Módulo 1. Introducción al blockchain y las criptomonedas

Introducción

Vivimos en una época de revolución, como seguramente habrás oído tantas veces. "Blockchain es una tecnología revolucionaria", "lo cambiará todo", etc. Pero creo que la mayoría de nosotros no somos conscientes de hasta qué punto el blockchain está cambiando el mundo.

Este curso, "El futuro de las criptomonedas y el deporte", te ayudará a comprender e investigar cómo funciona la tecnología blockchain, y lo que significa en el mundo de los videojuegos, los deportes y el fútbol. Esperamos que aprendas algo nuevo, que este curso te aporte una nueva perspectiva sobre la tecnología blockchain y que te permita comprender en profundidad las revolucionarias implicaciones que esta tecnología entraña.

¿Qué es el blockchain?

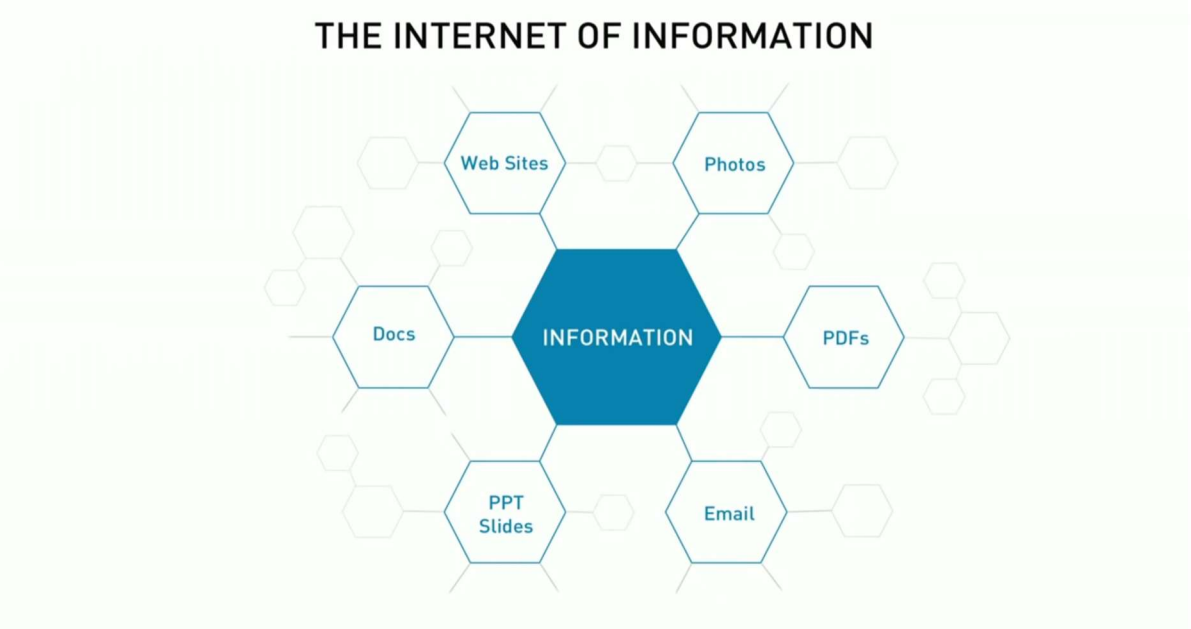
Internet, la red de la información

Mucha gente hace que el blockchain suene más complicado de lo que realmente es. Es cierto que su aspecto técnico puede complicarse muy rápidamente, pero no necesitamos entrar en todo eso todavía.

Para entender el blockchain, resulta útil pensar en cómo funciona Internet en primer lugar, y qué hemos hecho con ello durante los últimos 30 años. Hasta que nació el blockchain, Internet era una red de información. Era sólo eso, una red en la que cualquiera podía compartir información con el mundo, y obtener información a cambio. Esto no implica que esta innovación no sea algo importante: como sabes, cambió el mundo para siempre.

De repente, la información se hizo omnipresente, fácil de intercambiar y prácticamente gratuita. Sin embargo, hay un aspecto de esta red de información que tenemos que considerar porque es crucial para entender el concepto de blockchain. Internet comparte información haciendo copias de ella.

Figura 1: Internet, la red de la información



Fuente: Tapscott, 2016, https://bit.ly/3tyOMqK

The internet of information	Internet, la red de la información
Web site	Sitio web
Photos	Fotos
Pdf's	PDF
Docs	Documento
Email	Email
Ppt slides	Presentaciones de PPT
Information	Información

Tomemos como ejemplo un correo electrónico. Cuando envías un correo electrónico, no envías el propio correo. El destinatario recibe una copia de ese correo, y tú también guardas una copia del correo en tu carpeta de "Enviados". Así que, en realidad, ahora hay dos correos electrónicos. Y si el receptor responde, se hace otra copia. Si la conversación continúa, al final habrá tantas copias del correo electrónico original que no podrás seguirles la pista. Lo mismo ocurre con las descargas, como por ejemplo, las películas. No se descarga la película en sí, se descarga una copia de la película, o de una canción, o de un libro. Si subes una foto a las redes sociales, no subes la foto en sí, sino una copia de la

foto. Sigues teniendo la foto en tu teléfono. Y así es como funciona Internet. Es una red de información que transmite copias de información libremente distribuidas.

Esto no suele ser un problema para los correos electrónicos, los medios de comunicación o los sitios web. Pero supongamos que quieres enviar 100 dólares a través de Internet. Es sumamente importante que no envíes una copia. Cuando envías dinero a alguien, la otra persona recibe 100 dólares y tú pierdes 100 dólares. Si conservara una copia de esos 100 dólares en mi carpeta de "enviados", podría volver a gastar esos 100 dólares. Es lo que se conoce como "doble gasto", y tradicionalmente se ha resuelto proponiendo una tercera entidad que pasara por alto las transacciones. Volveremos sobre esta idea más adelante.

Blockchain, la red de los activos

Hemos establecido que, hasta que surgió el blockchain, Internet era una red de información, que se distribuía a través de Internet mediante copias. Pero ahora Internet está experimentando una profunda transformación y está entrando en una nueva era: la Internet de los activos digitales. Seguro has oído hablar de criptomonedas, tokens, NFT o activos digitales. Todos ellos son términos nuevos que se refieren a un tipo de propiedad totalmente nueva: la propiedad digital. La tecnología Blockchain es la columna vertebral de este nuevo sistema de propiedad, que permite llevar un registro de quién posee qué, sin necesidad de terceros ni entidades centralizadas.

