BITCOIN EN 10 MINUTOS

Todo lo que siempre quisiste saber sobre Bitcoin

Brought to you by **Relai**

¿QUÉ ES BITCOIN?

Bitcoin, la criptodivisa más exitosa a nivel mundial, ha sido protagonista de muchos titulares en todo el planeta. Muchas personas buscan beneficiarse de su éxito, mientras que otras, por el contrario, se muestran indiferentes o incluso escépticas. Esta moneda digital ha desatado innumerables debates acerca del dinero, la inversión y la tecnología. Algunos ven a Bitcoin como un simple vehículo de especulación o como una burbuja, mientras que otros hablan de innovación, revolución monetaria o incluso de una alternativa al sistema monetario actual.

Varios países, entre ellos China, consideran a Bitcoin una amenaza y han declarado la guerra contra él. Otros gobiernos, como el de El Salvador, han hecho de Bitcoin medio de pago oficial con la esperanza de crecer económicamente.

Pero, ¿qué es Bitcoin? ¿Es dinero? ¿Oro digital? ¿Una moneda para nerds y especuladores? ¿O es algo totalmente diferente? En los siguientes capítulos intentaremos llegar al fondo de todas estas preguntas, y daremos un vistazo en profundidad a esta moneda digital para así entender mejor su filosofía y la funcionalidad que se esconde detrás de ella.

LA HISTORIA DE BITCOIN

El inicio de Bitcoin se remonta a principios de los años noventa. En 1992 un grupo de informáticos californianos creó una lista de correo electrónico para intercambiar ideas con personas afines sobre temas como la criptografía, las matemáticas, la política y la filosofía. Se llamaron a sí mismos los ‚Cypherpunks', un juego de palabras que mezcla la palabra 'cyberpunk' (o 'ciberpunk' en castellano, una figura recurrente en la literatura de ciencia ficción que se muestra escéptica ante la sociedad - ¡y con toda razón!) y la palabra 'cipher' ('cifrar' en inglés).

Los ‚Cypherpunks'

Los ‚Cypherpunks' rápidamente se convirtieron en un grupo bastante diverso pero a pesar de sus diferentes trayectorias, les unía la convicción de que la internet llegaría a convertirse en uno de los campos de batalla más importantes por la libertad humana.

Para protegerse de la amenaza que representa el control, la vigilancia y la censura de la internet, y para preservar una red libre y abierta, los Cypherpunks utilizaron un arma muy poderosa: la criptografía, la codificación de información.

En su manifesto (en español) de 1993, declararon: "Los Cypherpunks escribimos código [informático]. Sabemos que alguien tiene que escribir software para defender la privacidad, [...] y nosotros lo haremos".

Pero la criptografía, por sí sola, no es suficiente para garantizar una internet libre. Los Cypherpunks estaban convencidos de que la internet no se-

ría verdaderamente libre sin su propia forma de dinero. Una forma de dinero que fuera independiente de los estados y los bancos centrales, una criptomoneda tan justa y descentralizada como la internet misma.

Experimentos monetarios

Sin embargo, la creación de una forma de dinero digital independiente supuso retos técnicos. Ya en 1990, el experto en criptografía David Chaum había creado eCash, la primera criptomoneda, que si bien no era descentralizada, garantizaba la anonimidad de sus usuarios gracias a la criptografía. No obstante, eCash no pudo imponerse frente a otros sistemas de pago en línea. La empresa detrás del proyecto tuvo que declararse en quiebra tras 8 años de servicio y eCash desapareció.

Más experimentos le siguieron, entre los cuales cabe destacar E-Gold. E-Gold era una criptomoneda respaldada por oro físico y estaba disponible a todo el mundo. Fundada en 1996 durante la era de las puntocom, la empresa ganó la simpatía de sus homólogos, y llegó a procesar transacciones por un valor de más de dos mil millones de dólares al año en su momento de más auge.

Pero E-Gold estaba controlada por una institución central y, por lo tanto, era vulnerable a ataques. Los problemas legales no tardaron en llegar y el gobierno de los Estados Unidos emprendió acciones legales contra la compañía. En 2008, E-Gold fue declarada culpable por un tribunal estadounidense por blanqueo de dinero y violanción de la Ley Patriótica. Todos sus activos fueron congelados y E-Gold tuvo que cesar operaciones.
Estos intentos fallidos demostraron a los Cypherpunks dos cosas. En primer lugar, tanto eCash como E-Gold estaban respaldadas por un colateral. Colateral que había resultado ser su talón de Aquiles, ya que podía ser confiscado por los gobiernos. Por lo tanto, una criptomoneda libre no debería tener puntos de ataque centralizados como una empresa registrada, una cuenta bancaria o una ubicación en un servidor centralizado. Y en segundo lugar, que ni los gobiernos, ni los reguladores tenían interés en permitir la existencia de una moneda digital independiente del estado.

Los Cypherpunks seguían sin encontrar una solución a la pregunta fundamental: ¿Cómo conseguir que una moneda digital pueda funcionar de forma independiente sin una contraparte central que se encargue de llevar la contabilidad y que garantice que no se gaste dinero más de una vez? Después de todo, si hubiera una forma de solucionar el problema del doble gasto sin depender de una autoridad central, sería posible crear una forma de dinero digital totalmente libre, propia de la internet.

Un acto místico de creación

Por estas razones, los Cypherpunks empezaron a discutir posibles dise-

ños para una criptomoneda que no requiriera de una instancia central o de colateral. Dos de los conceptos más importantes fueron b-money (1998) y BitGold (2005). Estas ideas teóricas, que nunca se llevaron a la práctica, ya eran muy similares a Bitcoin en su concepción. Se preveía un par de llaves públicas y privadas para el cifrado, y una prueba de trabajo para la creación de monedas digitales adicionales, tal y como ocurre con Bitcoin. Es más, en su whitepaper, el inventor de Bitcoin confirmó que conocía tanto b-money como BitGold.

Sin embargo, como b-money y BitGold se basaban en un sistema de votación para el consenso (es decir, para determinar quién posee qué unidades monetarias), ambas eran vulnerables a ataques maliciosos que pudieran manipular dichas votaciones y distorsionar así el registro de propiedad de la red.

Ese problema seguía obstaculizando la creación de una forma de dinero propia de la internet, hasta que el viernes 31 de octubre de 2008 se presentó una solución. Ese día se envió por correo electrónico a los Cypherpunks el Whitepaper de Bitcoin (en Español), en el que Satoshi Nakamoto explicaba su concepto de red de pagos descentralizada. Dos meses después, el 3 de enero de 2009, la red Bitcoin se puso en marcha. Bitcoin como tal no tenía ningún valor aún.

¿Quién es Satoshi Nakamoto?

Tanto el Whitepaper de Bitcoin como los mensajes enviados por correo electrónico por parte del creador de Bitcoin estaban firmados con el nombre de Satoshi Nakamoto. Sin embargo, su verdadera identidad sigue siendo desconocida hasta hoy, ya que su nombre parece ser un seudónimo. Para dirigirse a personas afines y, posteriormente, a la comunidad de desarrolladores de Bitcoin, Nakamoto usó al menos tres direcciones de correo electrónico diferentes (que encriptó minuciosamente para ocultar la verdadera identidad del remitente).

Varias personas han afirmado ser Satoshi Nakamoto pero hasta el día de hoy todas ellas han fracasado en demostrarlo. La prueba definitiva que consistiría en el envío de bitcoin desde una de las direcciones del monedero perteneciente a Satoshi aún no ha sido aportada por nadie.

Además, el grupo de personas que se comunicaron “personalmente” con Satoshi Nakamoto a través de la internet es muy reducido. Satoshi Nakamoto escribió su último mensaje a la comunidad Bitcoin el 12 de diciembre de 2010, mensaje que no fue en absoluto una nota de despedida. Satoshi simplemente dejó de comunicarse después de publicarlo.

Su retiro, sin embargo, fue solo de la comunidad en general, ya que Nakamoto continuó reuniéndose virtual-

mente con un pequeño grupo de programadores a quienes les informaba sobre el futuro desarrollo de la red Bitcoin. Pero en abril de 2011, envió su último mensaje a este grupo. De la misma forma en que Nakamoto apareció misteriosamente en 2008, desaparecería tres años más tarde.

“Bitcoin Pizza Day”

¿Pero cómo llegó Bitcoin a valer algo en primer lugar? Al principio, se podían minar bitcoins y enviar de un lado a otro entre los miembros de la red, pero las unidades digitales como tal no tenían valor. Además, el grupo de personas que sabían acerca de Bitcoin era muy pequeño, ¡y ni hablar del número de personas que sabían usarlo!

