PREGUNTAS 100 ESENCIALES

A COLOR

ISMAEL SANTIAGO MORENO

INTRODUCCIÓN AL BLOCKCHAIN Y LAS CRIPTOMONEDAS

EN 100 PREGUNTAS

TODO LO IMPRESCINDIBLE EXPLICADO CON RIGOR

www.100Preguntas.com

nowtilus saber

Introducción al Blockchain y criptomonedas en 100 preguntas

Introducción al Blockchain y criptomonedas en 100 preguntas

Ismael Santiago Moreno

nowtilus

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

Título: *Introducción al Blockchain y criptomonedas en 100 preguntas*
Autor: © Ismael Santiago Moreno

Copyright de la presente edición: © 2021 Ediciones Nowtilus, S.L.
Camino de los Vinateros, 40, local 90, 28030 Madrid
www.nowtilus.com

Elaboración de textos: Santos Rodríguez

Diseño de cubierta: NEMO Edición y Comunicación

ISBN Digital: 978-84-1305-175-8
Fecha de publicación: marzo 2021

A mis hijos Adriana e Ismael, que dan sentido a mi vida, estudio y trabajo diario.
Gracias por vuestra comprensión, cariño y amor.

Índice

Conceptos y tecnologías que posibilitan las criptomonedas y Blockchain

1

¿Encontramos relación entre «Red entre pares o iguales» y Blockchain?

Las redes entre pares o iguales, o también denominadas P2P o Peer-to-Peer son un tipo de redes formadas por miles o incluso millones de ordenadores (o nodos) situados en cualquier parte del planeta donde no existe un punto central de conexión, ya que son redes descentralizadas que funcionan con un mismo protocolo de comunicaciones, con el propósito de crear una gran red para compartir cualquier tipo de información. De esta manera, los integrantes de este tipo de redes pueden intercambiar

información de forma directa y sin intermediarios, para ello solo necesitan descargarse un software que conecte su ordenador con el resto de personas que están dentro de la red P2P y así comunicarse con ellos.

Pero ¿qué son los nodos y los protocolos?

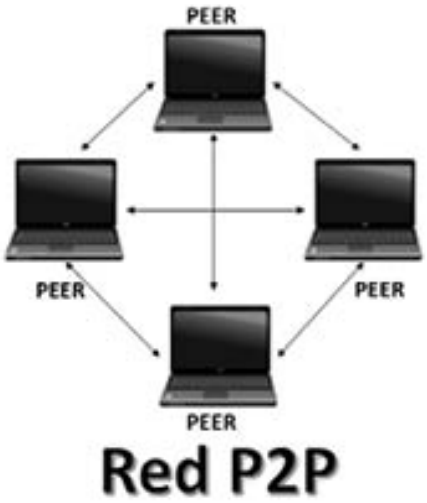
Un nodo puede ser una megacomputadora o un mero ordenador personal. Independientemente de la capacidad de computación, todos los nodos han de contar con el mismo software/protocolo para comunicarse entre sí. Estos nodos están interconectados a través de una red P2P y pueden comunicarse entre sí para transmitir y compartir información y datos a través de dicha red.

Desde el punto de vista de la tecnología de cadena de bloques (blockchain), los nodos lo forman todos aquellos ordenadores que están interconectados a esta red, ejecutando el programa informático que se encarga de todo su funcionamiento.

En ingeniería, cuando se habla de protocolos de comunicaciones se hace referencia a un sistema de reglas, en forma de software informático, que permiten a una red de ordenadores (nodos) comunicarse entre sí para transmitir información. Por ejemplo, el protocolo de una cadena de bloques o blockchain otorga un estándar común para definir la comunicación entre los ordenadores participantes en su red.

Una red entre iguales o P2P es una red donde no hay ningún tipo de jerarquía ya que los nodos cumplen la función de clientes y servidores. En una red de estas características cada ordenador estaría en un plano de igualdad con los demás, facilitando una comunicación de tipo horizontal. El interés que han despertado las redes P2P se debe principalmente al uso que se ha hecho de las mismas para la transmisión de contenidos digitales.

Las redes entre pares o iguales gestionan y optimizan el empleo del ancho de banda del resto de los usuarios de la red mediante la conectividad entre los mismos, obteniendo de esta forma más rendimiento en las conexiones que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación.



El funcionamiento de una red P2P se basa en la construcción de un protocolo de comunicaciones que permita a las personas que usan dicho software comunicarse de forma directa y sin intermediarios. Fuente: Ismael Santiago.