El problema del doble gasto

Antes de que naciera blockchain, si querías gastar dinero online, tenías que hacerlo a través de un banco o algún tipo de sistema de pago institucional en el que pudieras confiar. No podías enviar dinero en efectivo a través de tu dispositivo, así que confiabas en alguna institución importante para que gestionara tus pagos.

Todo ello, para evitar el famoso problema del doble gasto (Rhodes, 2022), como ya hemos mencionado. Hay que asegurarse de que cuando alguien utilice su dinero, no pueda seguir utilizándolo una y otra vez. Por tanto, se necesita una autoridad central que lleve la cuenta de todos los pagos que se realizan en el mercado. Esto garantiza que cuando pagas 20 dólares, el receptor recibe 20 dólares y tú pierdes 20 dólares. Esta autoridad central puede ser un banco o cualquier otra entidad en la que confíen tanto el comprador como el vendedor, o el emisor y el receptor. Es necesario confiar en la autoridad central para realizar la transacción. Si no hay confianza, con el tiempo se dejará de realizar transacciones. Tradicionalmente, los bancos llevan la cuenta de cuánto dinero tiene, gasta o recibe cada persona.

En general, es una buena solución contar con terceros que lleven la cuenta del dinero, y es lo que nos permite gastar y recibir dinero sin mayores inconvenientes. Pero esto no está exento de inconvenientes.

El más importante es que los bancos e instituciones financieras que llevan el control del dinero representan un único punto de falla. Si falla el banco, falla toda la red, y no hay copia de seguridad ni una segunda opción para seguir utilizando la red de forma segura. Básicamente, si falla el nódulo central de la red, falla toda la red. En consecuencia, los bancos son objetivos muy vulnerables a robos y ataques de hackers. Por eso la seguridad en los bancos es tan estricta.

Otra inquietud importante es que la red depende de los bancos y, por tanto, tenemos que confiar en ellos. Pero las personas que dirigen los bancos son humanas y están expuestas a todos los defectos humanos que existen, como el resto de nosotros. No faltan ejemplos de bancos e instituciones que cometen errores garrafales, y eso generalmente se traduce en pérdidas de dinero para la gente común, a veces mucho dinero.

Cómo nació blockchain

En 2008, alguien llamado Satoshi Nakamoto propuso una nueva solución a este dilema del doble gasto. Aún hoy se desconoce quién es Satoshi Nakamoto, si se trata de una persona, un hombre o una mujer, o un grupo de personas, estadounidenses, europeas o japonesas. No se sabe nada de Satoshi, pero lo que se publicó con ese nombre inició una revolución.

Con el título "Bitcoin: a peer-to-peer electronic cash system" (Bitcoin: un sistema de dinero electrónico entre pares), Satoshi Nakamoto propuso un sistema que podía gestionar pagos en línea sin necesidad de terceros ni autoridades centrales como bancos o gobiernos. El "libro blanco del bitcoin", como se conoce hoy en día, sugería una red descentralizada que podría utilizarse para transferir dinero entre dos nodos, sin riesgo de doble gasto y sin un único punto de falla.

Recordemos que en 2008 el mundo se enfrentaba a una de las peores crisis económicas de la historia, sin duda la más grave desde el colapso del 29. Y los responsables detrás de esta crisis masiva (que, en aquel momento, parecía el apocalipsis) fueron, lo adivinaste, los bancos. El repentino estallido de una burbuja inmobiliaria producida por los préstamos indiscriminados concedidos por los bancos acabó con millones de personas desempleadas y un enorme rescate gubernamental que pasó a la historia. Por eso muchos consideran a Bitcoin como el resultado de la crisis, un producto de la ira y la falta de confianza que inspiraban los bancos en aquel momento (Winklevoss y Winklevoss, 2021).

Otra cuestión contra la que Bitcoin se posiciona es la política monetaria irresponsable. Durante 2008, los bancos recibieron un gran rescate por parte del gobierno estadounidense para evitar la bancarrota. Ese dinero fue emitido a voluntad por el estado. La impresión de dinero es un gran debate entre los economistas, y la mayoría de los de tendencia ortodoxa aseguran que la emisión de dinero por parte del gobierno sin el

respaldo adecuado conduce a una devaluación de la moneda. Bitcoin entra claramente en esta categoría: una cantidad restringida de Bitcoin es lo que dará valor a la moneda. Por esta razón, sólo se emitirán 21 millones de bitcoins en toda la historia. Está escrito en el código de la propia Blockchain, y el último Bitcoin se emitirá en el año 2140. Nunca habrá más de 21 millones de bitcoins, y esa escasez es lo que la hace valiosa y muy demandada.

Pero, ¿cómo funciona?

Básicamente, la cadena de bloques ("blockchain") es una red de computadoras que mantiene un registro de todas las transacciones que se realizan en ella. La cadena de bloques de Bitcoin, por ejemplo, registra todas las transacciones de Bitcoin del mundo. La cadena de bloques de Ethereum, por otro lado, registra todas las transacciones de Ether (la moneda nativa de la cadena de bloques de Ethereum) y todas las transacciones que tienen lugar dentro de un contrato inteligente en la cadena de bloques de Ethereum. Veremos (mucho) más sobre este tema más adelante. Bitcoin es el ejemplo más sencillo, así que vamos a centrarnos en él.

Imaginemos una red de computadoras. Cada computadora es un nodo en la cadena de bloques de Bitcoin. En cada una de esas computadoras hay una copia de un registro. Ese registro contiene todas las transacciones de la cadena de bloques de Bitcoin escritas en él.

Así, supongamos que el Nodo A de la red quiere enviar Bitcoin al Nodo B. Toda la red sabe cuánto Bitcoin tiene el Nodo A y cuánto envía al Nodo B. Imaginemos que el Nodo A envía un Bitcoin al Nodo B.

Lo que ocurre a continuación es que cada computadora de la red actualiza el registro (generalmente llamado ledger o libro mayor), de modo que todos los miembros de la red saben que el Nodo A le dio un Bitcoin al Nodo B. El Nodo A ya no tiene derecho sobre el Bitcoin que acaba de enviar, ahora la propiedad de ese Bitcoin pertenece al Nodo B, y toda la red lo sabe.