Todo esto cambió el 22 de mayo de 2010, cuando una petición inusual apareció en el foro de internet bitcointalk.org. Un hombre de 28 años llamado Laszlo Hanyecz, de Florida, ofrecía 10.000 bitcoins a la persona que le llevara dos pizzas a su casa. Un estudiante californiano aceptó la oferta y le entregó en su casa dos pizzas grandes por valor de 41 dólares. A cambio, Hanyecz le envió 10.000 bitcoins.

Desde ese día los bitcoiners celebran anualmente el 22 de mayo como el “Bitcoin Pizza Day”. El día se hizo popular porque ilustra tres cosas:

- Los bitcoins tienen valor
- Los bitcoins son aptos como medio de intercambio y pago
- Bitcoin como moneda no es inflacionaria. La cantidad de bitcoins adicionales que se ponen en circulación disminuye constantemente, lo que puede conducir a un aumento de su valor.

Las dos pizzas pasarían a la historia como las dos pizzas más caras del mundo. Calculando su coste con el precio de Bitcoin de diciembre de 2021, se habría pagado por ellas la increíble suma de 460 millones de dólares estadounidenses. ¡Eso es mucho dinero! Pero el receptor de los 10.000 bitcoins también los gastó. En una entrevista, declaró que los había vendido poco después para pagar un viaje por carretera. Al precio actual de bitcoin probablemente también se trate del viaje por carretera más caro de la historia de la humanidad.

El “Bitcoin Pizza Day” también ilustra de forma contundente por qué el ‚hodling‘ (palabra derivada del ver-

bo ‚to hold' en inglés) es tan popular entre los amantes de Bitcoin. 'Hodling' significa guardar los bitcoins durante largos períodos de tiempo con la intención de (tal vez) no venderlos nunca. Después de todo, ¿quién iba a querer gastar sus bitcoins hoy cuando su valor podría valer el doble, el triple o incluso diez veces más en los próximos años?

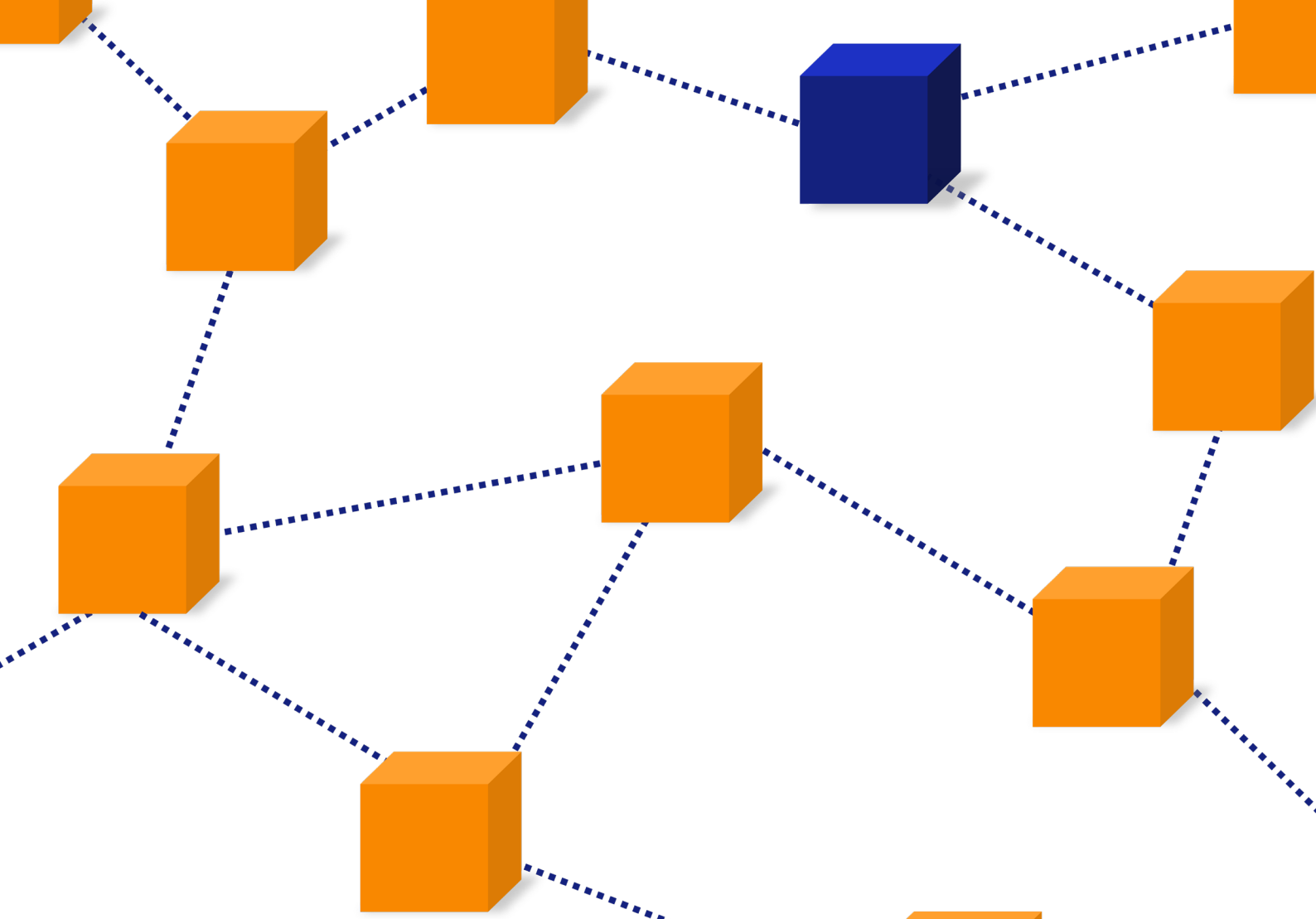
¿CÓMO FUNCIONA BITCOIN?

Después de conocer la historia de Bitcoin, es hora de adentrarnos en su funcionamiento. El objetivo es entender cómo funciona la red de Bitcoin, qué problemas resuelve y cuáles son sus beneficios prácticos.

La finalidad de Bitcoin es ser una red descentralizada. Ningún participante de la red debe ser capaz de gobernar o controlar la red por sí solo. El poder de decisión y la supervisión se distribuyen entre todos los participantes. Esto es fundamental porque ningún individuo, gobierno o empresa debe ser capaz de cambiar la red de forma independiente, sino que los cambios sólo deben ser posibles de forma colectiva.

Bitcoin funciona de tal manera que cada participante de la red tiene una copia idéntica actualizada del libro de contabilidad de dicha red y, como resultado, todo el mundo sabe quién posee qué bitcoins en todo momento. Así, nadie puede afirmar que posee más bitcoins de los que realmente posee, porque cada participante de la red puede comprobar esa información en su copia del libro de contabilidad y comprobar si es falsa.

