BITCOIN EN 10 MINUTOS

Todo lo que siempre quisiste saber sobre Bitcoin

Brought to you by Relai

¿QUÉ ES BITCOIN?

Bitcoin, la criptomoneda más famosa y exitosa del mundo, está en los titulares de todo el globo. Muchos quieren lucrarse a costa de su éxito, mientras que otros se muestran indiferentes o incluso desconfiados.
Los cripto-activos han provocado innumerables debates sobre dinero, inversiones y tecnología. Algunos ven a Bitcoin como un instrumento puramente especulativo o lo denuncian como una burbuja, mientras que otros hablan de innovación, revolución monetaria o incluso redención y salvación del sistema monetario actual.

Varios países, incluido China, ven a Bitcoin como una amenaza y le han declarado la guerra a la criptomoneda. Otros gobiernos, como el de El Salvador, han introducido Bitcoin como medio de pago oficial con la esperanza de obtener un crecimiento económico con ayuda de la criptodivisa.

Pero, ¿qué es Bitcoin? ¿Es dinero? ¿Oro digital? ¿Una moda para informáticos y especuladores? ¿O algo completamente diferente? En los siguientes párrafos llegaremos al fondo de estas preguntas y analizaremos más de cerca la moneda digital para comprender mejor la filosofía y la funcionalidad detrás de Bitcoin. Para lograr esto es importante comenzar desde el principio, con la historia de los orígenes de Bitcoin.

LA HISTORIA DE BITCOIN

Los inicios de Bitcoin se remontan a principios de los noventa. En 1992, un grupo de informáticos de California inició una lista de correo electrónico para intercambiar opiniones y conocimientos con personas de ideas afines sobre criptografía, matemáticas, política y filosofía. Se llamaron a sí mismos ‚Cypherpunks', un juego de palabras entre cyberpunk (persona en la literatura de ciencia ficción que es escéptica de la sociedad, y con razón) y cipher (encriptar).

Los Cypherpunks

Los Cypherpunks pronto se convirtieron en un grupo variopinto. A pesar de sus diferentes orígenes les unía la convicción de que Internet se convertiría pronto en uno de los escenarios más disputados por la libertad humana.

Para protegerse de la amenaza del control, la vigilancia y la censura de Internet y preservar un Internet libre y abierto, los cypherpunks utilizaron un arma poderosa: la criptografía, el cifrado de la información.

En su manifiesto de 1993 afirmaban: „Los Cypherpunks escriben el código [informático]. Sabemos que alguien tiene que escribir el software para defender la privacidad, y [...] vamos a escribirlo".

Pero la criptografía por sí sola no sería suficiente para un Internet libre porque, y los Cypherpunks estaban convencidos de ello, Internet no puede ser verdaderamente libre si no tiene su propio dinero. Un dinero independiente de los estados, los bancos centrales y las empresas; una criptomoneda tan justa y descentralizada como el propio Internet.

Experimentos monetarios

No obstante, la creación de dinero digital independiente planteaba a los Cypherpunks retos técnicos. Ya en 1990 el criptólogo David Chaum había creado eCash, la primera criptodivisa, que no estaba descentralizada pero garantizaba el anonimato gracias a la criptografía. Sin embargo, eCash no fue capaz de imponerse a otros sistemas de pago online en el largo plazo. La empresa detrás del proyecto tuvo que declararse

en quiebra tras 8 años de servicio y eCash desapareció.

Al anterior le siguieron otros intentos, entre los que destacó E-Gold. E-Gold era una criptomoneda respaldada por oro que estaba abierta a todo el mundo. Fundada en 1996 durante la era de las puntocom, la empresa tuvo un gran éxito entre sus pares, ya que procesó transacciones por valor de más de 2.000 millones de dólares al año en su punto álgido.

Pero E-gold estaba controlada por una institución central y por tanto era vulnerable a los ataques. Pronto surgieron problemas legales y el gobierno de Estados Unidos emprendió acciones legales contra E-Gold. En 2008, un tribunal estadounidense declaró a E-Gold culpable de blanqueo de dinero y de violación de la Ley Patriota. Todos los activos fueron congelados y E-Gold tuvo que cesar sus operaciones.
Estos intentos fallidos demostraron dos hechos a los Cypherpunks: en primer lugar, tanto el eCash como el E-gold estaban respaldados por una garantía o colateral. Este colateral había demostrado ser un punto débil, ya que podía ser confiscado por los estados. Por lo tanto, una criptomoneda libre no debería tener puntos centrales de ataque como una empresa registrada, una cuenta bancaria o unos servidores centralizados. Y en segundo lugar, que tanto a los gobiernos como a los reguladores no les interesa el dinero digital independiente del Estado.

Para los Cypherpunks la pregunta básica para la que aún no se había encontrado una solución seguía siendo: ¿Cómo podría funcionar un dinero digital independiente que no tuviera un punto central que lleve la contabilidad y que garantice que el dinero no se gasta dos veces? Después de todo, si fuera posible resolver el problema del doble gasto sin depender de una parte central podría ser posible crear un dinero digital libre y nativo de Internet.

Un Acto de Creación místico

Por estos motivos los Cypherpunks empezaron a proponer diseños para una criptodivisa sin una parte central y sin garantías. 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 diseño. Se preveía un par de claves públicas/privadas para el cifrado y una prueba de trabajo para la creación de monedas digitales adicionales, como también ocurre con Bitcoin. En su libro blanco (o Whitepaper), el creador de Bitcoin confirmó que conocía b-money y BitGold.

Sin embargo, debido a que b-money y BitGold dependían de un sistema de votación por consenso (un acuerdo para decidir quién posee qué unidades monetarias en la actualidad), eran vulnerables a ataques maliciosos que podían manipular dichas

elecciones y por lo tanto distorsionar la propiedad.