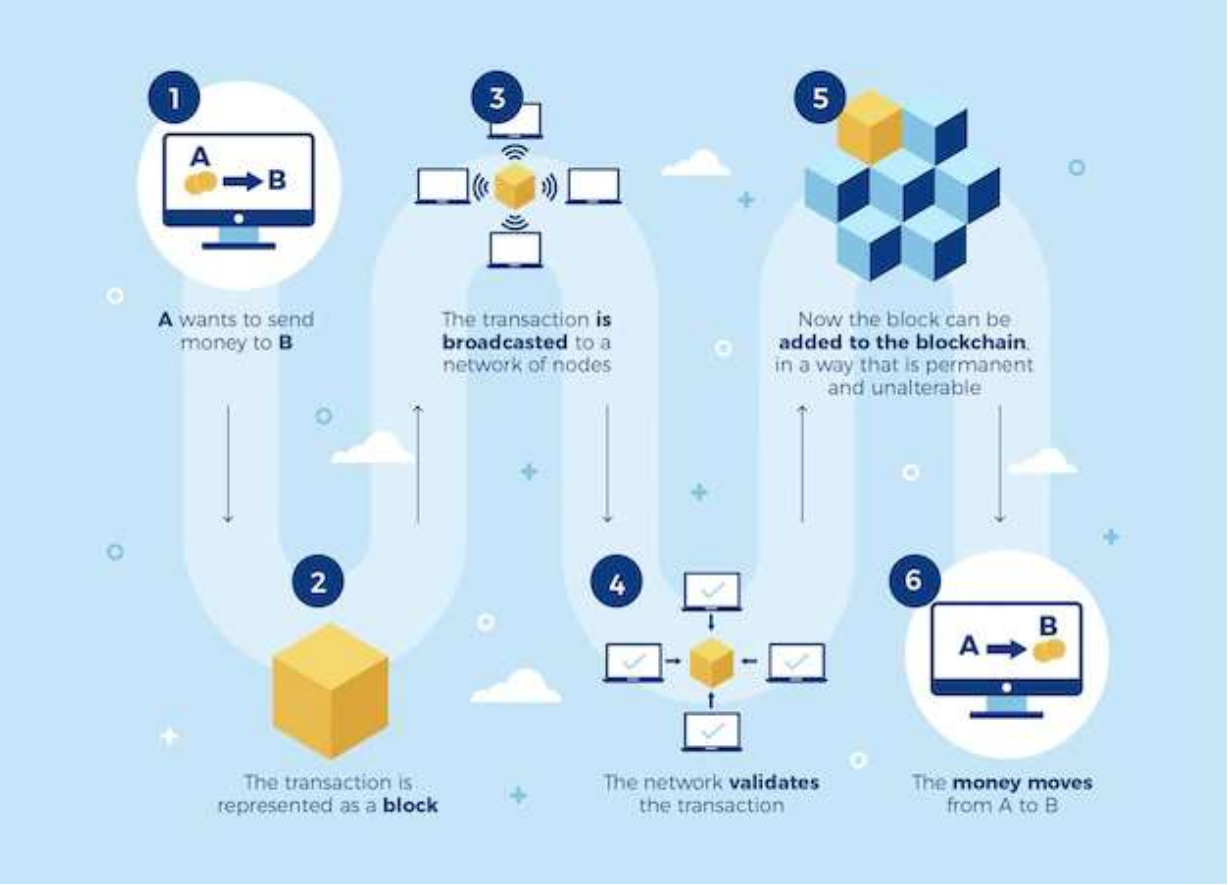
El truco aquí es que no hay un único libro mayor, o un único registro, que esté siendo supervisado por una institución central, o un banco. Existen muchas copias de ese mismo registro guardadas en muchas computadoras y actualizadas en tiempo real por cada computadora de la red cada vez que se realiza una transacción. Por supuesto, las computadoras de la red hablan entre sí y verifican que todas tengan la misma información. Así, si el Nodo A envía un Bitcoin al Nodo B, la transacción sólo se liquida una vez que todas las computadoras de la red están de acuerdo en que se está realizando la transacción, y la copia del registro se actualiza en cada computadora.

El registro es el mismo en cada computadora que pertenece a la red, y cada cambio, por mínimo que sea, se actualiza en toda la red, es decir, cada registro actualiza su información.

Entender cómo funciona realmente el mecanismo blockchain puede resultar complicado y requiere cierta reflexión. Por supuesto, lleva su tiempo. Puedes reforzar tu aprendizaje con el vídeo "Bitcoin: How Cryptocurrencies Work", de SciShow. Explica blockchain en detalle y de una manera impresionante.

Fuente: SciShow. (21 de diciembre de 2016). *Bitcoin: How Cryptocurrencies Work* [Video]. YouTube. https://www.youtube.com/watch?v=kubGCSj5y3k

Figura 2: Infografía de Blockchain



Fuente: [Imagen en línea de blockchain infographic], (2021), https://bit.ly/3tyDZNh

A Wants to send money to B	A quiere enviar dinero a B
The transaction is broadcasted to a network of nodes	La transacción se transmite a una red de nodos
Now the block can be added to the blockchain in a way that is permanent and unalterable	Ahora el bloque puede añadirse a la cadena de bloques de forma permanente e inalterable