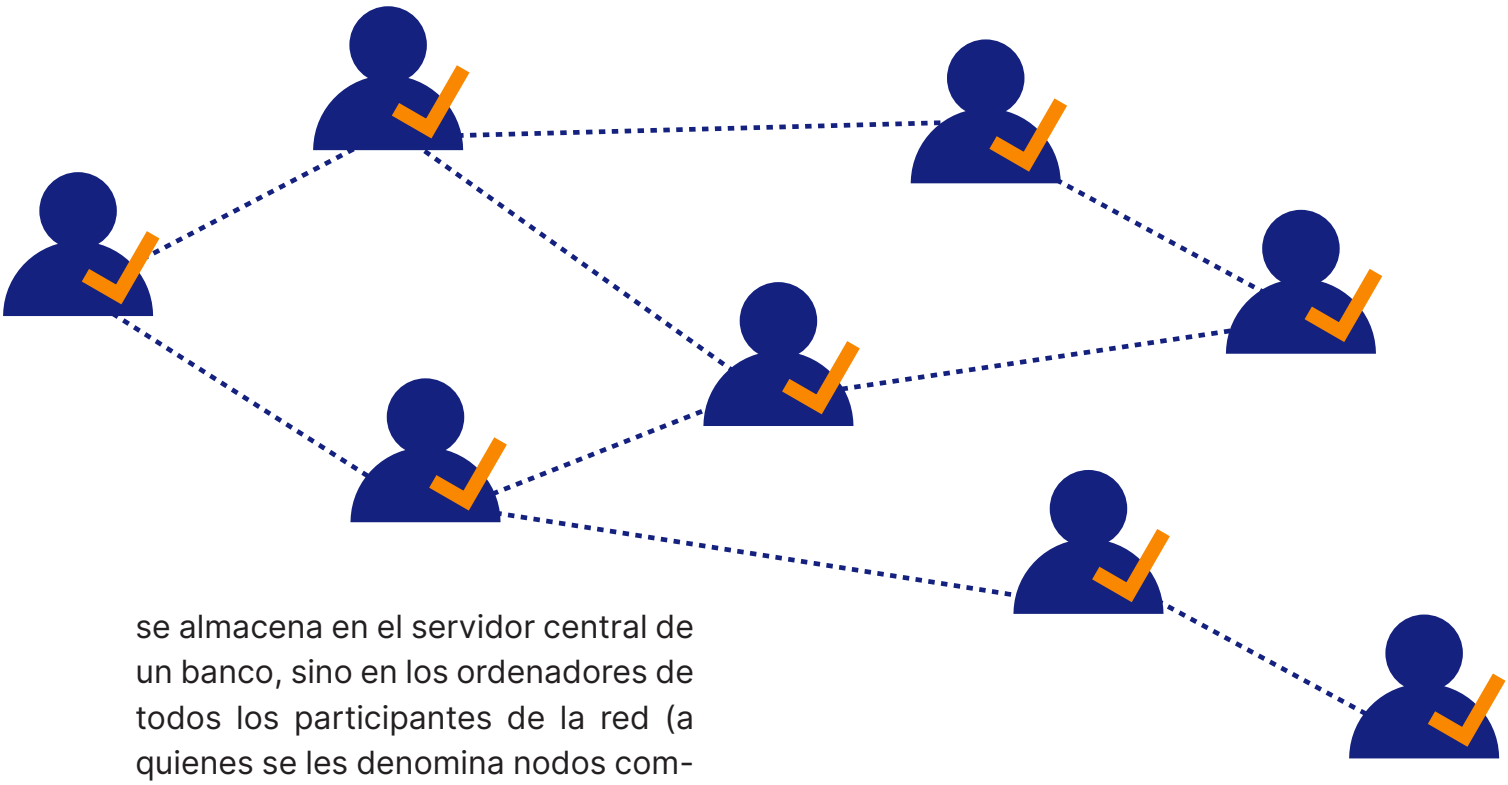
Antes del lanzamiento de Bitcoin, las redes descentralizadas se enfrentaban a dos grandes retos. Por una parte, ¿cómo se podía garantizar que todos los participantes recibieran las últimas actualizaciones sobre los cambios de propiedad dentro de la red, es decir, la información sobre qué bitcoins se han transferido y a quién. Y por otra parte, ¿cómo podrían los participantes verificar con absoluta certeza que la información que han recibido es correcta?



La cadena de bloques

Estas dificultades se superaron gracias a la inversión de la así llamada blockchain (o cadena de bloques). Una cadena de bloques almacena información y datos en orden cronológico. En el caso de Bitcoin, todas las transacciones desde la creación de Bitcoin se almacenan en orden cronológico en decenas de miles de bloques, que juntos forman una cadena de bloques. Cualquier partícipe de la red que quisiera saber a quién le pertenece qué bitcoins puede rastrear el historial completo de transacciones de la cadena de bloques de Bitcoin y determinar así con exactitud quién posee qué en la actualidad. Si alguien quiere enviar un bitcoin, cualquiera puede comprobar si ese bitcoin realmente pertenece a la persona en cuestión.

Hasta aquí este mecanismo no es nada nuevo, ya que los bancos utilizan un proceso similar. Si un cliente quiere gastar un dólar, el banco consulta el historial de transacciones para ver si el dólar sigue perteneciendo al cliente o si ya se ha gastado previamente, si ya ha sido enviado a otra persona. La característica única de una cadena de bloques sin embargo, es que esta información no



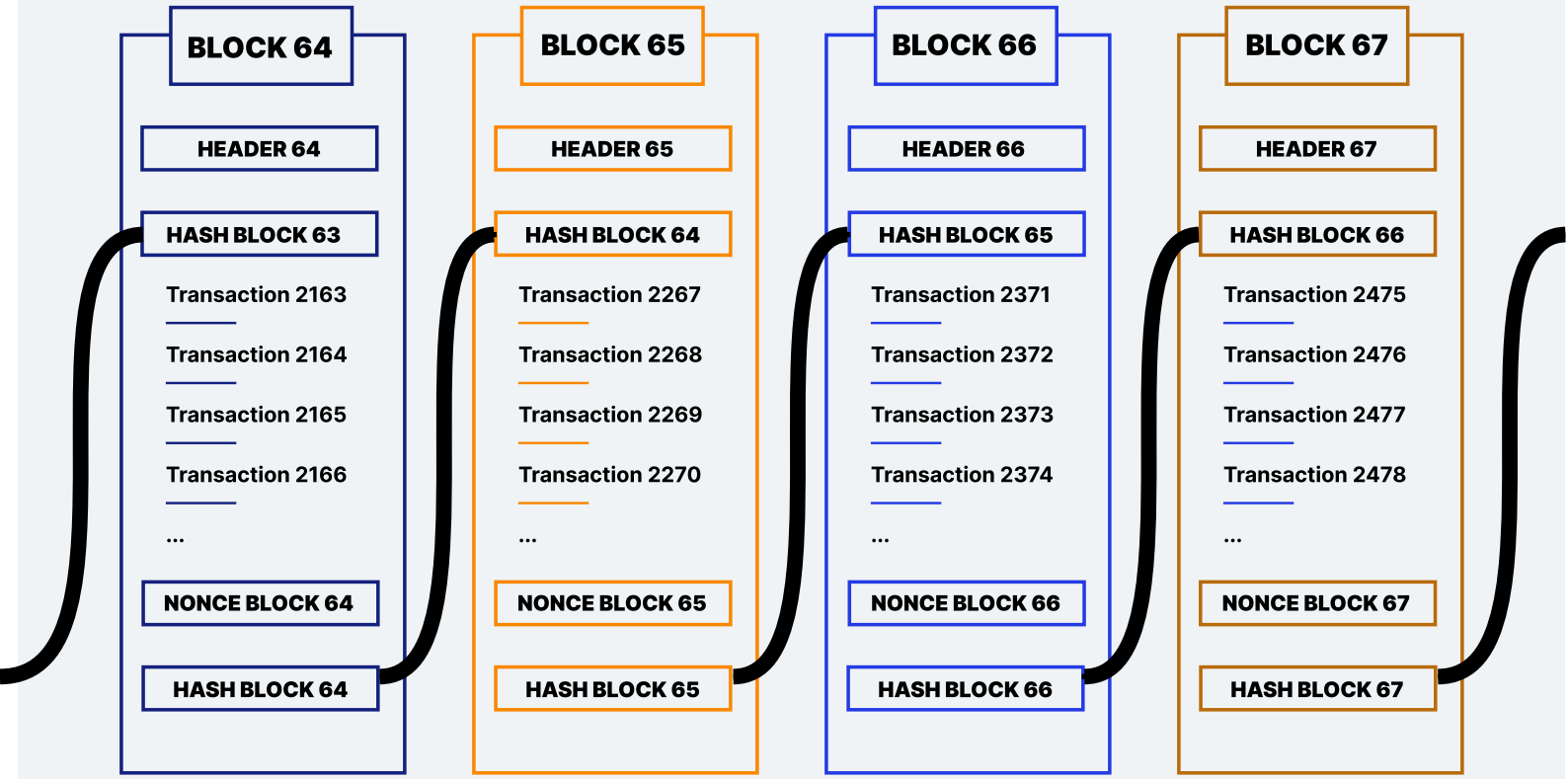
se almacena en el servidor central de un banco, sino en los ordenadores de todos los participantes de la red (a quienes se les denomina nodos completos) y, por tanto, existen decenas de miles de copias en todo el mundo. Ésta es también la razón por la que Bitcoin no puede ser eliminado: para conseguirlo habría que eliminar todas las copias de la cadena de bloques que hay en todos los ordenadores participantes del mundo entero al mismo tiempo.

Sin embargo, el reto al que se enfrentan las cadenas de bloques es el de garantizar que cada participante de la red sea capaz de determinar con absoluta certeza que su copia de la cadena de bloques es correcta y que ninguna transacción errónea o fraudulenta entre en su copia del libro de contabilidad. Dado que cada 10 minutos se añaden nuevos bloques con nuevas transacciones a la cadena de bloques, ésta crece constantemente y debe actualizarse continuamente en todos los ordenadores participantes en el mundo.

Los bloques recién adjuntados deben ser verificados por todos. La verificación se realiza mediante reglas inmutables que se definen en el código de programación de la red de Bitcoin. Estas reglas definen exactamente qué transacciones están permitidas y qué transacciones no. Cada usuario que descargue una copia de la cadena de bloques puede, por lo tanto, verificar si todas las transacciones cumplen con las reglas dadas. Si una transacción viola las reglas, es decir, si es incorrecta o fraudulenta, ésta será rechazada por los participantes de la red (los nodos completos) y no se incluye en la cadena de bloques.