Para este último problema, que seguía obstaculizando la creación de un nuevo dinero en Internet, se presentó una solución el viernes 31 de octubre de 2008. Ese día se envió por correo electrónico a los Cypherpunks el Libro Blanco de Bitcoin (el Bitcoin Whitepaper), en el que Satoshi Nakamoto explica su concepto de una red de pagos descentralizada. Dos meses después, el 3 de enero de 2009, la red Bitcoin se puso en marcha.

Las reacciones iniciales a la nueva red fueron apagadas. Algunos entusiastas empezaron a probar la red y a informar de errores. Al principio era principalmente el propio Satoshi Nakamoto quien mantenía la red en funcionamiento, pero poco a poco la noticia del nuevo dinero de Internet se extendió por los foros de informática y tecnología y el interés por la red creció. Al cabo de un año la red Bitcoin ya contaba con algunos usuarios. No obstante, Bitcoin en sí mismo aún no tenía valor.

¿Quién es Satoshi Nakamoto?

Tanto el libro blanco o "Whitepaper" de Bitcoin como la comunicación por correo electrónico del creador de Bitcoin estaban firmados con el nombre de Satoshi Nakamoto. Sin embargo, la verdadera identidad del inventor de Bitcoin sigue siendo desconocida hasta hoy, ya que su nombre parece ser un alias. Para dirigirse a personas afines y posteriormente a la comunidad de desarrolladores de Bitcoin, Nakamoto utilizó al menos tres direcciones de correo electrónico diferentes que encriptó minuciosamente para ocultar la verdadera identidad del remitente.

Varias personas ya han afirmado ser Satoshi Nakamoto, pero hasta hoy todos ellos han fracasado en demostrarlo porque la prueba definitiva, es decir, el envío de bitcoins desde una de las direcciones del monedero que muy probablemente pertenezca a Satoshi, aún no ha sido aportada por nadie.

Además, el grupo de los que se han comunicado „personalmente" con Satoshi Nakamoto a través de Internet es muy reducido. Satoshi Nakamoto escribió su último mensaje a la comunidad de Bitcoin el 12 de diciembre de 2010, pero no fue en absoluto un mensaje de despedida. Satoshi simplemente dejó de comunicarse después de eso.

Su retiro, sin embargo, fue sólo para la comunidad en general. Nakamoto siguió reuniendo a un pequeño grupo de programadores de base a su alrededor y les informó sobre el desarrollo posterior de la red Bitcoin, pero en abril de 2011 envió un último mensaje a este grupo también. Tan misteriosamente como apareció Nakamoto en 2008 volvió a desaparecer tres años después.

El „Día de la Pizza“ de Bitcoin

¿Pero cómo consiguió tener valor Bitcoin en primera instancia? Al principio Bitcoin se podía minar y enviar de un lado a otro entre los miembros de la red, pero las unidades digitales no tenían valor. Además, el grupo de personas que conocían Bitcoin y sobre todo, que podían enviarlo y recibirlo, era todavía muy pequeño.

Esto cambió el 22 de mayo de 2010, cuando apareció una inusual petición 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 pidiera dos pizzas a domicilio. Un estudiante californiano aceptó la oferta y recibió en su casa dos pizzas grandes por valor de 41 dólares. A cambio Hanyecz le envió los 10.000 bitcoins.

Desde ese día los Bitcoiners celebran anualmente el 22 de mayo como el „Día de la Pizza“ de Bitcoin. El día se hizo popular porque ilustra tres cosas:

- Los bitcoins tienen valor
- Los bitcoins son útiles como medio de intercambio y pago
- Bitcoin como moneda es deflacionaria. El número de bitcoins adicionales que se ponen en circulación disminuye constantemente, lo que puede conducir a un aumento del valor.

Las dos pizzas han pasado a los libros de historia como las más caras del mundo. Calculando su coste con el precio del Bitcoin de diciembre de 2021, se pagaron por ellas la increíble cifra de 460 millones de dólares estadounidenses. Eso es mucho dinero. Pero el receptor de los 10.000 Bitcoin ya los ha gastado también. En una entrevista declaró que había vendido los Bitcoin poco después para pagar un viaje por carretera - al precio actual de Bitcoin - probablemente también el viaje por carretera más caro de la historia de la humanidad.

