordenadores conectados entre pares, redes descentralizadas donde los usuarios pueden intercambiar datos y contenido a través de internet sin la necesidad de un intermediario.

En enero de 2009, apenas dos meses después de publicar el primer documento, Nakamoto subió la primera versión del *software* de Bitcoin. Días más tarde, Hal Finney, primer usuario de la red con identidad conocida —y una de las personas más estrechamente relacionadas con Satoshi Nakamoto—, recibió diez bitcoines, confirmando así la primera transacción de bitcoines de la historia. En noviembre de ese mismo año, Nakamoto publicó un mensaje en el foro Bitcointalk, donde daba abiertamente la bienvenida a nuevos usuarios, abriendo con ello el proyecto a la comunidad mundial. Desde entonces, la red fue creciendo gradualmente y se fueron agregando más usuarios a la plataforma mediante la descarga del *software.* Esto permitió la aparición de nuevos nodos para guardar copias del registro de transacciones. Asimismo, provocó que se popularizara el trabajo de minería necesario para validar transacciones y generar nuevas monedas, casi de igual manera que con la minería tradicional, en la que se extraen metales preciosos. Más adelante detallaremos estos conceptos.

El **código abierto** u *open source* es un concepto que se refiere a una forma de distribuir contenido digital, como un programa informático, en el que se permite a los usuarios disponer e incluso modificar

dicho contenido libremente. Tras esta forma de operar se esconde una verdadera cultura por compartir y construir proyectos de manera colaborativa, siendo Bitcoin un buen ejemplo de ello.

Tras unos meses apoyando la progresiva adopción de Bitcoin, a finales de 2010 Satoshi Nakamoto publicó una actualización con la última versión del *software* de Bitcoin. Además, aprovechó para recalcar que su identidad permanecería en el anonimato, reafirmando el valor de su trabajo como un proyecto de código abierto desarrollado por la comunidad y de libre uso para el mundo entero. Desde entonces, quedará por resolver el misterio de quién o quiénes se esconden tras el nombre de Satoshi Nakamoto.

RECUERDA

La identidad de Satoshi Nakamoto es, sin duda, uno de los grandes misterios de nuestro tiempo, la pregunta del millón de dólares, de euros o de bitcoines... En la última década se han barajado varios nombres, como Wei Dai, creador del b-money y de la librería Cypto++; Nick Szabo, que desarrolló el concepto de Bit Gold; Adam Back, criptógrafo que desarrolló Hashcash; Craig Wright, informático australiano que se autoproclamó inventor de Bitcoin; o el propio Hal Finney, primer usuario de la red Bitcoin. Aunque muchos medios e investigadores han tratado de desvelar su identidad, nunca se ha llegado a una conclusión. Parece que seguirá siendo una de las grandes incógnitas de la humanidad.

Los elementos fundamentales de la red Bitcoin

Tras conocer el origen de esta tecnología, es importante destacar los pilares básicos sobre los que se fundamenta esta red global que constituye Bitcoin. De hecho, sobre ellos también se sustentan el resto de criptomonedas y *blockchains*. Aunque en el próximo capítulo entraremos en más detalle y pondremos ejemplos, aquí va una primera explicación de elementos fundamentales, como los nodos, los mineros y el consenso. En un primer momento, la explicación de estos conceptos puede parecer algo compleja, pero, cuando los domines, podrás decir que has evolucionado de *dummy* a casi experto, así que ¡a por ello!

RECUERDA

En el glosario que encontrarás al final del libro dispones de las descripciones de todos los conceptos clave. Si te parece que esta sección es algo compleja para ti, avanza al siguiente capítulo y ya volverás a

esta parte técnica cuando lo consideres oportuno. Te recordamos que esta guía está escrita para que la leas y releas como te resulte más útil.

Los nodos

En primer lugar, es fundamental que comprendas la esencia de Bitcoin como una red mundial descentralizada y distribuida en ordenadores que trabajan P2P (*peer-to-peer*). Es decir, todos los miembros de la red se comunican entre ellos sin que ninguno centralice la comunicación. Cada uno de estos equipos informáticos es un nodo, y se estima que hoy en día hay más de 10.000 nodos de Bitcoin repartidos por el mundo. Además, todos se encuentran conectados entre sí formando una sólida red en la que cada uno guarda una copia parcial o completa del historial de transacciones. Si es un nodo completo, el ordenador almacena el registro íntegro con la primera transacción de hace más de una década. A inicios de 2020, el peso de este registro de transacciones es de unos 260 gigas de información.