Prueba de Trabajo (PoW) y minería

Además, la red de Bitcoin tiene un mecanismo para limitar la adición de nuevos bloques. Si cualquier persona pudiera añadir nuevas transacciones y bloques de transacciones a la cadena de bloques de la red, ésta terminaría en caos. La cadena de bloques no podría ser actualizada al mismo



La cabecera, el resultado de la función hash del bloque anterior, todas las transacciones del bloque actual y un Nonce (número aleatorio) se introducen en una función matemática. El Nonce se cambia hasta que el resultado de la función hash tiene suficientes ceros precedentes. Este proceso se denomina minería.

estado con la suficiente rapidez en el mundo entero.

Para evitarlo, Bitcoin funciona con un mecanismo de Prueba de Trabajo. Para que alguien se gane el derecho de añadir un nuevo bloque a la cadena de bloques, él o ella debe aportar una prueba de trabajo. Una analogía muy simple de este proceso es un grupo de personas (a quienes llamaremos "mineros") buscando agujas en un pajar. El primero que encuentre una aguja, podrá añadir un nuevo bloque a la cadena de bloques. Además, esa persona será recompensada con nuevas unidades de bitcoin, así como con la comisión de las transacciones contenidas en el bloque. Tan pronto como el bloque se haya unido a la cadena, este proceso se repetirá.

En la práctica, los mineros ejecutan una función hash matemática (el algoritmo hash SHA-256) en la búsqueda no de agujas, sino de ciertos números específicos. El número hash del bloque anterior, las transacciones del bloque actual y un número aleatorio (el "nonce") son combinados en un hash. El número aleatorio es modificado hasta que la función hash arroje un resultado con un número mínimo de ceros a la izquierda. Por ejemplo, el bloque #700000, creado el 11 de septiembre de 2021, tenía el número hash válido: 0000000000000000590fc0f3eba193a278534220b2b37e 9849e1a770ca959.

La búsqueda de ese número, también llamada "minería", tiene dos funciones principales. En primer lugar, enlaza los bloques de forma matemática-criptográfica para que todo el mundo pueda verificar fácilmente su orden correcto. Al mismo tiempo, el mecanismo de Prueba de Trabajo hace casi imposible cambiar ese orden. Y en segundo lugar, este mecanismo retrasa la adición de nuevos bloques, de modo que, en promedio, sólo se añada un nuevo bloque a la cadena de bloques cada 10 minutos. Así, todos los participantes de la red en todo el mundo tienen tiempo suficiente para actualizarse al mismo estado, al estado más reciente de la cadena de bloques.

En resumen, los mineros mantienen la red de Bitcoin en funcionamiento. Gracias a ellos las nuevas transacciones son procesadas y añadidas a la cadena de bloques. Los nodos completos guardan copias del libro de contabilidad, se aseguran de que se cumplan las reglas de la red y garantizan que no entren transacciones fraudulentas en la cadena de bloques.

21 millones de bitcoins

A pesar de que constantemente se añaden más bloques a la cadena de bloques de Bitcoin y de que los mineros son recompensados por este trabajo con nuevos bitcoins, el número total de bitcoins está limitado a 21 millones. Nunca habrá más de 21 millones de bitcoins. Pero estos 21 millones de monedas no están en circulación desde un inicio, sino que son liberadas por el código de Bitcoin según un estricto calendario de emisión.

Cuando se lanzó Bitcoin, el código liberaba 50 nuevos bitcoins a los mineros aproximadamente cada diez minutos. Cuatro años más tarde, el número de bitcoins liberados cada diez minutos se redujo a la mitad. A este proceso se le denomina "halving" ("reducción a la mitad" en castellano) y describe el hecho de que la recompensa de bloque para los mineros se disminuye a la mitad cada cuatro años. La cantidad de bitcoins restantes se minará hasta el año 2140. Después de eso, los mineros sólo serán recompensados a través de las comisiones de transacción.

El hecho de que Bitcoin tenga una cantidad estrictamente limitada de unidades es una de sus características fundamentales que como criptomoneda le convierten en un bien extremadamente escaso. Esa escasez digital absoluta es también un requisito muy importante para que Bitcoin funcione como reserva de valor a lo largo de los años y es la razón por la cual a menudo se le denomina oro digital u oro 2.0

El resultado: propiedad digital

Examinando en conjunto todas las características de la red de Bitcoin

se puede apreciar su importancia. Por primera vez en la historia existe un bien digital que sólo está disponible en una cantidad estrictamente limitada. Los bitcoins no pueden ser copiados o dipicados

Gracias a este logro, Bitcoin es considerado propiedad digital. Porque al igual que cada parcela de tierra es única y existe sólo una vez, cada bitcoin también es único y existe sólo una vez en el mundo digital.

Dichas unidades de bitcoin pueden ser poseídas realmente. Únicamente la persona que posea la correspondiente llave privada, que es una combinación de números y letras de 64 caracteres, puede transferir la cantidad de bitcoin asociada a dicha llave a otras personas. En otras palabras, sin esta llave privada, los bitcoin no pueden ser robados, confiscados o bloqueados. Esto permite al propietario tener el control absoluto sobre sus recursos financieros, independientemente de si es un millonario, un refugiado político o un acreedor perseguido. Por primera vez desde la inversión del ordenador se es posible poseer activos digitales.
nazione di numeri e lettere composta da 64 caratteri, può muovere i bitcoin associati. In altre parole, senza questa chiave privata, i bitcoin non possono essere rubati, confiscati o bloccati. Questo permette al proprietario di avere un controllo assoluto sulle proprie risorse finanziarie, indipendentemente dal fatto che si tratti di un milionario, un rifugiato politico o un creditore perseguitato. Per la prima volta dall'invenzione del computer è possibile possedere veramente beni digitali.

¿POR QUÉ BITCOIN?

Pero, ¿por qué tanto revuelo en torno a Bitcoin? La posibilidad de poseer un activo digital puede ser revolucionaria. Pero, ¿por qué querría alguien poseer bitcoins?

Lo mejor de dos mundos

En siglos pasados se utilizaban como medio de pago metales preciosos y, posteriormente, dinero en efectivo en forma de monedas y billetes. Estos tenían la ventaja de que podían almacenarse y gastarse con independencia de terceros. Por eso se dice que el dinero en efectivo es "libertad impresa". Sin embargo, la desventaja de los metales preciosos y el dinero en efectivo es que son difíciles de utilizar en el espacio digital de la internet. Por eso, desde la llegada de las compras en línea, las tarjetas de débito y crédito se han establecido como el medio de pago dominante entre los usuarios.

El problema es que ahora, que la mayoría de la gente utiliza dinero electrónico en lugar de dinero en efectivo, los riesgos de contrapartida a los que se enfrentan los usuarios son cada vez mayores. Si, por ejemplo, una entidad financiera se declarara insolvente, los ahorros de sus clientes podrían verse afectados. Además, como ocurrió en Argentina en 2001 o en Chipre en 2013, los bancos también pueden limitar de forma drástica los retiros de dinero en efectivo de sus clientes, establecer controles de capital o expropiar forzosamente fondos de las cuentas de ahorro de forma que la gente deje de tener control sobre su dinero. O también, como ocurre hoy en día en muchos países occidentales, puede pasar que a los clientes no se les permita enviar dinero a sus familiares por el simple hecho de vivir en países sancionados como Cuba o Irán, dado que todas las transacciones deben ser primero aprobadas por un tercero.

Con el paso del dinero en efectivo al dinero digital almacenado en cuentas bancarias hemos perdido el control sobre nuestro propio dinero. Ese