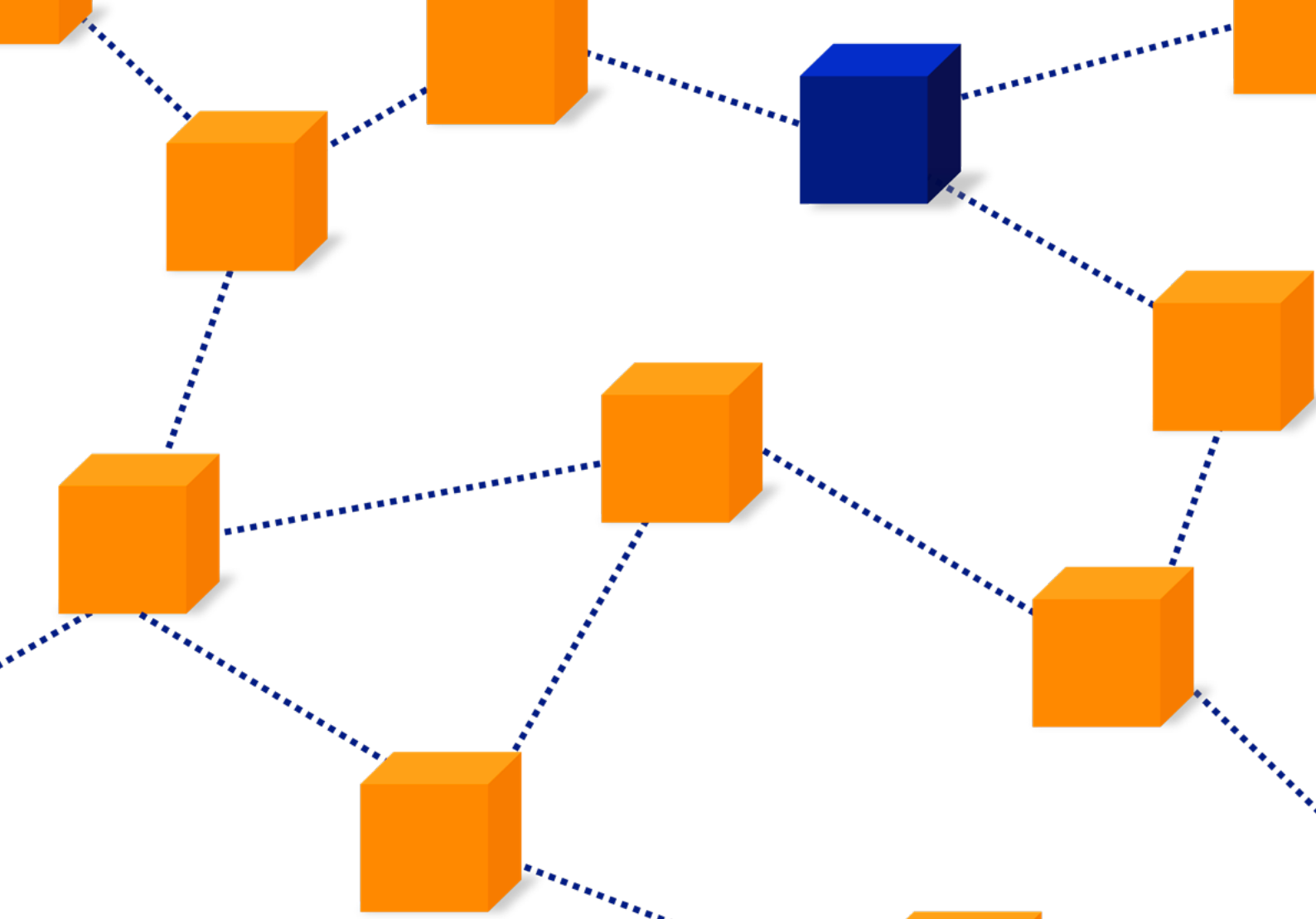
El „Día de la Pizza“ de Bitcoin también ilustra de forma impresionante por qué el ‚hodling‘ - derivado de ‚to hold‘ (conservar o mantener en inglés) - es tan popular entre los Bitcoiners. “Hodling” significa conservar los Bitcoin durante largos periodos de tiempo con la intención de (posiblemente) no venderlos nunca. Después de todo, ¿quién quiere gastar sus bitcoins hoy cuando podrían valer el doble, el triple o incluso diez veces más en los próximos años?

¿CÓMO FUNCIONA BITCOIN?

Después de conocer la historia de Bitcoin, ahora nos sumergiremos en su modo de operar. El objetivo es entender cómo funciona la red Bitcoin, qué problemas resuelve y cuáles son sus beneficios prácticos.

La intención de Bitcoin es ser una red descentralizada. Ningún participante de la red debe ser capaz de gobernar la red por sí solo; el poder de decisión y la supervisión se distribuyen entre todos los participantes. Esto es importante porque ningún individuo, ningún gobierno y ninguna empresa puede cambiar la red de forma independiente, sino que los cambios sólo son posibles de forma colectiva.
Bitcoin funciona de tal manera que cada participante de la red tiene una copia idéntica del libro mayor más actualizado en todo momento - como resultado, todo el mundo sabe siempre quién posee actualmente qué bitcoins. Por lo tanto nadie puede afirmar que posee más bitcoins de los que tiene, porque cada participante de la red puede comprobar esta afirmación con su copia del libro mayor y demostrar que es falsa.