¿Qué características son las deseables para las redes entre pares o iguales (P2P)?

Las características deseables en una red P2P son las que mecionamos a continuación:

- *Descentralización*: son redes donde todos los nodos son iguales y por tanto ningún de estos resulta imprescindible para el funcionamiento de tal red.

- *Robustez*: la naturaleza distribuida de las redes P2P permite encontrar la información sin hacer peticiones a ningún servidor centralizado.
- *Escalabilidad*: lo deseable es que cuantos más nodos estén conectados a una red P2P mejor será su funcionamiento, ya que cuando los nodos comparten sus propios recursos el total de los recursos de la red P2P aumenta. Esto es diferente en una arquitectura del modo servidor-cliente con un sistema fijo de servidores, en los cuales el aumento de clientes podría significar una transferencia de datos más lenta para todos los usuarios.
- *Distribución de costes entre los usuarios*: se aportan o comparten recursos a cambio de otros recursos, como archivos, ancho de banda o almacenamiento de disco, entre otros.

En este tipo de redes P2P no todo son ventajas, también encontramos inconvenientes, sobre todo en lo que respecta a cuestiones como la seguridad.

Las redes P2P, al servir para intercambiar y compartir información de forma directa entre dos o más usuarios, han provocado que alguno de estos las emplee para intercambiar archivos cuyo contenido está sometido a las leyes de derechos de autor, lo que ha generado una gran polémica entre defensores y detractores de tales redes.

En 1999 nació Napster, un innovador proyecto desarrollado en los Estados Unidos por los emprendedores Shawn Fanning y Sean Parker, quienes popularizaron el concepto de red distribuida de forma masiva entre los usuarios, introduciendo una aplicación para compartir música y archivos. Napster fue el comienzo de las redes P2P, como las conocemos en la actualidad.

Fue un proyecto creado con la finalidad de permitir el intercambio y distribución de música. Lo único que necesitaban sus usuarios era descargar su software y formar parte de esta red, que llegó a superar los 26 millones de usuarios cuando entonces los usuarios de Internet eran 248 millones. Estos 26 millones de usuarios de Napster podían intercambiar sus archivos de música sin ningún tipo de intermediarios. Debido al hecho de que Napster distribuía música sin pago de derechos de autor, la plataforma fue finalmente cerrada tras un largo juicio en julio de 2001.

Sin embargo, lo que Napster había hecho llamó al mundo a desarrollar sistemas más descentralizados. Gracias a estas redes descentralizadas se había preparado el terreno para otras redes P2P tan conocidas como puede ser Bitcoin, sistema que originó la primera criptomoneda con el mismo nombre.

Cualquier persona que desee unirse y contribuir a la red del sistema Bitcoin puede hacerlo libremente con tan solo descargar e instalar el software de Bitcoin en su ordenador.

2

¿EL SOFTWARE DE CÓDIGO ABIERTO FACILITA EL DESARROLLO DE LAS CRIPTOMONEDAS?

Para entender la dinámica de mercado de la tecnología de cadena de bloques o blockchain es muy importante conocer el concepto de código abierto y no todo lo que se llama

software de código abierto es software libre, siendo este último el que permite a sus usuarios emplear, estudiar, mejorar y/o redistribuir el mismo, bien con los cambios que se realicen posteriormente o en su forma original. Para todo esto resulta esencial contar con el código fuente de dicho software.

Existen diferencias entre el software libre y el software de código abierto. El software libre requiere obviamente disponer de código abierto, si bien lo contrario no siempre es cierto, impidiendo su empleo o modificación con fines militares o comerciales.

Cuando se permite el acceso al código fuente y se dispone la autorización para poder cambiarlo, la comunidad de programadores puede mejorar el programa a nivel general, llevando a cabo mejoras en la usabilidad y solucionando eventuales fallos, lo que se traduce en un software de mayor calidad. Este proceso es de naturaleza descentralizada, si lo comparamos con sus homólogos de código propietario, donde el control se concentra en un grupo reducido de desarrolladores que trabajan a las órdenes de una determinada organización.

Un software es libre si otorga a los usuarios de manera adecuada las denominadas cuatro libertades: libertad de usar, estudiar, distribuir y mejorar, de lo contrario no se trata de software libre.

A continuación, nos adentramos en la historia del Software Libre y del Software de Código Abierto.