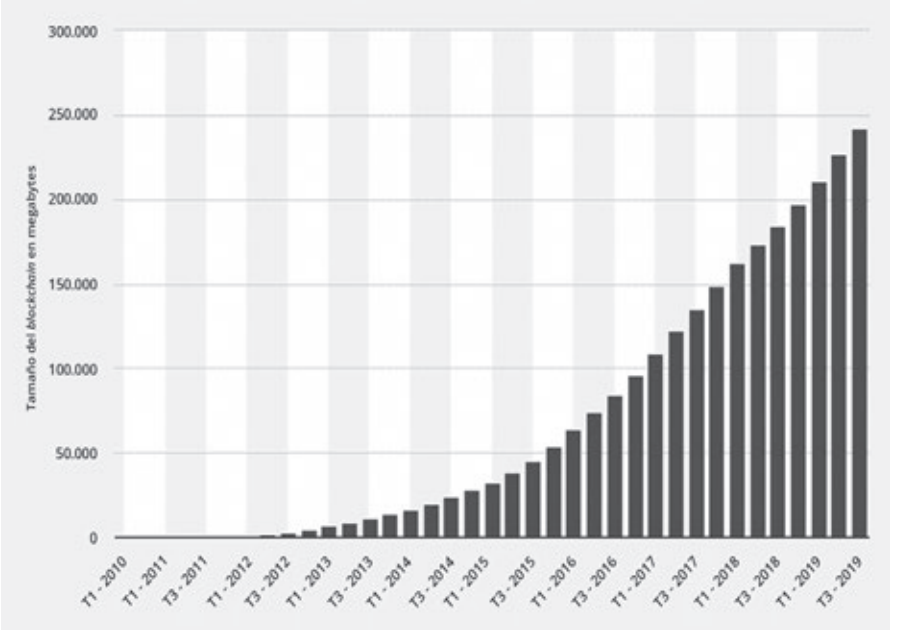

Figura 1-1 Tamaño del *blockchain* de Bitcoin en su primera década, de 2010 a 2019, por cuatrimestres (en megabytes).

Otro punto importante para explicar por qué la red Bitcoin es una red P2P y descentralizada es que, como todos los ordenadores de la red están conectados entre sí, nadie puede tomar el control de la operativa. Además, se trata de una red resistente a la censura por parte de cualquier Gobierno o entidad, lo cual es otra de las fortalezas primordiales de Bitcoin. Asimismo, este carácter participativo significa que cualquier usuario puede convertirse en un nodo, ya que Bitcoin es una red abierta y su *software* es de código abierto y gratuito. Tú mismo puedes descargarte el *software* de Bitcoin, formar un nodo y respaldar la red descentralizada más grande del mundo.

El libro contable: DLT

Cada nodo cuenta con algo similar a un libro mayor que hace la función de un gran registro de contabilidad, el cual almacena cada operación ejecutada de manera inmutable. Es algo similar al registro de un banco, donde la entidad almacena la contabilidad de las operaciones y balances de todos sus clientes. En este caso, el libro mayor no es único, sino que hay una réplica exacta de este por cada nodo completo existente. De ahí se derivan las siglas DLT (*Distributed Ledger Technology*), utilizadas para definir estos libros de contabilidad distribuida.

Este mecanismo constituye una ventaja de suma importancia, ya que uno de los grandes problemas a los que se enfrenta el sistema financiero para asegurarse de que las cosas funcionan de manera correcta es la garantía de que un mismo dinero no sea usado dos veces. Esta es una de las razones de la demora en las transferencias bancarias internacionales tipo SWIFT, ya que deben emplearse mecanismos de seguridad para revisar que el emisor no gaste el dinero de una transferencia una vez emitida antes de que el importe llegue a la parte receptora y ella pueda gastarlo.

Por lo que respecta a Bitcoin, el libro mayor no puede modificarse de forma autónoma, ya que se encuentra replicado en todos los nodos. Todos los nodos deben estar de acuerdo ante un hecho, una "verdad", y uno no puede cambiar esa "verdad" sin que los otros también lo hagan. De esta forma, se evita el problema del doble gasto y la posibilidad de una manipulación de la red.

El consenso

La clave de esta tecnología es el consenso, el instrumento que permite asegurar que la información es válida y verdadera. Los nodos tienen que pactar entre ellos sobre quién validará una transacción para

añadirla al bloque. Una vez se ponen de acuerdo, se graba la transacción y se valida como correcta, todos los nodos de la red cuentan con una copia de esa información. El mecanismo para hacerlo de una forma descentralizada radica en que, al no haber una entidad central que decida cuál es el bloque válido que todos añaden, se debe realizar mediante métodos criptográficos, los cuales permiten que se llegue de forma repartida a este consenso con respecto a cómo añadir otro bloque.