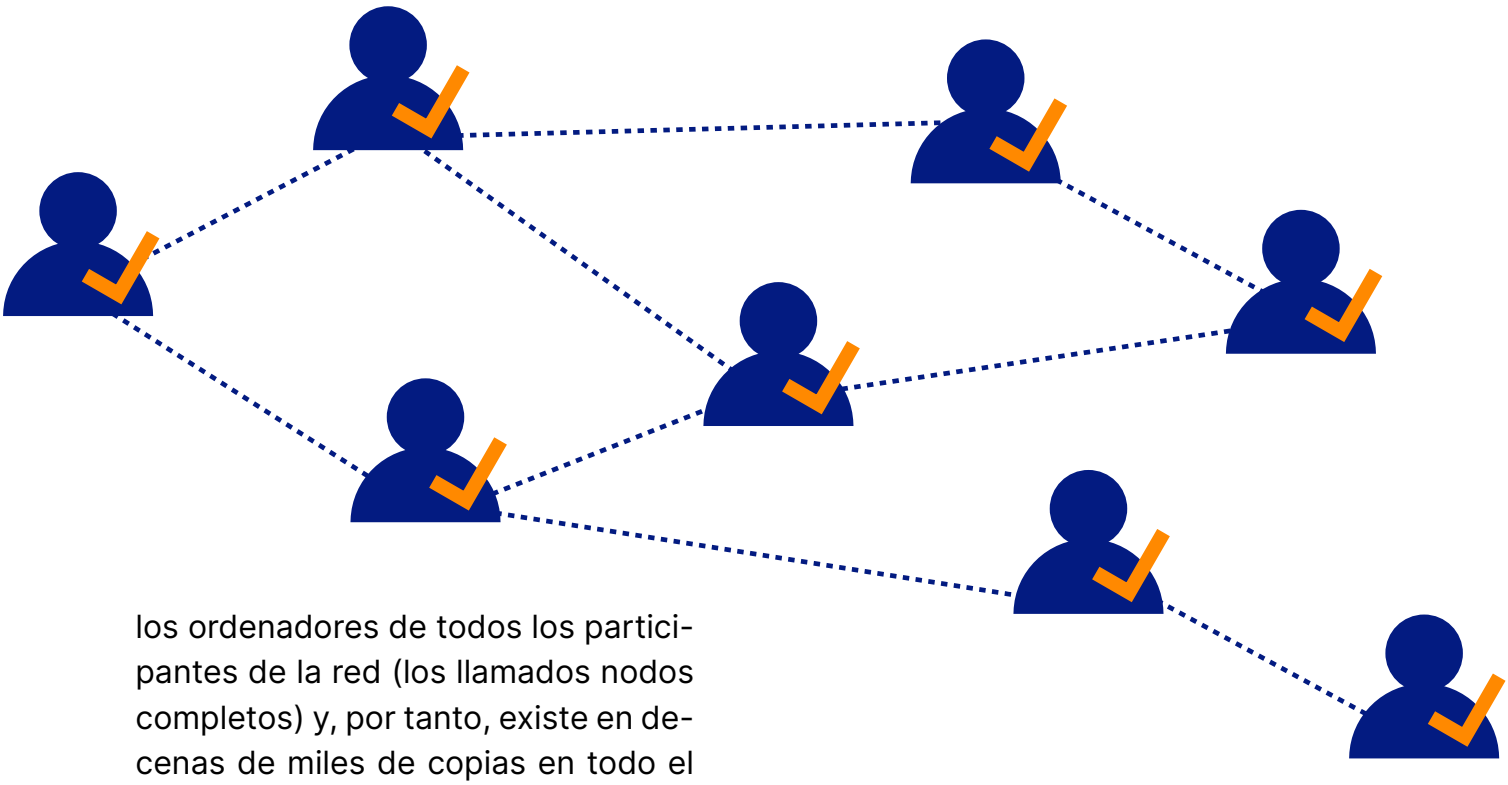
Antes del lanzamiento de Bitcoin las redes descentralizadas se enfrentaban a dos grandes retos: en primer lugar, cómo se podía garantizar que todos los participantes recibieran las últimas actualizaciones sobre los cambios de propiedad, es decir, la información sobre qué bitcoins se habían transferido y a quién. Y en segundo lugar, cómo podían los participantes verificar con absoluta certeza que la información que recibían era correcta.



La Cadena de Bloques (Blockchain)

Estas dificultades se han superado gracias a la invención de la cadena de bloques o "blockchain". Una "blockchain" 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 la "blockchain" de Bitcoin. Cualquier participante de la red que quiera saber a quién pertenece cada Bitcoin puede rastrear el historial de transacciones en la "blockchain" de Bitcoin y determinar exactamente quién posee cuántos bitcoins en la actualidad. Así, si alguien quiere enviar un bitcoin, cualquiera puede comprobar si ese bitcoin pertenece realmente 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 franco suizo el banco consulta el historial de transacciones para ver si el franco sigue perteneciendo al cliente o si ya ha sido gastado (enviado a otra persona). Sin embargo, la característica única de una "blockchain" es que esta información no se almacena en un servidor central del banco, sino en