Entre los años 1960 y 1970, el software no se consideraba un producto sino un añadido de los grandes ordenadores de la época que los vendedores entregaban a sus clientes para que estos pudieran utilizarlos. En esta época, programadores y desarrolladores de software

compartían libremente sus programas informáticos. En ámbitos universitarios y empresariales, se creaban y se compartía el software sin restricciones.

La situación cambió en los años ochenta, cuando los ordenadores más modernos comenzaban a emplear sistemas operativos privativos, obligando a los usuarios a aceptar condiciones restrictivas que impedían compartir, intercambiar o poder cambiar dicho software. Aunque el programador tuviese capacidad para solucionar el problema o error encontrado en el software y lo deseara hacer desinteresadamente, el contrato le impedía modificar dicho programa informático.

El 27 de septiembre de 1983, Stallman anunció el inicio del Proyecto GNU, que tenía como objeto crear un sistema operativo completamente libre. En 1985, Stallman fundó la organización Free Software Foundation (FSF) y publicó el Manifiesto GNU para describir el propósito del proyecto y explicar la importancia del software libre. En 1986 publicó la definición de «Software Libre» e introdujo el concepto de copyleft, que desarrolló para otorgar libertad a los usuarios y restringir las posibilidades de apropiación del software. En 1989 publicó la primera versión de la Licencia Pública General GNU (General Public License - GPL) codificando las ideas del software libre en un documento legal.

Richard Stallman inició el Proyecto GNU para escribir un sistema operativo completo y libre de las restricciones sobre el uso de su código fuente. Fuente: Génesis Gabriella en Pixabay.

Otro evento de enorme trascendencia fue la aparición de Linux, el cual es el nombre del núcleo de un sistema operativo desarrollado por Linus Torvalds y publicado como código fuente modificable en 1991.

La audiencia de un núcleo en el Proyecto GNU significaba que no existían sistemas operativos completos, aunque ya se habían desarrollados muchos componentes. Torvalds rellenó el hueco que existía, lo que hizo que muchos desarrolladores de software en el mundo empezaran a contribuir.

La combinación de los componentes software del Proyecto GNU con el núcleo Linux permitió materializar la idea de un sistema operativo completamente libre.

Entre mediados y finales de los 90 aparecieron muchas nuevas empresas tecnológicas que ofrecían servicios en la web. En la base estaba un Sistema Operativo GNU/Linux, con Apache como proveedor del servicio web, Mysql como motor para el almacenamiento de datos y PHP como lenguaje para la programación de las páginas web dinámicas.

En 1997, Eric Ratmond publicó un análisis reflexivo de la comunidad hacker y los principios del software libre. Este documento fue un factor clave para que Netscape Communications Corporation adoptara el modelo de desarrollo comunitario del software libre. Este código fue la base del navegador Mozilla Firefox.

Raymond y otros llegaron a la conclusión de que el activismo social de la FSF no era atractivo para las compañías como Netscape y buscaron una manera de adecuar el movimiento del software libre al mundo de los negocios. Fue así como sugirió el uso de la expresión «Código Abierto» para liberarse de las connotaciones ideológicas y de confrontación con el término «Software Libre».

Si nos centramos en las criptomonedas y en su tecnología implícita llamada blockchain o cadena de bloques encontramos que el protocolo Bitcoin y su software se publican abiertamente para que cualquier programador en cualquier lugar del mundo pueda revisarlo o crear su propia versión modificada. Bitcoin tampoco tiene propietarios, sino que lo controlan los usuarios que participan de dicho ecosistema.

Bitcoin solo puede funcionar correctamente si hay consenso entre todas las partes y es precisamente ahí donde radica gran parte de su fortaleza y su debilidad. Por lo tanto, todos los usuarios, mineros, inversores y programadores comparten un gran aliciente para proteger dicho consenso.

El código fuente de Bitcoin ha sido utilizado como la base para muchos otros proyectos de software. La forma más común de software generado a partir de él son otras criptomonedas o tokens.

La MIT License fue la licencia de software elegida en su día por Satoshi Nakamoto para Bitcoin. Se trata de una licencia que suele ser empleada cuando el creador del software quiere que el código resulte accesible al mayor número posible de desarrolladores. Técnicamente se trata de una licencia corta, sencilla y fácil de entender.

3

¿LOS PROTOCOLOS JUEGAN UN PAPEL PROTAGONISTA EN TODO ESTO?

En informática y telecomunicaciones, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades (ordenadores, Smart phones, etc.) de un sistema de comunicación se comuniquen entre sí para transmitir información.