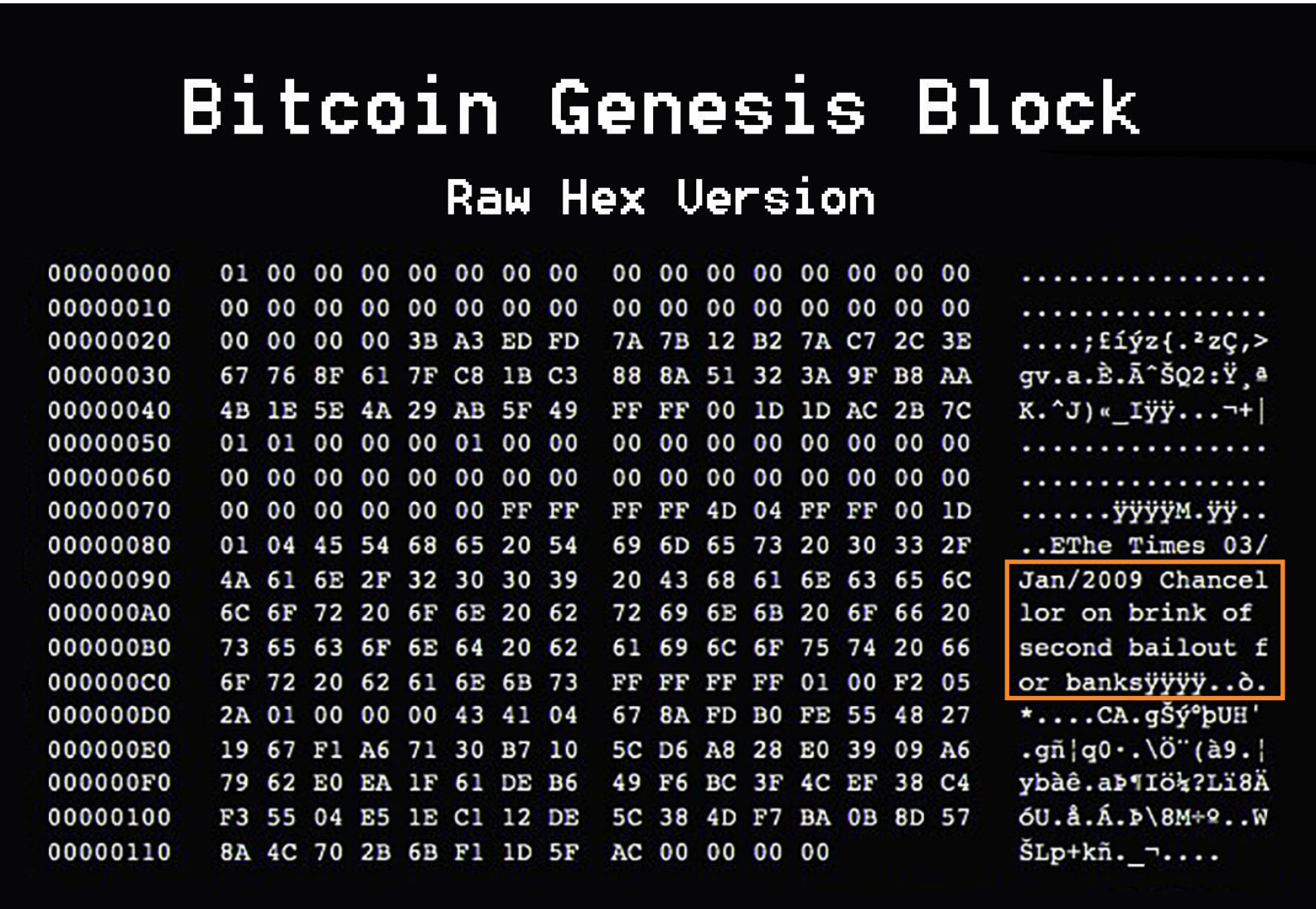
es el precio que tenemos que pagar ahora para poder participar en una vida cada vez más digitalizada.

Bitcoin, sin embargo, ofrece una solución a ese dilema. Como dinero digital es ideal para su uso en la internet y además, al mismo tiempo, puede almacenarse como propiedad digital sin tener que depender de terceros (por ejemplo de bancos) para su custodia. Así, los propietarios de Bitcoin pueden guardar sus monedas (en forma de llaves privadas) "debajo el colchón" o dónde crean que sea conveniente.

El momento oportuno

Bitcoin se creó en medio de la crisis financiera mundial de 2008/2009. En el primer bloque de su cadena de bloques (también conocido como Bloque Génesis) Satoshi Nakamoto dejó un mensaje contundente citando un titular publicado en el periódico The Times que decía: "El canciller al borde del segundo rescate de los bancos".

Con este acto, Satoshi quiso expresar la filosofía crítica del estado propia de los Cypherpunks. Durante la crisis financiera de 2008, los bancos centrales pusieron en circulación grandes cantidades de dinero recién creado para rescatar así al sistema



bancario. Al final, fueron los ahorradores quienes terminaron pagando por ello ya que sus ahorros perdieron valor al diluirse por el exceso de dinero en circulación. Todo esto reafirmó una vez más la desconfianza que los Cypherpunks sienten hacia el estado y hacia los bancos centrales, y reforzó su convicción de que se necesitaba urgentemente una forma de dinero independiente de los gobiernos.

El mismo fenómeno, pero a una escala muchísimo mayor, se ha repetido una vez más desde el estallido de la pandemia del Covid-19. Sólo en 2020, la masa monetaria en los Estados Unidos se expandió en un 50% y, en otros países, la impresión de dinero no se detiene. Una consecuencia directa de este tipo de política fiscal son los bajos tipos de interés y la fuerte inflación de los activos.

Protección contra la devaluación del dinero

Bitcoin se lanzó en el mejor momento posible. Nunca antes el tema del dinero y sus interrogantes habían sido tan relevantes como hoy. Gracias a su oferta limitada de 21 millones, Bitcoin ofrece una alternativa muy atractiva frente a los balances sin fin de los bancos centrales. Su oferta limitada ofrece protección contra la dilución del capital propio tal y como se ha observado con todas las monedas del mundo durante las últimas décadas.

Su diseño está concebido para garantizar la preservación del poder adquisitivo durante largos periodos de tiempo. Dado que los bitcoins son escasos, en teoría podrían satisfacer dicha tarea incluso mejor que el oro cuyo volumen de producción es aproximadamente de un 1-2% anual. Además, los costes de almacenamiento y transporte de Bitcoin son también significativamente menores en comparación con el oro, lo que también permite una mejor conservación de su valor a largo plazo.

Protección de la propiedad

Otro problema que Bitcoin logra mitigar es la protección de la propiedad. Mientras que el coste de almacenar oro o dinero en efectivo de forma segura es enorme, Bitcoin puede ser almacenado y transportado con un coste prácticamente nulo. Incluso cantidades importantes de dinero pueden ser transportadas a cualquier parte del mundo únicamente con un código formado por doce o veinticuatro palabras. Una vez memorizado y destruido físicamente, este código no puede ser robado por nadie, y por lo tanto, los bitcoins detrás del código estarán seguros permitiéndole a su propietario llevarlos a dónde quiera.

COMPRAR BITCOIN

Hay dos maneras de conseguir bitcoins. O bien minándolos, o bien comprándoselos a otra persona. Dado que la minería con dispositivos caseros se ha vuelto prácticamente imposible hoy en día, la única forma que les queda a los nuevos usuarios es comprar bitcoins.

Exchanges y brokers "cripto"

La forma más fácil de comprar bitcoin es a través de casas de cambio digitales conocidas como exchanges o brokers. Estas funcionan de forma muy similar a las plataformas de negociación de acciones. Tras abrir una cuenta, se pueden transferir pesos, euros o dólares estadounidenses a través de una transferencia bancaria o por medio de una tarjeta de crédito.

Una vez que el dinero ha llegado a la cuenta del usuario en el exchange, se puede comprar bitcoin las 24 horas del día con solo unos pocos clics al precio de mercado actual. En Europa, por ejemplo, es posible comprar bitcoin sin necesidad de registrarse, verificarse o depositar dinero gracias a la aplicación Relai.

Peer-to-peer

Como alternativa a los exchanges de criptomonedas, también se puede comprar bitcoin directamente a otros partícipes en el mercado gracias a plataformas peer-to-peer (P2P o persona a persona). Esto permite un mayor anonimato, ya que no hay que revelar datos personales en el proceso.

Cajeros de Bitcoin

También existe la posibilidad de comprar y retirar bitcoin a través de cajeros automáticos. Estos ya están disponibles en muchos países, como por ejemplo en España, México, El Salvador o Argentina. En los cajeros automáticos de Bitcoin, se puede comprar y retirar bitcoin de forma anónima con dinero en efectivo o con tarjetas de crédito. No es necesario tener una cuenta, ni un monedero criptográfico.