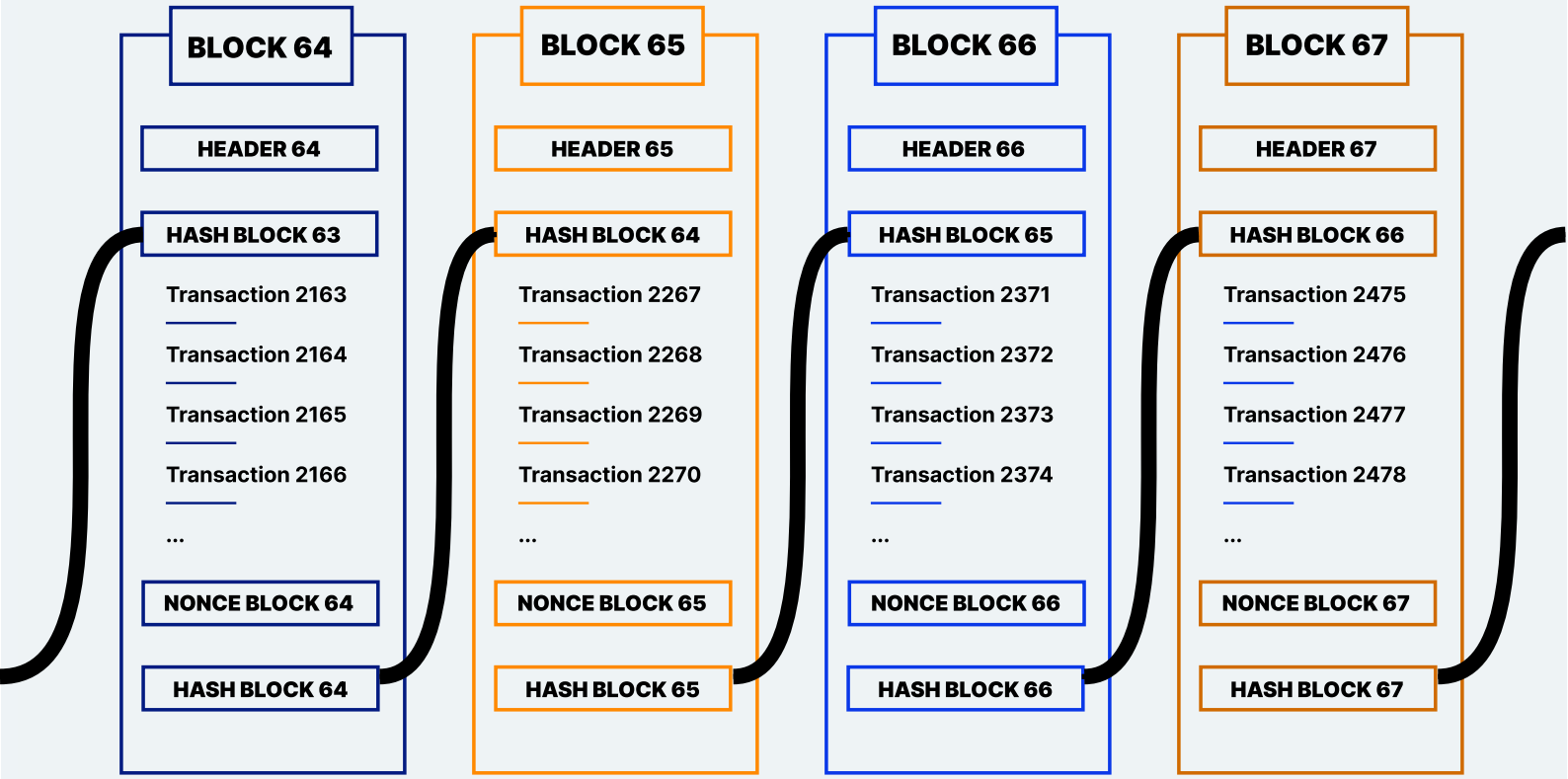
los ordenadores de todos los participantes de la red (los llamados nodos completos) y, por tanto, existe en decenas de miles de copias en todo el mundo. Esta es también la razón por la que Bitcoin no puede borrarse sin más: para hacerlo habría que eliminar la copia de la cadena de bloques de todos los ordenadores participantes del mundo al mismo tiempo.

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

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

La Prueba de Trabajo (Proof-of-Work) y la Minería de Bitcoin

Además, la red Bitcoin tiene un mecanismo para limitar la adhesión de nuevos bloques. Si cualquiera pudiera añadir en cualquier momento nuevas transacciones y bloques a la cadena de bloques la red acabaría en el caos, ya que la "blockchain" no podría actualizarse en todo el mundo de la misma forma con la suficiente rapidez.



La cabecera, el resultado de la función hash del bloque anterior, junto a 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.

Para evitar esto Bitcoin funciona con un mecanismo de prueba de trabajo. Para que alguien se gane el derecho a añadir un nuevo bloque a la cadena de bloques debe aportar una prueba de trabajo. Una simple ilustración de este proceso es un grupo de personas buscando agujas en un pajar. El primero que encuentre una aguja podrá añadir un nuevo bloque a la"blockchain". Además, el descubridor es recompensado con nuevas unidades de Bitcoin y con la suma de todas las comisiones de transacción contenidas en ese bloque. Tan pronto como el bloque se haya unido a la cadena, este proceso comienza de nuevo para el siguiente bloque.

En la realidad, los mineros ejecutan una función hash matemática (algoritmo hash SHA-256) en la búsqueda de números específicos. El número hash del bloque anterior, las transacciones del bloque actual y un número aleatorio (nonce) se combinan en un hash. El número aleatorio se modifica 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: 000000000000000590fc0f3eba193a278534220b2b37e9849e1a770ca 959.

Es decir, un bloque consta de 3 partes:

- Cabecera: el número hash del bloque anterior.
- Cuerpo: las transacciones del bloque.
- Parte final: respuesta a una incógnita de un complejo problema matemático. Es el número aleatorio (un solo número único) que buscan encontrar los mineros.

El problema matemático de la parte final del bloque se trata de una ecuación muy compleja cuya única solución no puede calcularse de forma sistemática mediante una fórmula. Solo es posible calcular su resultado probando distintos números uno a uno. Además, dicha solución funciona de tal manera que hace que el hash del bloque entero (cabecera, cuerpo y parte final) arroje un número de bits determinado con un mínimo de ceros a la izquierda, como hemos comentado previamente. El símil de buscar la aguja en el pajar viene precisamente de la probabilidad mínima y la gran dificultad que tiene resolver una ecuación matemática tan compleja simplemente probando distintas soluciones y números uno a uno.

La búsqueda de este número (la solución del problema matemático), también llamada minería, tiene dos funciones principales: en primer lugar, enlaza los bloques de forma criptográfica-matemática para que todo el mundo pueda verificar fácilmente el orden correcto de la cadena, y al mismo tiempo el mecanismo de la prueba de trabajo hace casi imposible cambiar este orden. En segundo lugar, este mecanismo retrasa la incorporación de nuevos bloques de modo que, de media, sólo se añade un nuevo bloque a la “blockchain” cada 10 minutos aproximadamente. Así, todos los participantes de la red en todo el mundo tienen tiempo suficiente para actualizarse al mismo y al último estado de la cadena de bloques.

En resumen, los mineros mantienen la red Bitcoin en funcionamiento. Gracias a ellos las nuevas transacciones se procesan y se añaden a la blockchain. Los nodos completos guardan copias del libro mayor, se aseguran de que se cumplan las normas y garantizan que no entren transacciones fraudulentas en la blockchain.