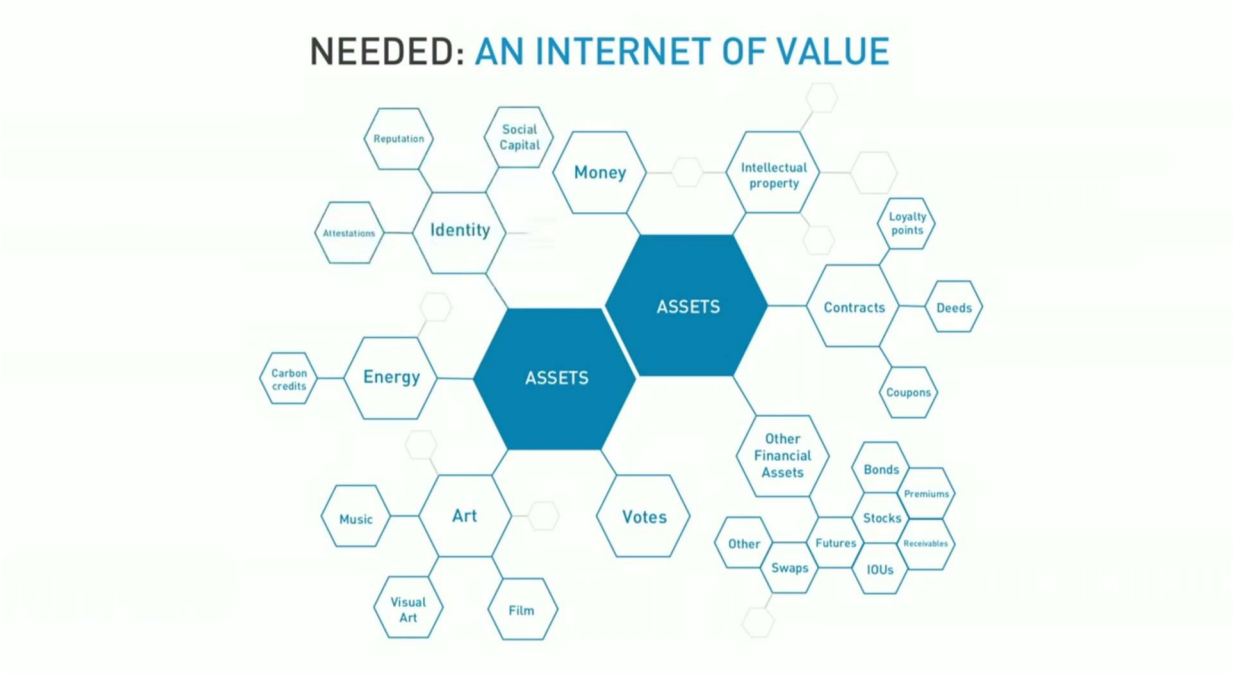
The transaction is represented as a block	La transacción se representa como un bloque
The network validates the transaction	La red valida la transacción
The money moves from A to B	El dinero pasa de A a B

Nacen los activos digitales

Esta es una palabra que oirás mucho en el mundo de blockchain. Como mencionamos antes, Internet solía ser una red de información, donde las copias de información se distribuían libremente y sin fin. Con el nacimiento de blockchain, Internet se ha convertido en una red de activos, en la que podemos intercambiar no sólo valores, sino también propiedades. Gracias a blockchain, podemos transferir activos de un usuario a otro, sin necesidad de intermediarios, en un entorno sin permisos ni confianza.

Cuando se piensa en activos digitales, probablemente lo primero que viene a la mente son las criptomonedas. Y sí, por supuesto, las criptomonedas son activos digitales, y los más destacados. Pero hay muchos tipos de activos que pueden intercambiarse a través de la cadena de bloques. Piensa en activos financieros como bonos, acciones, futuros o contratos, propiedad intelectual, identificaciones digitales, cupones o puntos por fidelidad, créditos de carbono e incluso arte, como música, imágenes y películas. La lista es interminable.

Figura 3: Internet, la red de los valores



Fuente: Tapscott, 2016, https://bit.ly/3tyOMqK

Needed: an internet of value	Se necesita: Internet, la red de los valores
Reputation	Reputación
Social capital	Capital social
Identity	Identidad
Attestations	Certificados
Carbon credits	Créditos de carbono
Energy	Energía
Art	Arte
Music	Música
Visual art	Arte visual
Film	Películas
Votes	Votos
Other	Otros
Swaps	Canjes
Futures	Futuros
IOUs	IOUs
Stocks	Acciones
Receivables	Créditos
Premiums	Premiums
Bonds	Bonos
Other financial assets	Otros activos financieros
Coupons	Cupones
Contracts	Contratos
Deeds	Escrituras
Loyalty points	Puntos por fidelidad
Intellectual property	Propiedad intelectual
Money	Dinero
Assets	Bienes

¿Qué es un bloque? ¿Por qué se llama Blockchain (cadena de bloques)?

Aún no hemos hablado de cómo se estructura una cadena de bloques. Hemos dicho que la blockchain es una red de computadoras que registran todas las transacciones de la red. Pues bien, este registro se realiza mediante un complejo conjunto de problemas matemáticos (en los que interviene un algoritmo criptográfico de alta gama llamado SHA-256, desarrollado por la NSA a principios de la década del 2000). Todas las computadoras de la red compiten entre sí con la esperanza de ser la primera en resolver el problema. Cuando una computadora resuelve el problema (un problema cada 10 minutos, aproximadamente), sella un bloque.

Un bloque es básicamente una lista de todas las transacciones que han tenido lugar en los últimos 10 minutos en la red. Ese bloque está codificado criptográficamente (por lo tanto, es seguro y anónimo) y tiene un sello de tiempo (para que todo el mundo sepa cuándo se produjeron esas transacciones). Cuando una computadora resuelve el

problema matemático, "sella" el bloque, es decir, se establecen las transacciones dentro de ese bloque, se marca la hora y, aquí está la parte importante, se difunde a todos los nodos de la red. Así, cada computadora recibe el último bloque, y ahora cada nodo conoce las transacciones de los últimos 10 minutos.
Cada vez que se crea un bloque, se añade a una cadena de bloques. Desde el nacimiento de Bitcoin, cada transacción se registra en estos bloques, que están conectados entre sí. El último bloque está conectado con el anterior, y éste con el anterior, y así sucesivamente. Cada transacción en la historia de Bitcoin ha sido registrada en estos bloques y vinculada a los bloques anteriores, por lo que realmente se puede ver cómo se realizaron las transacciones hasta el principio de la historia de Bitcoin. El primer bloque, llamado "bloque génesis", está disponible y es público para que cualquiera pueda verlo y revisarlo, al igual que todos los demás bloques.

Esta cadena de bloques (o blockchain, de ahí su nombre), es almacenada y actualizada constantemente por cada computadora de la red. Y esto es crucial para asegurar la cadena de bloques, y es lo que hace que la cadena de bloques sea una de las formas más seguras de almacenar información. Imagina que quisieras hackear la red, y quisieras hacer creer a todo el mundo que has recibido 100 Bitcoins, cuando en realidad, no es así. Es realmente (quiero decir, realmente) difícil de hacer.

Tendrías que hackear un bloque en la blockchain y adjudicarte 100 Bitcoins que no te pertenecen. Pero no sólo un bloque, sino todos los bloques vinculados previamente a él, hasta el principio, y luego todos los bloques vinculados después de él. No sólo en una computadora, sino en cada computadora de la red (es decir, millones de computadoras a partir de ahora), simultáneamente. Y cada uno de los bloques asegurado con los más altos niveles de encriptación. Por eso es tan difícil.