Los sistemas de comunicación utilizan protocolos bien definidos para intercambiar mensajes. Cada mensaje tiene un significado exacto destinado a obtener una respuesta de un rango de posibles respuestas predeterminadas para esa situación en particular. Normalmente, el comportamiento especificado es independiente de cómo se va a implementar. Los protocolos de comunicación tienen que ser acordados por las partes involucradas.

Con estas definiciones y aclaraciones, podemos comenzar a comprender el concepto de protocolo de comunicación. Se trata del conjunto de pautas que

posibilitan que distintos elementos que forman parte de un sistema establezcan comunicaciones entre sí, intercambiando información.

Un protocolo en Internet es una serie de reglas que siguen los ordenadores en Internet para que puedan comunicarse entre ellos.

Los protocolos de comunicación en Internet más importantes son TCP (cuyas siglas pueden traducirse como Protocolo de Control de Transmisión) e IP (Protocolo de Internet). Su acción conjunta (TCP/IP) posibilita el enlace entre todos los equipos que acceden a la red.

Otro protocolo importante es el protocolo de comunicación de Internet o IP, cuya función es permitir la comunicación en dos direcciones, en destino u origen, para que sea posible la transmisión de datos.

Otros ejemplos de protocolos de Internet son el protocolo HTTP (Hypertext Transfer Protocol) que es un conjunto de reglas para construir y compartir páginas web. La creación de HTTP llevó a la World Wide Web, lo que conocemos como Internet.

El protocolo SMTP (Simple Mail Transfer Protocol) es una serie de reglas para enviar mensajes por Internet. La creación de SMTP posibilitó el envío de emails.

Pero ¿quién es el propietario de estos protocolos de Internet?

Nadie es el propietario de un protocolo. Los protocolos de Internet son herramientas que puedan ser utilizadas de muchas maneras y son inventados para ser estándares útiles. Protocolos como TCP/IP, HTTP o SMTP han posibilitado la creación del Internet de la Información siendo la base del éxito de empresas como Twitter, Google, Facebook, entre muchas otras. Sin la existencia de estos

protocolos previos y su correcto empleo ninguna de las citadas empresas hubiera podido desarrollar su modelo de negocio.

Uno de los protocolos tecnológicos más conocidos por el público en general es BitTorrent, que se emplea para compartir contenidos de forma descentralizada, como música, libros o películas.

BitTorrent se configura sobre un sistema descentralizado entre iguales o P2P (Peer-to-Peer), permitiendo el intercambio directo de contenidos entre ordenadores sin necesidad de contar con un intermediario de confianza, papel que sí encontramos en plataformas como Netflix, que cuentan con un servidor central.

El Protocolo de Control de Transmisión o TCP es uno de los elementos esenciales de Internet. Fuente: techeek en Pixabay.

La innovación que ha proporcionado el protocolo Bitcoin es la combinación de la tecnología P2P y la criptografía. Esta combinación de tecnologías, junto a la estructura de

incentivos de tokens o criptomonedas (bitcoins, Ethers, etc.), fomenta la participación y la utilización en estos protocolos, revolucionando el hasta entonces aburrido mundo de los protocolos, posibilitado además que una comunidad de inversores globales invierta en ellos, democratizando la financiación y el desarrollo de tales protocolos abiertos. Esta circunstancia ha inspirado a muchos otros emprendedores para desarrollar aplicaciones sobre esta nueva base y crear nuevos protocolos que funcionan en un mundo descentralizado.

Bitcoin está vertebrado por su tecnología de cadena de bloques o blockchain, que utiliza en sus procesos un protocolo abierto para compartir contenidos de forma descentralizada, diseñado para intercambiar archivos entre iguales o P2P en Internet, en el cual una red de ordenadores o también denominados nodos se comportan como iguales entre sí, actuando al mismo tiempo como clientes o servidores con respecto a los demás nodos de la red, permitiendo el intercambio directo de información en cualquier formato, entre los equipos interconectados.

Para poder emplear el protocolo Bitcoin se necesita de la criptomoneda y unidad de cuenta bitcoin. Aclaremos ahora una confusión muy habitual, ya que el protocolo se escribe Bitcoin con «B» mayúscula y la unidad de cuenta que se usa en el protocolo Bitcoin se escribe con «b» minúscula o bitcoin.

La unidad de cuenta bitcoin se llama criptomoneda, porque la visión del creador del protocolo Bitcoin era crear un sistema de pagos descentralizado gestionado por una comunidad, sin la necesidad de contar con una entidad central que hiciera las funciones de banco central.