En el próximo capítulo detallaremos los distintos tipos de consenso como parte fundamental del *blockchain*, para, a su vez, diferenciar los distintos proyectos según la forma de validar las transacciones.

Los mineros

Finalmente, es momento de ver qué rol desempeñan los participantes, los mineros, y darnos cuenta de la importante actividad de minado que desempeñan. Entramos, entonces, en el segundo de los pilares básicos de la criptoeconomía.

INFORMACIÓN TÉCNICA

Los **mineros** son un grupo de ordenadores que forman parte de los nodos y que validan las transacciones de la red a cambio de una recompensa. El nombre se remite de forma simbólica a los antiguos buscadores de oro que abrían minas incansablemente buscando un filón para enriquecerse. Los mineros desempeñan una actividad muy importante para el correcto funcionamiento del sistema, siendo incentivados con su "oro digital", los bitcoins.

El procedimiento es el siguiente: cada petición de transacción se agrega a un bloque y, una vez consultado el registro contable disponible en los distintos nodos, se revisa si la información es correcta. En ese momento, los mineros compiten por descifrar el contenido de la información, validar las transacciones y encriptar de nuevo el resultado, que se agregará al libro de contabilidad. Cuando alguno de los mineros resuelve el problema y se llega al consenso, la información de las transacciones se registra en el nuevo bloque, se añade a la cadena de bloques y el resto de los nodos lo replican, guardando así una copia de forma inalterable, sin que pueda ser modificada. Los bloques de Bitcoin se minan aproximadamente cada diez minutos, y el minero que resuelve el problema y sella el bloque recibe una recompensa por el trabajo resuelto.

RECUERDA

¿En qué se diferencian un nodo de un minero? Un nodo solo tiene información del histórico del registro contable, mientras que el minero consulta a los nodos para validar transacciones, cerrar un bloque y

subir ese nuevo bloque a *blockchain*. Cuando el minero cierra el bloque, actualiza el registro contable, cuyo apunte se copia en todos los nodos. Por ese trabajo, el minero se lleva bitcoines de nueva creación. El nodo solo almacena información; el minero "trabaja" para validar transacciones.

El sistema de recompensas

Competir por descifrar el problema criptográfico es una idea interesante, ya que nos hace cuestionarnos lo siguiente: ¿por qué la gente compite por ello, si exige una gran inversión en equipos potentes, de alta capacidad de computación, e implica un gran consumo energético?

Como acabamos de describir, cada vez que un minero encuentra la solución a un problema y la registra en el bloque, se generan nuevos bitcoines que se transfieren al minero que ha logrado resolver el problema y agregarlo al bloque. Es el equivalente a un minero de una mina convencional cuando, con su excavación, consigue encontrar oro.

En las redes de criptomonedas —fundamentalmente para quienes practican esta actividad de forma profesional—, es esencial que exista una recompensa económica en contraprestación al servicio de minería que brindan a la red. Históricamente, ha habido otras redes informáticas entre usuarios P2P, como es el caso de la red BitTorrent. Sin embargo, estas redes presentan un problema: al no contar con una recompensa económica, el desarrollo, mantenimiento y expansión de la red resulta incierto, pues no está incentivado. La red Bitcoin es diferente, pues esta sí ofrece una recompensa económica por participar en ella, ya que, cada vez que se mina un bloque, se distribuyen nuevos bitcoines entre los usuarios que mantienen la red. Esta es una de las razones que ha llevado al crecimiento de Bitcoin y a que cada vez existan más personas interesadas en unirse a la criptoeconomía.

Una nueva política monetaria

A principios de 2009, la recompensa inicial por cerrar un bloque de Bitcoin era de 50 bitcoines. Desde entonces, cada 210.000 bloques, que corresponde a unos cuatro años, se produce un *halving*, que significa que la retribución se divide entre dos, y así progresivamente. Por ejemplo, desde mayo de 2020, la recompensa por cerrar un bloque se

reduce a 6,25 bitcoines (BTC) y, tras cuatro años, en 2024, será de solo 3,125 BTC. Esta política retributiva, que se incluye en el protocolo de Bitcoin lanzado por Satoshi Nakamoto en 2008, resulta de vital importancia para entender lo disruptiva que es esta tecnología, también desde un punto de vista económico.

Se conoce como ***halving*** al hito que consiste en la reducción a la mitad de la recompensa ofrecida a los mineros por validar bloques de una red de *blockchain*. En el caso de Bitcoin, este evento de produce repetidamente cada 210.000 bloques minados, que equivale a unos cuatro años.