Una nota al margen, que no es esencial, pero que es útil saber, ya que probablemente te encuentres en algún momento con el término "ataque del 51%". Esto significa que, técnicamente, toda la red podría verse comprometida si al menos el 51% de las computadoras son hackeadas, ya que se basa en un protocolo de consenso y si más de la mitad de las computadoras están de acuerdo en que algo sucedió, entonces el resto de la red tendría que aceptarlo, incluso si no son hackeadas. Pensemos en el Congreso. Sólo basta con que el 51% de los miembros del Congreso estén de acuerdo en algo para que se apruebe una ley. Lo mismo ocurre con Blockchain. Aun así, sería prácticamente imposible comprometer ni siquiera el 51% de la red, debido a su gran tamaño y a que crece día a día. Un ataque al 51% de, por ejemplo, la cadena de bloques de Bitcoin, requeriría una enorme cantidad de potencia computacional.

Por el momento, la única forma concebible de (tal vez) conseguir esa cantidad de potencia computacional, es con las computadoras cuánticas. Y la computación cuántica, aunque promete aumentar exponencialmente la potencia de las computadoras, aún se encuentra en una fase temprana y experimental de desarrollo. Incluso si la computación cuántica

irrumpiese en escena, la mayoría de los entusiastas de las criptomonedas coinciden en que, una vez que esa tecnología esté disponible, también podría aplicarse para reforzar la tecnología blockchain y, de este modo, hacerla incluso resistente a la computación cuántica (McShane, 2021).

¿Qué son los mineros? ¿Es cierto que consumen mucha energía?

Seguro has oído hablar de los "mineros" cientos de veces. Que consumen mucha energía, que están prohibidos en China y que ganan mucho dinero. Pero, ¿qué es un minero?

Hasta ahora, nos hemos estado refiriendo a blockchain como una "red de computadoras" que lleva la cuenta de las transacciones que tienen lugar en la red. De hecho, es cierto que es una red de computadoras, pero no deberías pensar en ellas como computadoras personales, o algo que normalmente verías en tu vida diaria. Al principio, cuando Bitcoin era una red pequeña, funcionaba a través de computadoras personales. A medida que la red se fue ampliando, el manejo de tantos números y el seguimiento de las transacciones se hizo cada vez más difícil y costoso a nivel energético. Así que se tuvo que recurrir a computadoras más específicas. Lo que tenemos hoy son pequeños dispositivos construidos específicamente para minar criptomonedas. Están construidos únicamente para ejecutar los complejos problemas matemáticos que mencionábamos antes y que eran parte integral del funcionamiento de blockchain. Parecen pequeños discos duros y tienen que ser apilados uno sobre otro, ya que uno solo no haría casi nada, y hay que tener un gran equipo de minería para ver algún beneficio significativo.

Así que, en esencia, eso son los mineros: las personas que poseen estas computadoras que se encargan de hacer funcionar la red Bitcoin a través de complejos cálculos matemáticos. Las computadoras se llaman equipos de minería y sus propietarios son los mineros.

Ser minero puede ser muy rentable. Ellos reciben los bitcoins recién emitidos que produce la red. Cada vez que se realiza una transacción en la red, ésta plantea un problema matemático a los mineros para que corroboren y certifiquen la transacción en un bloque. El primer minero que lo hace es recompensado por la red, que le entrega bitcoins nuevos (Hong, 2022).

Al principio, como la red era diminuta, el número de transacciones era pequeño, lo que significa que eran fáciles de corroborar, por lo que la minería era fácil. Ahora, se necesita un procesamiento mucho mayor, ya que la red ha crecido mucho, y una pequeña computadora de minería ciertamente no es suficiente para resolver los complejos cálculos que requiere la red. Los mineros se agrupan en lo que se conoce como "pools de minería", lo que aumenta sus posibilidades de ser el primer grupo en resolver los problemas matemáticos y repartirse la recompensa.

Además, a medida que crece el número de transacciones de Bitcoin y aumenta la complejidad de la minería, cada cuatro años se reduce a la mitad el número de bitcoins con que se recompensa a los mineros. Esto se conoce como "halving" (reducción a la mitad), y asegura que el número de bitcoins que se emiten a lo largo del tiempo disminuye, haciendo que el bitcoin sea más escaso y, por tanto, más valioso.

Los mineros también obtienen un porcentaje de Bitcoin al llevarse una comisión de cada transacción. Y en el futuro, cuando los 21 millones de bitcoins estén totalmente minados, obtendrán beneficios a través de las comisiones que se cobren por cada transacción de bitcoins.

Ejecutar todo el número de transacciones de Bitcoin cada día consume una enorme cantidad de energía. De hecho, los equipos mineros producen tanto calor que se sabe que algunos habitantes de los países nórdicos los utilizan como sistema de calefacción.

Éste es probablemente el principal argumento que plantean los detractores de Bitcoin para criticar esta nueva tecnología. En la actualidad, la red bitcoin consume tanta energía como un país pequeño, como el Líbano. Es una realidad innegable, pero eso no significa que no pueda mejorarse. No vamos a tratar este tema en este curso, ya que no es pertinente para nuestro objetivo. Pero debemos reconocer que Bitcoin utiliza una cantidad significativa de energía eléctrica, y también que podría ser la mayor oportunidad para acelerar la transición hacia un futuro energético sostenible. Una gran cantidad de la red Bitcoin funciona con energías renovables (algunas estimaciones aseguran que hasta el 75% de la red Bitcoin funciona con energía renovable) (Zmudzinski, 2019). Tiene sentido, ya que para maximizar los beneficios al minar Bitcoin, hay que mantener bajos los costos energéticos. Por lo tanto, Bitcoin genera un incentivo económico para utilizar energía sostenible.

¿Qué es la prueba de trabajo?

Normalmente abreviado como POW (proof-of-work) (Hertig, 2022), es el protocolo que asegura que cada bloque de la cadena tiene suficiente poder computacional para proporcionarle valor. Es el protocolo que proporciona el consenso detrás de la red.

Cada pago realizado en Bitcoin tiene que ser certificado, o corroborado, por los mineros. Como hemos visto, cada minero invierte cierta cantidad de energía (poder computacional para resolver problemas matemáticos) en hacer esto. Es difícil hacer funcionar la blockchain, los mineros tienen que "trabajar". Por eso cada Bitcoin está asegurado por el protocolo "proof-of-work". Si se ha realizado una transacción de Bitcoin, se puede estar seguro de que ha sido asegurada por el protocolo POW.