21 millones de Bitcoin

Aunque constantemente se añaden más bloques a la “blockchain” de Bitcoin y 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 el principio. Más bien son liberadas de acuerdo al código de Bitcoin siguiendo un estricto calendario de emisión.

Cuando se lanzó Bitcoin, el código

liberaba 50 nuevos Bitcoin a los mineros aproximadamente cada 10 minutos (como recompensa por minar 1 bloque). Cuatro años después del lanzamiento el número de Bitcoin liberados cada diez minutos se redujo a la mitad. Este proceso se denomina „halving“ y describe el hecho de que la recompensa por bloque para los mineros disminuye a la mitad cada 4 años. Actualmente ya hay 19 millones de Bitcoin en circulación. El resto de bitcoins se minarán hasta el año 2140. Después de eso los mineros sólo serán recompensados a través de las tasas de transacción.

La cantidad estrictamente limitada de unidades de Bitcoin es una de las propiedades fundamentales de la criptodivisa y hace de Bitcoin una mercancía extremadamente escasa. Esta escasez digital absoluta es también un requisito importante para que Bitcoin funcione como depósito de valor durante largos periodos de tiempo y es la razón por la que a menudo se llama a Bitcoin oro digital u oro 2.0.

El resultado: La propiedad digital

Examinando todas las características de la red de Bitcoin en su conjunto se puede ver la importancia de esta invención. Por primera vez en la historia existe un bien digital que sólo está disponible en un número estrictamente limitado. Los bitcoins no pueden copiarse ni duplicarse.

Gracias a este logro, Bitcoin se denomina a menudo propiedad digital. Porque al igual que cada pedazo de tierra de este planeta es único y existe sólo una vez, cada unidad de Bitcoin también es única y existe sólo una vez en el espacio digital.

Y estas unidades de Bitcoin pueden ser realmente propiedad. Sólo la persona que posee la clave privada correspondiente, que es una combinación de números y letras de 64 caracteres, puede mover los bitcoins en posesión. En otras palabras, sin esta clave privada Bitcoin no puede ser robado, confiscado o bloqueado. Esto permite al propietario tener un control absoluto sobre sus recursos financieros independientemente de si es un millonario, un refugiado político o un acreedor perseguido. Por primera vez desde la invención del ordenador, es posible poseer realmente activos digitales.

¿POR QUÉ BITCOIN?

Pero, ¿por qué todo este revuelo en torno a Bitcoin? La posibilidad de poseer realmente un activo digital puede ser revolucionaria, pero en primer lugar, ¿por qué querría alguien poseer Bitcoin?

Lo mejor de ambos mundos

En siglos pasados se utilizaban como medios de pago los metales preciosos, y posteriormente el dinero en efectivo en forma de monedas y billetes. Estos tenían la ventaja de que podían almacenarse y gastarse con independencia de terceros. El dicho „el dinero en efectivo es la libertad impresa“ lo resume muy bien. Sin embargo, la desventaja de los metales preciosos y del dinero en efectivo es que son difíciles de utilizar en el espacio digital de Internet. Por ello, desde la llegada de las compras en línea las tarjetas de débito y crédito se han impuesto entre la población.

Pero ahora que la mayoría de la gente utiliza dinero digital en cuentas bancarias en lugar de efectivo los riesgos de contrapartida a los que se enfrentan son cada vez mayores. Si por ejemplo una entidad financiera se declara insolvente, los ahorros de los clientes podrían perderse. O, como ocurrió en Chipre en 2013, si se limitan drásticamente las retiradas de efectivo, se establecen controles de capital y se produce una expropiación forzosa de las cuentas de ahorro, la gente deja de tener el control de su dinero. O, como ocurre actualmente en muchos países occidentales, si a los clientes de la banca no se les permite enviar dinero a sus familiares porque viven en Cuba o en Irán, dependen de que un tercero apruebe todas sus transacciones.

Con el paso del dinero en papel al digital almacenado en cuentas bancarias, en última instancia ya no tenemos el control de nuestro propio