4

¿Encontramos implementada la teoría de juegos en las criptomonedas?

La teoría de juegos es una rama de la economía que estudia las decisiones en las que para que un individuo tenga éxito tiene que tener en cuenta las decisiones tomadas por el resto de los agentes que intervienen en la situación. Esta teoría se centra en estudiar cómo se relaciona un sistema económico con la conducta de un individuo. Específicamente en los casos en los que los costes y beneficios no están fijados de antemano, sino que dependen de terceros.

En teoría de juegos no tenemos que preguntarnos qué vamos a hacer, tenemos que preguntarnos qué vamos a hacer teniendo en cuenta lo que pensamos que harán los demás, ellos actuarán pensando según crean que van a ser nuestras actuaciones.

Los estudios manejados por la teoría de juegos, permiten comprender de mejor manera cómo la cooperación o el individualismo pueden afectar a un sistema económico. Estos son aspectos de gran importancia en medio de un mundo cada vez más interconectado y de economías más interdependientes. Pero no solo eso, la teoría de juegos y sus análisis van mucho más allá como lo veremos a continuación.

En el año de 1928, el famoso matemático John von Neumann publicó una serie de trabajos sobre la teoría de juegos. Estos fueron el génesis de la teoría y una de las contribuciones más importantes de Neumann. Sin

embargo, la teoría de juegos comenzó a tener mayor relevancia tras el desarrollo del denominado *equilibrio de Nash*.

En relación al equilibrio de Nash este se alcanza en una situación en la que ninguno de los jugadores en un juego en el que hay dos o más jugadores, todos conocen los equilibrios de los demás, quieren cambiar unilateralmente su decisión porque cambiarla supondría empeorar su condición. Cuando todos los jugadores han tomado una decisión y no pueden cambiarla sin empeorar su bienestar, se considera que se ha alcanzado un equilibrio de Nash.

El equilibrio de Nash se ha utilizado para regular situaciones de competencia entre empresas y diseñar subastas de adjudicaciones públicas. Una legislación que tenga en cuenta el equilibrio de Nash puede evitar oligopolios, por eso en la legislación antimonopolio se suelen buscar formas de evitar que se pacten precios entre las partes implicadas.

Gracias a la teoría de juegos, es posible la existencia de la tecnología blockchain. Esa teoría utiliza dicha tecnología para conseguir que los «jugadores o mineros» puedan garantizar la seguridad de la red en todo momento.

El mejor ejemplo de empleo de la teoría de juegos lo encontramos en el protocolo de consenso de Prueba de Trabajo o *Proof of Work* (PoF), donde los mineros participan en un juego llamado «minería y confirmación de transacciones», cuyo objetivo es tomar las transacciones, procesarlas, verificarlas y decir que todo está correcto. Para conseguirlo, los mineros hacen uso de un equipamiento informático muy avanzado y de una sofisticada criptografía para verificar los datos. En el juego, cada minero toma una decisión y dicha decisión luego es verificada y respetada por el resto. Al final del juego, se logra el objetivo: garantizar que las transacciones de la red se realicen, sean seguras y que no perjudiquen al sistema.

La vida de John Forbes Nash Jr. quedó plasmada en la película de 2001 «Una mente maravillosa», ganadora de cuatro Premios Óscar, entre ellos el de Mejor Película. Fuente: WorldSpectrum en Pixabay.

Con esto se ha conseguido dar solución a un dilema habitual en seguridad informática para sistemas descentralizados conocido como el problema de los generales bizantinos, tema clásico en redes distribuidas como Bitcoin y otras criptomonedas.

El problema de los generales bizantinos es un experimento mental creado para ilustrar el dilema de lograr un consenso entre un conjunto de entidades con un objetivo común, pero donde existen saboteadores que buscan dinamitar todo el proceso. Además, se supone que las comunicaciones entre ellos son limitadas e inseguras.

El problema se presenta como una analogía con un escenario de guerra, donde un grupo de generales bizantinos se encuentran acampados con sus tropas alrededor de una ciudad enemiga que desean atacar.

Por ejemplo, supongamos un posible escenario de guerra en el que un grupo de generales bizantinos están asediando una ciudad desde distintos lugares y tienen que acordar entre ellos cómo proceder de forma coordinada.