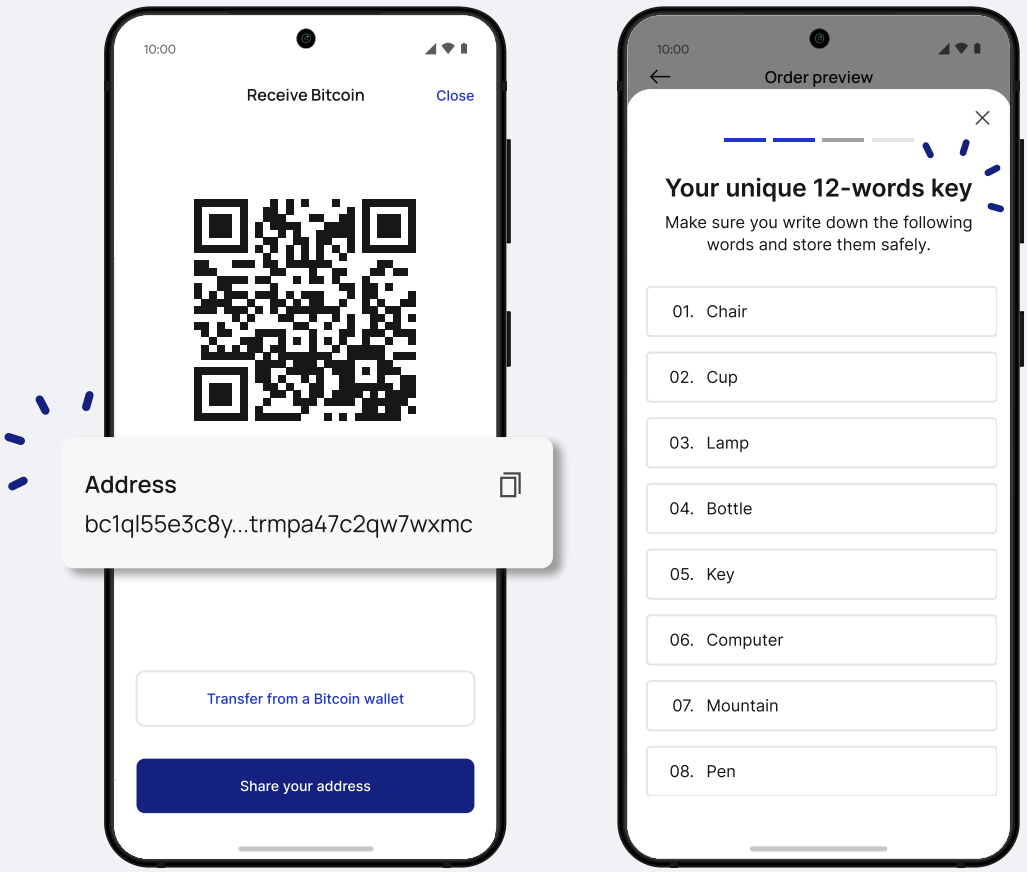
Almacenar bitcoins de forma segura

Una vez adquiridos los bitcoins, se plantea la cuestión de su manejo y almacenamiento de forma segura. Bitcoin y también otras criptomonedas se rigen por el principio: “not your keys, not your coins” (si no controlas tus llaves, no controlas tus monedas). Para ser realmente propietario de tus bitcoins, debes controlar tus propias llaves privadas. Esta expresión, que suena algo técnica, significa que únicamente tendrás el control de tu dinero si almacenas tus bitcoins en un monedero digital que te permita controlar tus llaves privadas.

Si mantienes tus bitcoins en un exchange, estos estarán bajo el control del exchange. Si el exchange es hackeado, quiebra o si se trata de una plataforma fraudulenta, podrías perder tus bitcoins para siempre.

Autocustoria

A diferencia de una cuenta bancaria, Bitcoin te da la opción de almacenar todas tus unidades monetarias en un monedero personal. Esto te permi-



te, por decirlo así, ser tu propio banco de modo que tú tengas el control absoluto sobre tus bitcoins. A cambio debes aceptar la responsabilidad que ello conlleva. La llave privada, que a menudo viene cifrada en forma de doce o veinticuatro palabras, debe ser almacenada y mantenida a salvo por su respectivo propietario. Un manejo incorrecto o descuidado puede llevar a la pérdida irrevocable de sus fondos.

Monederos digitales

Los monederos digitales ayudan a almacenar bitcoin, o más exactamente, las llaves privadas de forma segura. Los bitcoins como tal nunca abandonan la cadena de bloques y no pueden ser transferidos a un monedero. Sólo las llaves de acceso a los bitcoins pueden almacenarse en un monedero.

Los monederos se crearon para permitir el almacenamiento de las llaves privadas de forma segura y sencilla. Además, permiten enviar y recibir bitcoin con unos pocos clics. Por ello, los monederos son una herramienta muy útil para el manejo de fondos en bitcoin.

Monederos de software

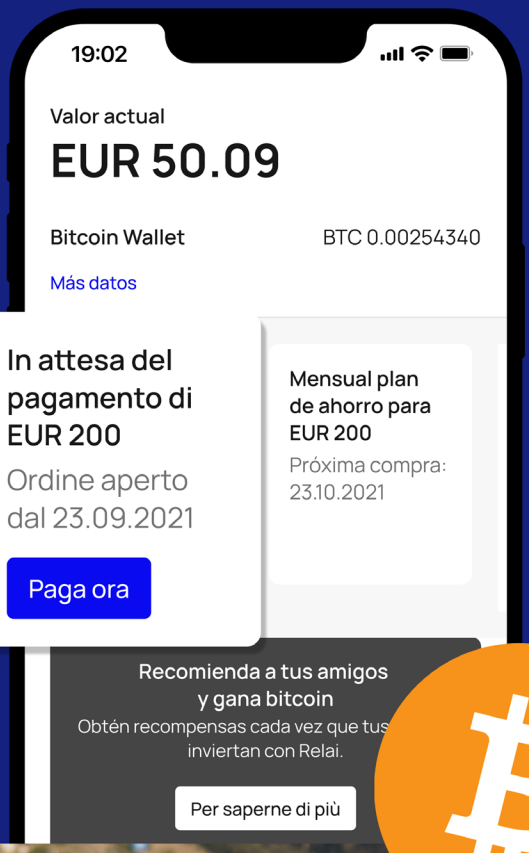
Los monederos más comunes son los monederos de software. Los monederos de software pueden configurarse como aplicaciones de escritorio o como aplicaciones para teléfonos móviles. Durante la configuración las llaves privadas del monedero se enumeran en forma de doce o veinticuatro palabras (a lo que se le conoce como frase semilla). Estas palabras pueden ser consideradas como el equivalente de los fondos en bitcoin que se tengan en el monedero. Quien conozca dichas palabras tendrá el control de las monedas. Por lo tanto, las palabras deben ser guardadas preferiblemente de forma análoga, es decir, en un medio físico como el papel, y almacenadas en secreto en un lugar seguro. Si el ordenador o el teléfono móvil en que está instalado tu monedero llegaran a extraviarse o ser robados, el monedero podría ser restaurado en otro dispositivo usando la frase semilla.

Los monederos de software tienen la ventaja de que se pueden configurar de forma rápida y de que son muy fáciles de usar. Sin embargo, como los monederos de software son programas informáticos instalados en dispositivos que tienen conexión a internet, siempre existe el riesgo de ataques por parte de hackers.

Monederos de hardware

Si quieres un nivel de seguridad superior, es recomendable que utilices un monedero de hardware. Un monedero de hardware es un pequeño dispositivo que almacena los códigos de acceso de tus bitcoins en un aparato similar a una memoria USB que solo se conecta al ordenador (y no a la

Made in Switzerland



LA APP BITCOIN MÁS FÁCIL DE EUROPA

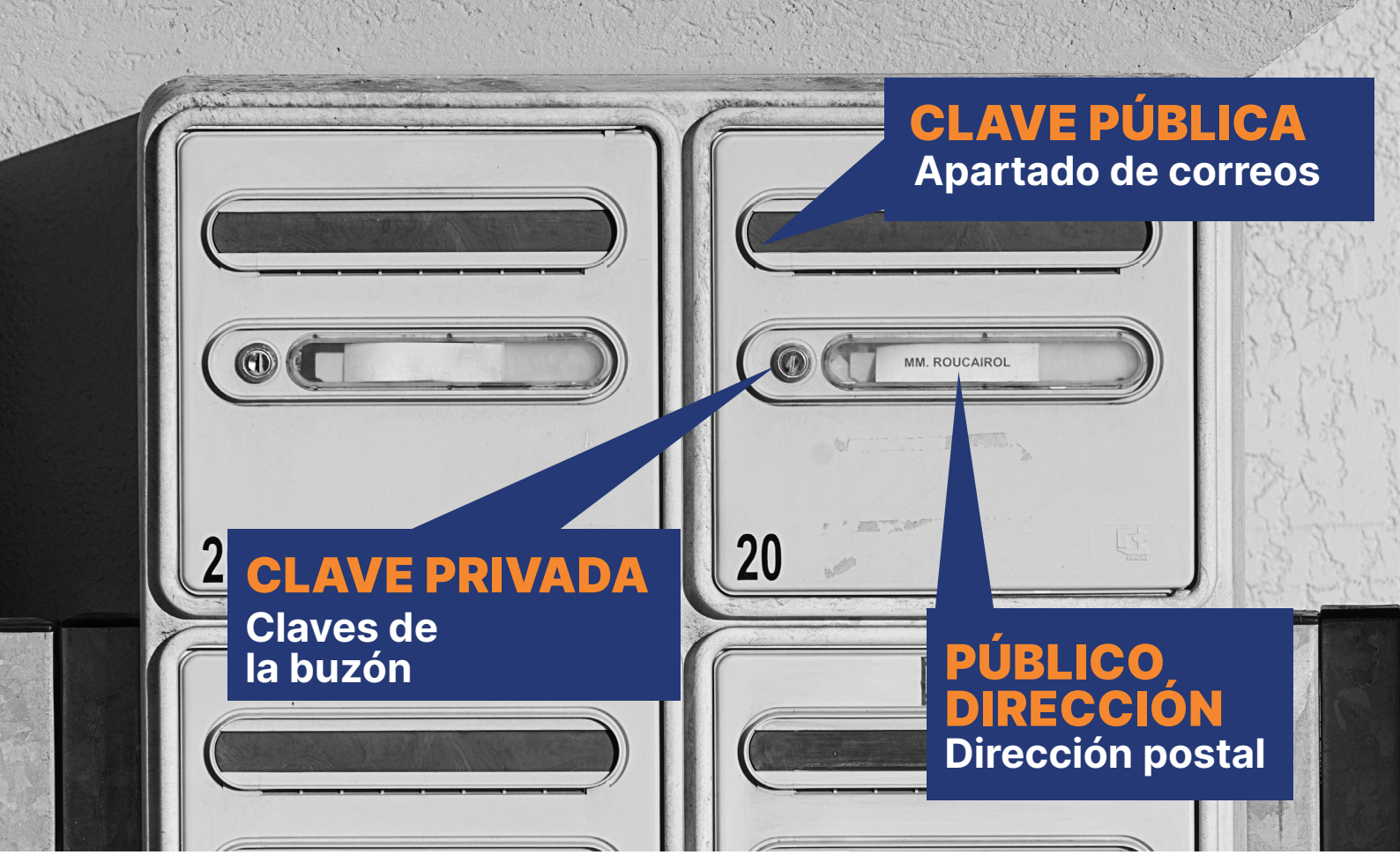
Bitcoins recibidos BTC 0.00254340
24.09.2021 CHF 50.65