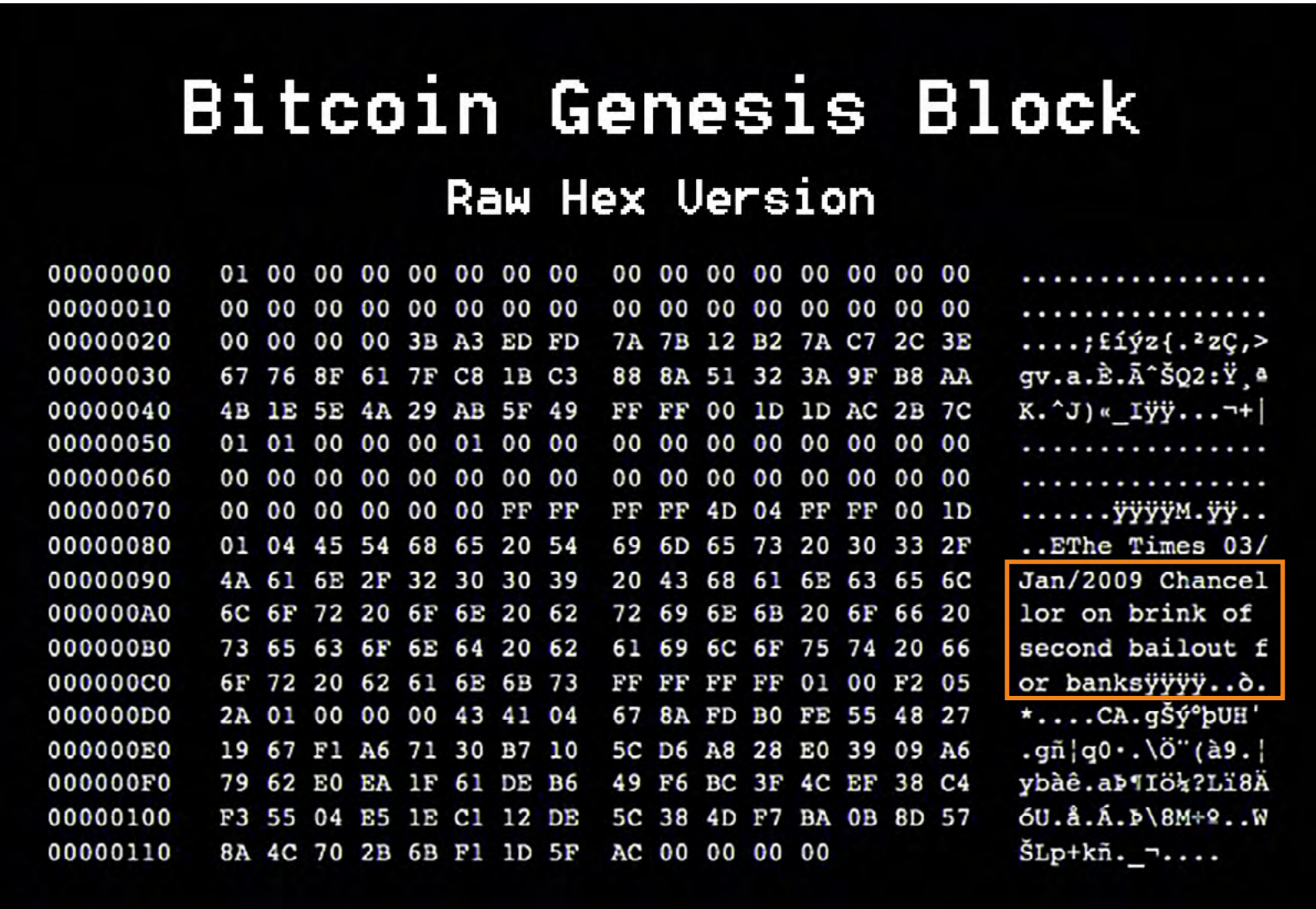
dinero. Hasta ahora, sin embargo, este inconveniente ha sido el precio que hemos tenido que pagar para participar en una vida digitalizada.

Bitcoin ofrece una solución a este dilema. Como dinero digital es ideal para usarse en el espacio digital, y al mismo tiempo Bitcoin puede almacenarse como propiedad digital sin tener que depender de terceros (bancos) para su custodia. Así, los propietarios de Bitcoin pueden guardar sus monedas -en forma de claves privadas- bajo el colchón o donde crean que es más seguro.

En el momento justo

Bitcoin se creó en medio de la crisis financiera mundial de 2008/09. En el primer bloque de la cadena de bloques de Bitcoin -también llamado bloque Génesis- Satoshi Nakamoto dejó un mensaje contundente. Citó un titular publicado en el periódico The Times que decía: „El canciller al borde del segundo rescate bancario“.

Con este hecho Satoshi expresó la filosofía crítica con el Estado de los Cypherpunks. En la crisis financiera de 2008 los bancos centrales pusieron en circulación grandes cantidades de dinero recién creado para salvar a los bancos. Al final, sin embargo, los ahorradores pagaron por ello, ya que



sus ahorros perdieron valor al diluirse por el exceso de oferta monetaria. Este hecho reafirmó una vez más a los Cypherpunks en su desconfianza hacia el Estado y los bancos centrales y reforzó su convicción de que se necesitaba urgentemente un dinero independiente del Estado.

El mismo procedimiento, sólo que a mayor escala, se ha repetido desde el estallido de la pandemia de Covid-19. Sólo en 2020 la masa monetaria de Estados Unidos se amplió en un 50%, y en otros países -incluida Suiza- la imprenta digital funciona constantemente. Una consecuencia directa de esto son los bajos tipos de interés récord -incluso tipos de interés negativos en Suiza- y la fuerte inflación de los activos.

Cobertura contra la Devaluación de la Moneda

Por tanto, Bitcoin se lanzó en el mejor momento posible. Pocas veces el tema del dinero ha sido más relevante y los interrogantes más grandes que en la actualidad. Con su oferta limitada de 21 millones Bitcoin ofrece un agradable contraste con los balances de los bancos centrales, que crecen sin cesar. Su oferta limitada ofrece protección contra la dilución del capital personal, como se ha observado con todas las monedas del mundo en las últimas décadas.

Debido a su configuración específica, Bitcoin está diseñado para garantizar la preservación del poder adquisitivo durante largos períodos. Dado que Bitcoin es limitado, debería ser incluso mejor en esta tarea que el oro, que tiene una entrada neta del 1-2% cada año. 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 del valor a lo largo del tiempo.

Protección de la Propiedad

Otro problema que mitiga Bitcoin es la protección de la propiedad. Mientras que el oro o el dinero en efectivo suelen tener que ser almacenados de forma segura y con un gran coste para protegerlos de los robos, Bitcoin puede ser almacenado y transportado con un coste prácticamente nulo. Incluso cantidades importantes pueden llevarse a cualquier parte del mundo con un código formado por doce o veinticuatro palabras. Una vez memorizado y destruido físicamente, este código no puede ser robado por nadie, lo que hace que los bitcoins detrás del código estén seguros y permite a su propietario llevárselos a la tumba si lo desea.

COMPRA DE BITCOIN

Hay dos maneras de conseguir bitcoins. O bien se gana bitcoins como minero, o bien se compran bitcoins 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 principiantes es comprar bitcoins a alguien.