Entre estos generales, solo hay uno que puede cursar la orden por ser el comandante. Además, dichos generales se comunican únicamente a través de mensajeros y las dos posibles órdenes del comandante son la de atacar o la de retirarse. Después de observar el comportamiento del enemigo, los generales deben comunicar sus observaciones y ponerse de acuerdo en un plan común de guerra que permita atacar la ciudad y ganar la contienda.

Además, existe la posibilidad de que algunos generales sean traidores y de que envíen mensajes con información errónea con el propósito de confundir a los generales leales. Un algoritmo que solucione este problema debe asegurar que todos los generales leales acuerden un mismo plan de acción y que unos pocos traidores no puedan conseguir su objetivo. Pues bien, uno de los grandes logros que supone Bitcoin es el hecho de ofrecer la primera solución práctica a este problema de los generales bizantinos.

La prueba de trabajo o *Proof of Work* es el algoritmo de consenso original en una red de blockchain. En la cadena de bloques, este algoritmo se emplea para confirmar transacciones y producir nuevos bloques. Con la prueba de trabajo, los mineros compiten entre ellos para completar transacciones en la red y obtener recompensas.

5

¿LA ESCASEZ DIGITAL DEFINE A LAS CRIPTOMONEDAS?

Inicialmente, trataremos de explicar el concepto de «escasez» en el ámbito de la economía para posteriormente proceder a aplicarla al ámbito de las criptomonedas y blockchain.

El principio de escasez, en economía, señala que los recursos son insuficientes para producir todos los bienes y servicios para satisfacer las necesidades de las personas. De esta forma, no es posible satisfacer todas las necesidades y siempre tendremos que elegir entre varias alternativas en las que queremos gastar nuestros recursos.

Son las características de la demanda las que contribuyen a definir la escasez de un recurso, donde su carencia no está definida por su cantidad, sino que responde a una situación en que la demanda futura esperada supera la oferta prevista, dándose una situación de superávit en el recurso en cuestión. Las causas son:

- Incremento de la demanda.
- Disminución o agotamiento de fuentes y/o recursos.

Si nos hiciéramos la siguiente pregunta: ¿cuánto puede valer un activo digital que puede ser fácilmente duplicado y del que puede haber una existencia infinita? La verdad es que un activo así valdría muy poco o prácticamente nada, porque sería fácil de acumular y crear.

Por ejemplo, un escritor puede crear un libro digital y en principio vender dicho libro a un precio de 3 euros. Pero una vez que el recurso comience a copiarse de forma descontrolada este empieza a perder valor. Al final, existirán tantas copias del mismo que el valor teórico del libro sería 0 euros. Una situación poco favorable para el autor que podría ver su esfuerzo sin retribuir por culpa de la «abundancia digital».

Con la llegada de Internet se ha ido desarrollando un fenómeno denominado Abundancia Digital, el cual hace referencia a la facilidad de la que gozan los usuarios de Internet al poder acceder a contenidos casi ilimitadamente, generándose una percepción de que el coste de almacenar y transferir datos es casi cero, aunque la verdad es que sí existe un coste de producción para autores y empresas y, en lo que respecta a la piratería de contenidos digitales en Internet, esto nos lleva al concepto que nos ocupa: la Escasez digital.

La escasez digital hace referencia al control sobre la abundancia y existencia de activos o recursos digitales. Tal escasez digital se ha intentado con escaso éxito en el ámbito de la lucha contra la piratería, pero fue Bitcoin y su tecnología de cadena de bloques o blockchain quienes lo consiguieron con notable éxito debido a la oferta limitada de criptomonedas, gracias a la imposibilidad de duplicar, falsificar y gastar dos veces las criptomonedas.

Para poder explicar lo positivo de la escasez, un buen ejemplo sería el dinero fiduciario, como el euro, el yen, el dólar estadounidense, etc. Por lo general, el dinero fíat tiene una existencia limitada ya que lo normal es que los bancos centrales no impriman infinitas cantidades de dinero, aunque podrían llegar a hacerlo desgraciadamente. La razón para ello es muy sencilla: imprimir infinitas cantidades de dinero lleva a que este pierda valor.

Pues bien, este mismo principio se aplica también en el mundo digital y lo hemos comprobado en Bitcoin, por ejemplo. La escasez o limitada existencia de bitcoins ayuda a que la criptomoneda se revalorice y mantenga en todo momento un valor positivo frente a cualquier situación.

El padre de Bitcoin, el anónimo Satoshi Nakamoto, destacó que la criptomoneda tendría una existencia limitada de un total de 21 millones de criptomonedas. De