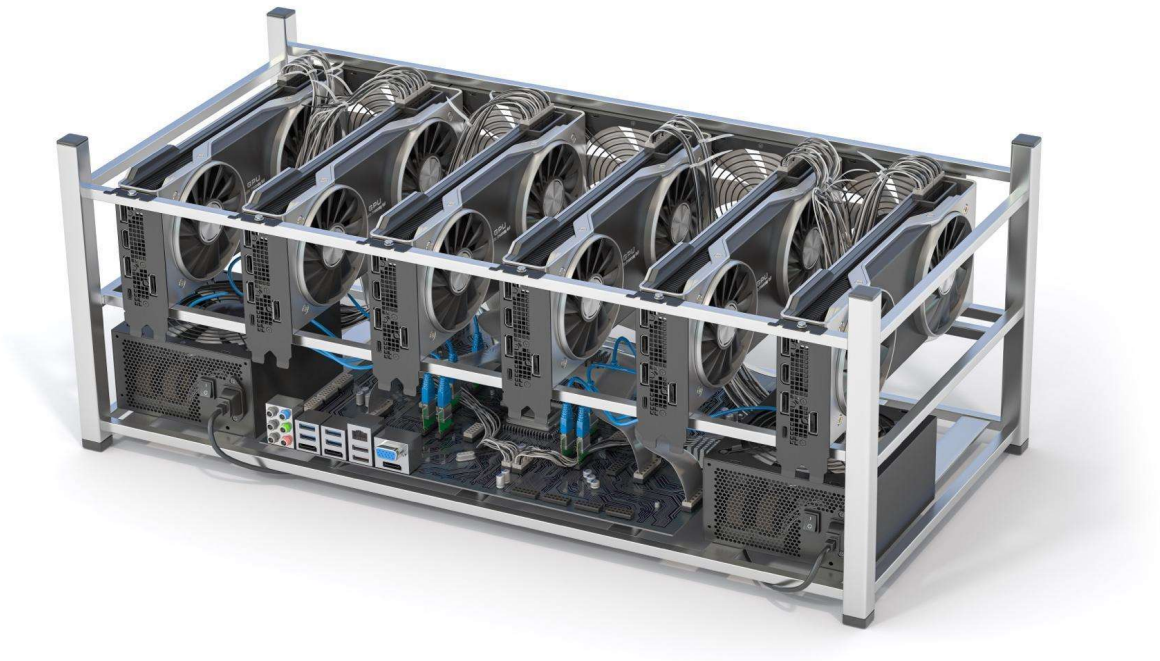
Además, si los Bitcoins fueran más fáciles de fabricar (o falsificar), el problema del doble gasto del que hablábamos antes no se solucionaría. En resumen, el proof-of-work es lo

que facilita la completa descentralización de la red y la no necesidad de un tercero controlador central o institución supervisora. Puedes ver este vídeo para obtener más información sobre la prueba de trabajo.
Hasta ahora, hemos utilizado los términos Blockchain y Bitcoin casi indistintamente. Sin embargo, Bitcoin es la criptomoneda y Blockchain es la tecnología que la hace posible. Ambos nacieron juntos. El libro blanco de Satoshi Nakamoto hablaba de Bitcoin, e implícitamente creaba esta nueva tecnología. Seguramente, para quien escribió el libro blanco, Bitcoin y Blockchain eran una misma cosa. Pero han pasado muchas cosas desde entonces. Y Satoshi inició una revolución. Muchos adoptaron su idea y la desarrollaron en numerosas aplicaciones. Así nacieron muchas blockchains, para otras criptomonedas, aparte de Bitcoin.

Fuente: Binance Academy. (22 de octubre de 2018). What is Proof of Work (PoW) – Explained for beginners [Video]. YouTube. https://www.youtube.com/watch?v=3EUAcxhuoU4&ab_channel=BinanceAcademy

Entre las demás blockchains que se crearon, hay una que es la más famosa, e igual de revolucionaria que Bitcoin, llamada blockchain Ethereum.

Figura 4: Blockchain Ethereum



Fuente: [Imagen en línea de *Ethereum blockchain*], (s.f.), https://bit.ly/3MM8m9X

¿Qué es Ethereum?

Ethereum es una cadena de bloques diferente a Bitcoin. Es una cadena de bloques independiente completamente nueva. Ethereum es el nombre de la cadena de bloques, y la moneda nativa se llama Ether. La blockchain también funciona con el protocolo proof-of-work, pero promete cambiar a un mecanismo de consenso diferente para 2023, llamado proof-of-stake, que será mucho más eficiente energéticamente y seguirá siendo seguro. Aunque ahora mismo no es significativo para nuestra comprensión del tema, es bueno saber que, a diferencia de la blockchain de Bitcoin, que ya está establecida y permanecerá así permanentemente, la blockchain de Ethereum está en constante desarrollo y ha mejorado significativamente.

Lo que sí tenemos que entender es que la blockchain de Ethereum introdujo un concepto asombroso llamado "contratos inteligentes". La idea de un contrato inteligente fue introducida por primera vez por un informático llamado Nick Szabo, que imaginó un contrato digital almacenado en un libro de contabilidad descentralizado como el que permite blockchain. Ethereum tiene su criptomoneda (Ether) como Bitcoin, pero también se puede usar para otras finalidades. Algunos la llaman "dinero programable", debido a los contratos inteligentes, que permiten escribir códigos en la cadena de bloques y conseguir que ejecute todo tipo de acciones.

¿Qué es un contrato inteligente?

Un contrato inteligente es básicamente un contrato que se autoejecuta. Es un acuerdo entre dos o más personas, una declaración escrita que garantiza que algo se haga. En el pasado, tenía que haber una tercera parte que se asegurara de que el contrato era respetado por todas las partes implicadas y, en caso contrario, habría consecuencias, ya fueran legales, financieras o de otro tipo.

En general, confiamos en el sistema judicial para asegurarnos de que se cumplan las condiciones de un contrato. Necesitamos abogados, escribanos, y en caso de que no se cumplan los contratos, que los jueces dicten sentencias, y que los gobiernos impongan multas y sanciones. Si pensamos no sólo en el sistema judicial, sino también en el financiero, el funcionamiento es similar. Exigimos a los bancos e instituciones que validen y supervisen las transacciones. Si queremos enviar dinero a otro país, deben llevarse a cabo cientos de procesos para lograr ese objetivo.