Por un lado, como ya se ha explicado, este mecanismo es la forma de incentivar el proceso de minería y permite que la red siga funcionando. Pero, más allá de quién se lleve la retribución, el *blockchain* define un nuevo modelo monetario. En el caso de Bitcoin, la cantidad de moneda que había al inicio era de cero unidades, mientras que la cantidad máxima de monedas disponibles será de 21 millones de unidades, a lo que se llegará aproximadamente en el año 2140. Dicho de otro modo, y en términos de economía convencional, será la base monetaria máxima, el límite de unidades de bitcóin que jamás habrá en circulación.

Volviendo al origen de Bitcoin, tras el bloque génesis de 2009 —que incluía el registro de la primera emisión—, pasó de no haber ningún bitcóin en circulación a que hubiera 50 bitcoines disponibles, transferidos a la cartera de Satoshi Nakamoto como retribución por minar ese primer bloque. Desde entonces, al minar un bloque cada diez minutos, la base monetaria de Bitcoin fue aumentando en 50 unidades cada diez minutos hasta el *halving* de 2012, en el que la retribución por bloque disminuyó a 25 unidades (fig. 1-2).

Esta política monetaria de Bitcoin lo diferencia completamente de nuestro sistema monetario actual. Aquí tienes algunas de las principales razones:

- No hay un organismo central que regule la emisión de dinero nuevo. Las reglas para generar el dinero están fijadas en el protocolo lanzado en 2009. Desde entonces, el protocolo elimina la necesidad de un ente regulador, como un Gobierno o una institución.
- El dinero pasa directamente a manos de los usuarios, en forma de mineros, sin que haya una institución que medie en la puesta en circulación. En el caso del sistema fiduciario, serían entidades como el Banco Central Europeo y el Banco de España.

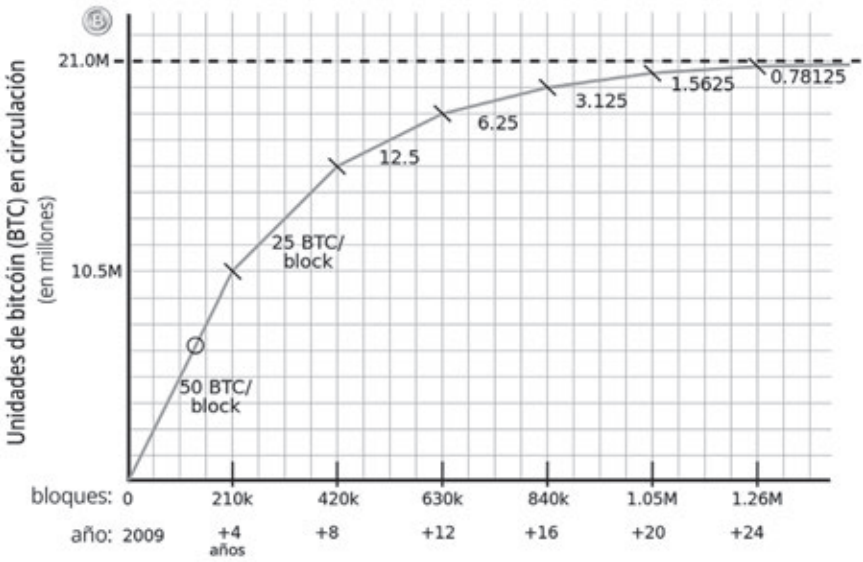

Figura 1-2 Evolución temporal de la cantidad de bitcoines disponibles en circulación.

- Hay una cantidad limitada de monedas. Según hemos comentado, nunca habrá más de 21 millones de bitcoines, mientras que los euros o los dólares se emiten continuamente en función de las necesidades de un organismo central o país.
- No es posible devaluar la moneda de forma centralizada. Al responder a una emisión de moneda regulada y progresiva, no se puede aumentar drásticamente la base monetaria de Bitcoin imprimiendo nuevo dinero, como sucede con el dinero fiduciario, lo cual implica una devaluación de su valor.
- Como resultado de lo anterior, es un sistema deflacionario en vez de inflacionario. Es decir, cruzando el mercado, la emisión y la disponibilidad de unidades de bitcóin, una unidad de bitcóin cada vez tiene más valor.

Podríamos hablar también de otros aspectos intrínsecos del bitcóin, como el hecho de ser una moneda cien por cien digital, además de constituir una red de pagos descentralizada y sin intermediarios… pero ya habrá tiempo para desgranarlo en los siguientes capítulos. ¡Nos queda mucho libro por delante!