Relai

Download on the App Store

GET IT ON Google Play

Compre bitcoins en 1 minuto desde tan solo 10 EUR/CHF sin verificación.



internet) cuando se necesite. El dispositivo está diseñado de tal manera que incluso un ordenador infectado con software malicioso no pueda acceder a las llaves privadas.

Al configurar un monedero de hardware, también se generan doce o veinticuatro palabras (la frase semilla) que deben anotarse de forma análoga y guardarse en un lugar seguro. Si por algún motivo llegara a perderse o dañarse el dispositivo de hardware, el monedero se podía ser restaurado en otro dispositivo con la ayuda de la frase semilla. Ejemplos de monederos de hardware son BitBox y Trezor.

Enviar y recibir bitcoin

Enviar y recibir bitcoin es muy fácil. Cada monedero de Bitcoin tiene su propia dirección pública generada a partir de la así llamada llave pública. Ésta sirve como dirección para recibir fondos, similar a un número de cuenta bancaria. Cualquiera que tenga esta dirección puede enviar bitcoin al monedero correspondiente. La dirección pública suele mostrarse en forma de código QR para simplificar su manejo.

Si quieres enviar bitcoin a alguien, basta con que introduzcas la dirección del destinatario en tu monedero bajo la pestaña “enviar” o que escanees el código QR correspondiente. Los costos de transacción se deducirán automáticamente del monedero del remitente. Dichos costos de transacción varían en función del uso de la red de Bitcoin y pueden consultarse aquí. La transferencia tarda en promedio unos diez minutos en llegar

al destinatario. Sin embargo, también puede tardarmás dependiendo de la tasa de transacción que se esté dispuesto a pagar.

Pagar con Bitcoin

Cuando se creó Bitcoin, el objetivo era que algún día se pudiera utilizar para pagar los gastos del día a día. Y en teoría, esto ya es posible. Algunas instituciones fiscales gubernamentales, organizaciones sin ánimo de lucro y un número creciente de empresas aceptan bitcoin como medio de pago. Pero como las transacciones a través de la red de Bitcoin pueden costar varios dólares y tardar unos diez minutos en ejecutarse, generalmente solo tiene sentido hacerlo con cantidades de dinero relativamente grandes. Para enviar cantidades pequeñas de bitcoin de forma barata y rápida, se necesita una solución alternativa.

La Lightning network,
¡rápida y más barata!

Por eso, se construyó una capa adicional sobre la red de Bitcoin a la que se le denominó Lightning. La Lightning Network permite realizar pagos usando Bitcoin en cuestión de segundos a un coste mínimo. En países como El Salvador la Lightning Network ya se usa con éxito.

El pago de productos cotidianos usando Bitcoin se realiza mayoritariamente a través de la Lightning Network. Y los avances de su infraestructura van a toda velocidad. Twitter, por ejemplo, ha introducido recientemente una función para enviar y recibir propinas usando la Lightning Network. Además, la aplicación Strike ofrece pagos en varias divisas de todo el mundo a coste cero usando también la Lightning Network. Por lo tanto, es de esperar que en el futuro sólo se use la red de Bitcoin para envíos de cantidades más grandes de dinero, mientras que el resto de transacciones se ejecuten por medio de la Lightning Network.

Dado que la Lightning Network se emplea principalmente para realizar envíos de cantidades de dinero pequeñas, en lugar de bitcoins suelen utilizarse como unidad de medida los “satoshis” (o simplemente “sats”). 1 bitcoin equivale a 100.000.000 satoshis.

Para usar la Lightning Network es necesario crear un monedero compatible con esta red.

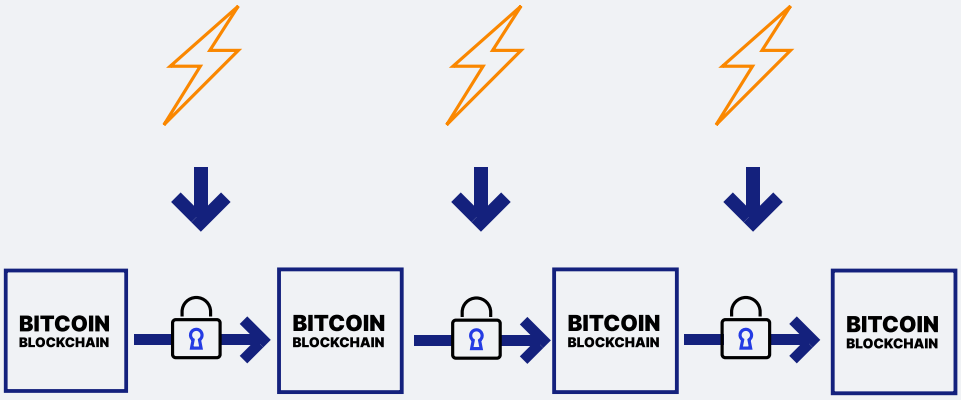
UNA MIRADA HACIA EL FUTURO

En sus más de diez años de existencia, Bitcoin ha pasado por muchos altibajos. La criptomoneda ha sido declarada “muerta” y ha caído en el olvido del público en general varias veces tras fuertes caídas de su precio. A pesar de ello, Bitcoin ha conseguido extenderse de forma imparable por todo el mundo durante la última década.

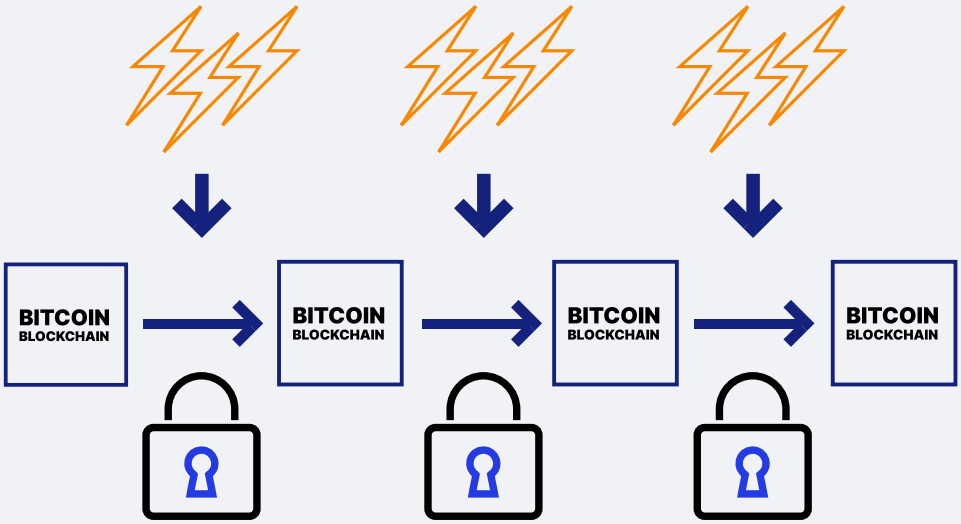
Bitcoin y energía

Una de las preocupaciones principales que se plantean a menudo en relación al desarrollo de Bitcoin es el consumo de energía de su red. La minería de Bitcoin consume una cantidad significativa de electricidad en todo el mundo y es probable que este consumo aumente en el futuro a medida que más gente se dedique a la minería de Bitcoin.