En cambio, con los contratos inteligentes, todo eso cambia. Lo que es especialmente llamativo de los contratos inteligentes de blockchain es que se puede escribir un contrato, traducirlo a código informático, y luego registrarlo en la blockchain (en este caso, la blockchain de Ethereum). Por lo tanto, al igual que en la blockchain de Bitcoin, cada uno de los nodos de la blockchain de Ethereum tendrá una copia del contrato y se asegurará de que éste se ejecute cuando se supone que debe hacerlo.

En palabras de Don Tapscott, presidente ejecutivo del Blockchain Research Institute, el sistema financiero es como una máquina de Rube Goldberg.

> Una máquina ridículamente compleja que hace algo muy sencillo como cascar un huevo o cerrar una puerta. Sinceramente, me recuerda un poco al sector de los servicios financieros. Usas tu tarjeta en una tienda y un pedido pasa por una docena de empresas, cada una con sus propios sistemas informáticos, algunos de ellos mainframes de los años 70, realmente antiguos (...) y tres días después, se produce una liquidación. Pues bien, con la industria financiera de blockchain, no habría liquidación, porque el pago y la liquidación es la misma actividad. Es sólo un cambio en el libro mayor. (Tapscott, 2016, https://bit.ly/3tyOMqK)

Figura 5: Máquina de Rube Goldberg

Fuente: Swartz, s.f, https://bit.ly/3Hmgsop

De hecho, un contrato inteligente de blockchain se ejecuta al instante. Y el hecho de que esté descentralizado, permite evitar cualquier manipulación por parte de terceros. Cada nodo de la cadena de bloques sabe cuándo y cómo tiene que funcionar el contrato. Una vez que el contrato está escrito en código en la blockchain, es inmutable. Por eso mucha

gente utiliza la frase "el código es ley", porque una vez creado el contrato inteligente, no hay vuelta atrás.

Así, por ejemplo, supongamos que una persona quiere prestar un bitcoin a otra. No tienen por qué conocerse. Sólo tienen que acordar las condiciones. "Te presto un Bitcoin, que tienes que devolver con este tipo de interés en esta fecha. Y si no lo devuelves, me quedaré con la garantía". Una vez que el contrato esté escrito en código (el lenguaje de código de Ethereum se llama Solidity), el resto se hará solo. Sin necesidad de abogados ni demandas.

Los contratos inteligentes dieron lugar a un sinnúmero de innovaciones

Puede parecer increíblemente sencillo, pero la creación de contratos inteligentes abrió todo un abanico de posibilidades. Si lo piensas, casi cualquier cosa puede establecerse como un contrato, no sólo los acuerdos financieros o legales. Por ejemplo, un juego es un contrato. Un conjunto de normas establecidas que hay que seguir o, de lo contrario, ocurre algo. Por otra parte, una organización, una empresa, incluso un gobierno o la constitución de un país son contratos. Seguramente puedes comenzar a comprender cómo un contrato inteligente puede tener implicaciones considerables, mucho más allá de las finanzas descentralizadas (que, en sí mismas, ya son una innovación gigantesca).

Así que, poco después de su creación, se empezaron a construir proyectos sobre la blockchain de Ethereum. Cada uno de estos proyectos se basa en un contrato inteligente específico escrito en código y, por tanto, inmutable. Dentro de estos contratos, se introducen muchas condiciones y reglas. Muchos contratos inteligentes incluyen incluso la creación de "tokens": criptoactivos digitales que pueden intercambiarse entre las partes que participan en el contrato inteligente (Cryptopedia Staff, 2021).

Al principio puede resultar útil pensar en los tokens como "monedas" que se construyen sobre otra "moneda". Aunque esto no es técnicamente exacto y muchos tokens no son necesariamente una "criptomoneda" en sí misma, podría ser más fácil pensar en los tokens de esta manera.

Los tokens digitales entonces son creados por desarrolladores (programadores) que escriben contratos inteligentes en la blockchain de Ethereum con ciertas reglas y condiciones que se establecen en el contrato, y por lo tanto, cada token tiene un uso y propósito específico. Y si su uso es realmente significativo, y se crea una demanda suficiente para un token específico, ese token sube de valor y puede venderse, comprarse o intercambiarse.

Desde la creación de los contratos inteligentes, ha habido una explosión absoluta de tokens disponibles para la compra. Muchas de las llamadas "criptomonedas" que ves y de

las que oyes hablar en todas partes, son en realidad tokens basados en Ethereum, como Solana, USDC y polygon.

Dapps y DAO

En un artículo, Vitalik Buterin (2014) expuso algunos de los temas más importantes que vamos a tratar a continuación, incluyendo contratos inteligentes, DAOs, Dapps, y más. Así que se recomienda encarecidamente la lectura de dicho artículo (publicado en la página oficial de la fundación Ethereum).

Como hemos señalado, los contratos inteligentes tienen implicaciones considerables. Todo se puede traducir como un contrato si se piensa en ello. Tomemos, por ejemplo, una aplicación en tu teléfono. Si quieres saber el tiempo, descargas una app que te da los datos de forma ordenada basándose en la información que das como datos de entrada. Así que, en teoría, lo único que ocurre es que tú haces algo y, como consecuencia, ocurre otra cosa, siguiendo unas reglas establecidas. Das tu ubicación y un plazo establecido, y la aplicación responde en consecuencia: tendrás este tiempo en los próximos días.

Así, cuando un contrato inteligente da lugar a una aplicación, se denomina Dapp, o aplicaciones descentralizadas. Tomemos, por ejemplo, la famosa plataforma de intercambio Uniswap. Lo que hace es facilitar el intercambio de criptomonedas entre usuarios (se conozcan o no, no importa, para eso tenemos un contrato inteligente). Un usuario tiene un token, y quiere venderlo. El contrato inteligente tiene escrito en su código un conjunto de reglas y condiciones establecidas que igualan al vendedor y al comprador, asegurándose de que ninguno de ellos tiene malas intenciones o que pueden incurrir en algún tipo de robo.

Algo a tener en cuenta es que las apps descentralizadas como Uniswap no tienen un centro de control centralizado, ni nadie que supervise lo que sucede. Funciona completamente por sí misma, es un cripto-mercado donde nadie tiene ningún control central. Así que asegúrate de no cometer ningún error porque no hay nadie a quien reclamar. Si querías vender 2 bitcoins, pero en lugar de eso vendiste 3, ya está, no hay vuelta atrás. Una vez establecido en la blockchain, se queda en la blockchain.