Cuando se habla de Bitcoin y de su minería, es importante entender que la cantidad de energía que alimenta a la red es fundamental para la seguridad de la misma. Cuanta más energía requiera la red, más segura



Cuanto menos energía en forma de potencia de cálculo se utilice para construir la cadena de bloques de Bitcoin, más fácil será modificarla posteriormente.



Cuanta más energía en forma de potencia de cálculo se utilice para crear la cadena de bloques de Bitcoin, más difícil será cambiarla posteriormente.

será. Esto se debe a que, para que la cadena de bloques pueda ser alterada, se necesitará la misma cantidad de energía (medida en potencial de cálculo) que se invirtió inicialmente para crear la cadena de bloques. Si hay millones de ordenadores en todo el mundo proporcionado potencia de cálculo a la red de Bitcoin, será casi imposible que un individuo, una institución o un gobierno puedan reunir suficiente potencial de cálculo para realizar siquiera cambios pequeños en la cadena de bloques. Por eso el "hashpower" o potencia de cálculo, y el consumo de energía asociado son características muy importantes para la seguridad de la red de Bitcoin.

Además, los ordenadores usados en la minería de Bitcoin tienen la ventaja de que pueden estar ubicados en cualquier parte del mundo. Como los mineros necesitan de la electricidad más barata posible para poder ser rentables, suelen ubicarse en lugares donde hay excedentes de energía y, por tanto, donde la energía es más barata. A largo plazo, es probable que se concentren cada vez más y más en lugares con muchas fuentes de energía renovable ya que ésta generalmente es más barata.

Según el "Bitcoin Mining Council" (Consejo de Minería de Bitcoin), los

mineros de Bitcoin ya utilizan en la actualidad un 56% de energía renovable y la tendencia va en aumento. Muchos expertos creen que la minería de Bitcoin llegará a abastecerse de hasta un 100% de energía renovable en el futuro.

Sin embargo, hasta que esto ocurra, el debate sobre el consumo de energía de Bitcoin se centrará en si una forma de dinero y de depósito de valor segura e inconfesable justifica ese gasto o no.

El Salvador - Bitcoin como moneda de curso legal nacional

Hace unos años varios visionarios ya consideraban posible que algún día Bitcoin pudiera ser reconocido como moneda de curso legal por estados nacionales. Y en el verano de 2021 finalmente llegó ese momento: El Salvador fue el primer país del mundo en introducir Bitcoin como moneda de curso legal. En tiendas, restaurantes y en proveedores de servicios de todo tipo, no sólo se puede pagar con dólares estadounidenses, sino también con bitcoins. Para conseguirlo, el gobierno proporcionó a los ciudadanos un monedero de Bitcoin personalizado que permite realizar pagos en cuestión de segundos y a un coste mínimo usando la Lightning Network.
Otros países como Ucrania, Brasil y Panamá están debatiendo actualmente proyectos de ley similares. Si más países siguieran el ejemplo de El Salvador, esto, por un lado, aumentaría aún más la demanda de Bitcoin y, por otro lado y lo que es más importante, afianzaría la credibilidad de Bitcoin como forma de dinero. La aceptación de Bitcoin como moneda de curso legal en más y más países representa una fase decisiva en el proceso de adopción de Bitcoin a nivel global.

Leyes y regulaciones

Esta evolución ha conducido a que los estados, los bancos centrales y las empresas tengan la necesidad de ocuparse intensamente con el tema de las criptomonedas. Varios estados, entre ellos Suiza, han publicado reglamentos y directrices referentes a las criptomonedas. Este paso ha sido muy bien recibido por muchos de los participantes en el mercado ya que crea un nivel de seguridad jurídica tanto para los proyectos de criptomonedas como para los inversores mismos.

También en los EE.UU se espera que se empiecen a introducir más regulaciones. Hasta ahora se había adoptado un enfoque de laissez-faire. La comunidad internacional sigue con atención este desarrollo y las medidas exactas que lleguen a tomarse en los Estados Unidos, ya que estas sin duda tendrán un impacto importante en todo el sector de las criptomonedas.

Otras criptomonedas

Bitcoin no es, ni mucho menos, la única criptomoneda que existe en la actualidad. Actualmente hay más de 16.000 criptodivisas y criptoactivos diferentes. Estas monedas y tokens tienen diferentes características y funcionalidades, y no todas han sido diseñadas para convertirse en formas de dinero. Algunas se parecen más a las acciones en el sentido de que su valor refleja el éxito de un proyecto criptográfico. Otras son necesarias para hacer uso de un servicio concreto. Y otras (conocidas como memecoins) son monedas cuya única finalidad es la diversión.

Monedas digitales de los Bancos Centrales (CBDC)

Las criptodivisas están en un proceso de transición de una fase de descontrol y desorden, a una fase de regulación. Esta evolución no ha dejado indiferentes a los bancos centrales, quienes se han planteado la idea de emitir sus propias criptodivisas. A éstas se les conoce como Monedas digitales de los Bancos Centrales (o CBDC por sus siglas en inglés), y combinarían, según sus defensores, la estabilidad de una moneda estatal con las ventajas de una moneda emitida usando la tecnología blockchain. En resumen, se trataría de una forma de efectivo digital, por así decirlo.

Sin embargo, dependiendo de su diseño, cada CBDC puede adoptar formas muy diferentes.

Varios países ya han puesto en marcha pruebas piloto con diferentes tipos de CBDC, y de hecho ya se han lanzado CBDC en algunos países. No obstante, se espera con impaciencia si las zonas monetarias económicamente fuertes, como EE.UU., la Unión Europea o China, pondrán en marcha sus CBDC y de qué manera lo harán.

Competencia monetaria

Nuestra sociedad se ha acostumbrado tanto a las monedas estatales que hasta hace poco era muy difícil imaginar otros tipos de dinero. Sin embargo, hace no muchas décadas, era parte de la vida cotidiana la circulación paralela de diferentes tipos de dinero. Había billetes emitidos por diferentes bancos, monedas respaldadas por diferentes metales preciosos y otros valores monetarios que podrían utilizarse como medio de pago.

Con Bitcoin, las monedas no estatales han vuelto a resurgir como alternativa al dinero estatal. Hasta ahora, la mayoría de gobiernos han tolerado a Bitcoin. Hasta cierto punto, esto podría deberse a su naturaleza descentralizada y a que es muy difícil atacarlo y controlarlo. Para los ciudadanos, esto significa que ahora existe una alternativa digital a las divisas estatales semejante al oro y la plata. Sin duda, será muy interesante observar los efectos que esta “competencia monetaria” tendrá en el futuro.

BITCOIN , ¿Y AHORA QUÉ?

Si te estás preguntando qué deberías hacer con toda esta información, déja que te haga una sugerencia. Entrar en el mundo de Bitcoin no cuesta nada, ni tiempo, ni dinero. Y por el contrario puedes aprender mucho y conocer una tecnología que está a punto de cambiar nuestro mundo y nuestro futuro.

Por lo tanto, mi sugerencia es la siguiente: crea una cuenta con un exchange de criptomonedas o descarga un monedero en tu smartphone y compra una pequeña cantidad de bitcoin, por ejemplo, el equivalente a 5 dólares. O pídele a un amigo que te envíe algo de bitcoin a tu monedero. ¡Pero pon en tus manos por lo menos una vez esta tecnología!

Porque si Bitcoin llegará a convertirse en algo tan importante y tan omnipresente como la internet, no sólo lo conocerás teóricamente, sino que lo habrás usado en la práctica por ti mismo. A veces, eso marca la diferencia, ya que lograrás tener una mejor idea de esta tecnología, lo que te pone por delante de la mayoría de personas.

CIRCA

SOBRE EL AUTOR

Daniel Jungen es un economista y periodista financiero especializado en criptoactivos. Daniel es cofundador de InsightDeFi, una agencia de investigación especializada en todo lo relacionado a las criptomonedas. Junto con sus socios de InsightDeFi, Daniel publica un boletín quincenal (en alemán) sobre Bitcoin, DeFi y Crypto.

SOBRE RELAI

Fundada en Suiza por Julian Liniger y Adem Bilican, quienes vieron la necesidad de que por fin hubiera un servicio seguro y sin complicaciones para comprar bitcoins, Relai facilita el ahorro y la inversión en Bitcoin a todo el mundo. La aplicación está diseñada de forma simple e intuitiva, y permite a cualquier persona en Europa comprar y vender bitcoins en cuestión de minutos, sin necesidad de registros, verificación de identidad o depósitos.

Relai ha sido auditada de forma independiente y por medio de su plataforma ya se han invertido más de 35 millones de francos suizos. Relai ofrece a sus clientes la posibilidad de acceder a nuevas formas de ahorro e inversión.

Aprende más en Relai.app.

Gracias a James Arias Fajardo, que ha traducido este libro electrónico del inglés al español.