Otro uso fenomenal de los contratos inteligentes es la creación de DAO (Monolith, 2021), que significa organización autónoma descentralizada. Se trata de una organización dirigida por la comunidad en su conjunto, sin autoridad central. Por lo general, el contrato inteligente que establece una DAO, también crea sus propios tokens, utilizados para ejecutar y regular la DAO en lo que se conoce como "tokenomics". Ocasionalmente, cuando hay que tomar decisiones o realizar cambios en la DAO, quienes tienen voz y voto son quienes poseen tokens. Así, todo el que tenga un token puede participar en la regulación de la DAO.

Se puede ver cómo los contratos inteligentes no son sólo un acuerdo entre dos partes sobre la cantidad de Bitcoin que quieren prestar. Solo estamos viendo el principio de las posibilidades que ofrecen los contratos inteligentes. Si la aceptación aumenta, los contratos inteligentes empezarán a ser cada vez más frecuentes.

La increíble ventaja de tener contratos inteligentes es que preservan el anonimato del usuario, y además, son muy transparentes, ya que cualquiera puede ver en la blockchain lo que está ocurriendo. Nuestros datos están seguros, y nuestro dinero también, ya que estamos utilizando una red mucho más segura que el sistema bancario actual.

En los siguientes módulos profundizaremos en cómo está evolucionando el entorno blockchain, y cómo cada día se desarrollan nuevos e innovadores usos. Hace unos años, pensar en un mundo de juegos en 3D como Decentraland era absolutamente inimaginable. O la revolución NFT, que aunque muchos consideran una moda o una burbuja especulativa, puedo asegurar que tiene un potencial increíble, y que ha venido a redefinir lo que es la propiedad digital. Todo está cambiando muy deprisa, y ni siquiera hemos rozado la superficie. Puede resultar un poco difícil de entender, sobre todo al principio, pero estas nociones son esenciales para comprender cómo se desarrollará el futuro de blockchain.

Figura 6: Economía tradicional vs. Criptoeconomía

Fuente: [Imagen en línea], (s.f.), https://images.app.goo.gl/dyPeobtR9TuuYLV46

Traditional economy vs. crypto economy	Economía tradicional vs. Criptoeconomía
Economic agents	Agentes económicos
Money	Dinero
Productive assets	Activos productivos

Goods	Bienes
Exchange mechanisms	Mecanismos de intercambio
Institutions	Instituciones
Central banks Corporation Governments Households	Bancos centrales Corporaciones Gobiernos Hogares
Fiat (eg. Dollars, euro, yen)	Dinero fiat (por ejemplo, dólares, euros, yenes)
Factories Machines Software	Fábricas Máquinas Software
Food Clothing Cars Electronics	Comida Vestimenta Automóviles Electrónica
E-commerce Retail stores Stock market	Comercio electrónico Comercio minorista Mercado de valores
Governments Central Banks Corporations	Gobiernos Bancos centrales Corporaciones
Core developers Miners/validators Investors Entrepreneurs	Desarrolladores principales Mineros/validadores Inversores Empresarios
Fungible ERC20 tokens (ETH,DAI, etc)	Bienes fungibles Tokens ERC20 (ETH, DAI, etc.)
Smart contracts	Contratos inteligentes
NFTs	NFT
Decentralized exchanges Smart contracts	Exchanges descentralizados Contratos inteligentes
DAOs	DAO

Referencias

[Imagen en línea de blockchain infographic]. (2021). https://www.panel.es/wp-content/uploads/2021/09/343347-PAKDPD-299_low.jpg.webp

[Imagen en línea de Envato Elements]. (s.f.). https://elements.envato.com/es/mining-farm-from-graphics-cards-gpu-standing-in-a--ZMGS9ZP

Binance Academy. (22 de octubre, 2018). What is Proof of Work (PoW) – Explained for beginners [Video]. YouTube. https://www.youtube.com/watch?v=3EUAcxhuoU4&ab_channel=BinanceAcademy

Buterin, V. (6 de mayo, 2014). DAOs, DACs, DAs and More: An Incomplete Terminology Guide. *Ethereum Foundation Blog*. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Cryptopedia Staff. (17 de mayo, 2021). Digital Assets: Cryptocurrencies vs. Tokens. *Cryptopedia*. https://www.gemini.com/cryptopedia/cryptocurrencies-vs-tokens-difference#section-what-is-a-token

Hertig, A. (9 de marzo, 2022). ¿Qué es la prueba de trabajo? *Coindesk*. https://www.coindesk.com/learn/2020/12/16/what-is-proof-of-work/

Hong, E. (5 de mayo 2022). How Does Bitcoin Mining Work? *Investopedia*. https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

McShane, G. (12 de octubre, 2021). What is a 51% Attack? *Coindesk*. https://www.coindesk.com/learn/what-is-a-51-attack/

Monolith (21 de noviembre, 2021). Understanding DAOs: Decentralized Autonomous Organisations Explained. *Medium*. https://medium.com/monolith/understanding-daos-decentralised-autonomous-organisations-explained-23793570540f

Rhodes, D. (11 de noviembre, 2022). The Double Spending Problem, Explained. *Komodo*. https://komodoplatform.com/en/academy/double-spending-problem/

SciShow. (21 de diciembre, 2016). *Bitcoin: How Cryptocurrencies Work* [Video]. YouTube. https://www.youtube.com/watch?v=kubGCSj5y3k

Swartz, C. (s.f.). How to Make a Rube Goldberg Machine. *Scout Life*. https://scoutlife.org/hobbies-projects/projects/159359/how-to-make-a-rube-goldberg-machine/

Tapscott, D. (16 de septiembre, 2016). *How the Blockchain is changing money and business* [Video] YouTube. https://www.youtube.com/watch?v=Pl8OlkkwRpc

Winklevoss, C., & Winklevoss, T. (12 de marzo, 2021). Bitcoin: Origins and Cultural Significance. *Cryptopedia*. https://www.gemini.com/cryptopedia/bitcoin-satoshi-nakamoto-genesis

Zmudzinski, A. (7 de junio, 2019). Study: over 74% of mining is powered by renewable energy. *Cointelegraph*. https://cointelegraph.com/news/study-over-74-of-bitcoin-mining-is-powered-by-renewable-energy