Plataformas de Cambio de Criptomonedas & Brokers

La forma más fácil de comprar Bitcoin es a través de una plataforma de cambio de criptomonedas o de un broker. Estos funcionan de forma similar a las bolsas de acciones. Después de abrir una cuenta personal se pueden transferir francos suizos, euros o dólares estadounidenses mediante transferencia bancaria o tarjeta de crédito. Una vez que el dinero ha llegado a la cuenta personal en la casa de intercambio, se puede comprar Bitcoin las 24 horas del día con unos pocos clics al precio actual del mercado. En Europa es posible comprar Bitcoin sin necesidad de registrarse, verificarse o depositar dinero primero con la popular aplicación de inversión exclusiva en Bitcoin Relai.

Peer-to-peer

Como alternativa a las casas de cambio de criptomonedas, el Bitcoin también puede comprarse directamente a otros participantes en el mercado a través de plataformas peer-to-peer sin necesidad de un intercambio. Esto permite un mayor anonimato, ya que no hay que revelar datos personales en el proceso.

Cajeros de Bitcoin

También existe la posibilidad de retirar Bitcoin a través de cajeros automáticos. Estos ya están disponibles en muchos países como Suiza, Alemania y Austria. En los cajeros automáticos de Bitcoin se puede retirar Bitcoin de forma anónima con dinero en efectivo o tarjeta de crédito. No es necesario tener una cuenta ni un monedero de criptomonedas.

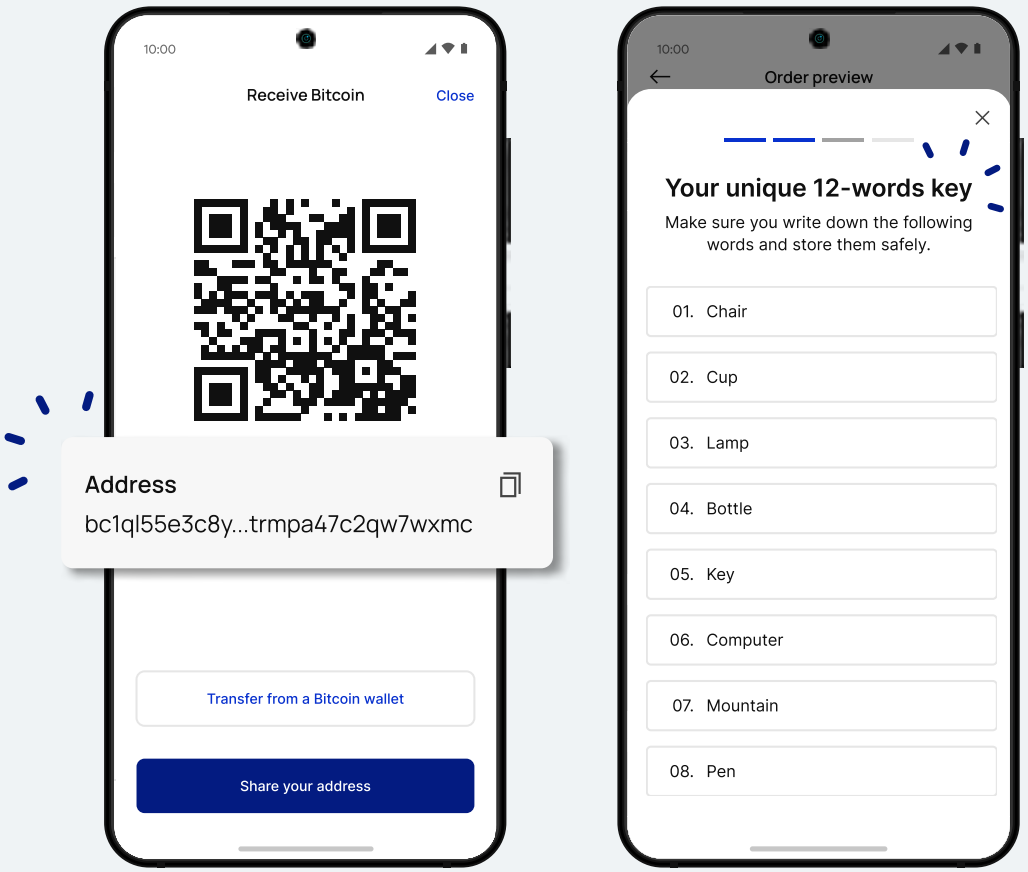
Almacenar Bitcoin de forma segura

Una vez adquiridos los bitcoins surge la cuestión de su custodia y almacenamiento de forma segura. Bitcoin y las criptomonedas se rigen por el principio: „si no son tus llaves (privadas), no son tus monedas“. Para ser realmente propietario de tus bitcoins, debes estar en posesión de las correspondientes claves privadas. Esta expresión, un tanto técnica, significa que tú sólo tienes realmente el control de tus bitcoins si los almacenas en un monedero digital personal del que tienes las claves privadas.

Mientras los bitcoins estén depositados en una plataforma de intercambio de criptomonedas, estarán bajo el control de la plataforma. Si la plataforma de intercambio es hackeada, quiebra o es fraudulenta, los bitcoins podrían perderse para siempre.

La Auto-Custodia

A diferencia de una cuenta bancaria, Bitcoin te da la opción de almacenar tus unidades monetarias en un monedero personal. Esto te permite ser tu propio banco y tiene la ventaja de que tienes un control absoluto sobre tus bitcoins. A cambio esto también conlleva responsabilidades. Las claves privadas, que a menudo vienen en forma de doce o veinticuatro palabras, deben ser almacenadas y mantenidas a salvo por el propio propietario de los respectivos bitcoins. Un manejo incorrecto o negligente puede llevar a la pérdida irremediable de los bitcoins.



Monederos: Monederos digitales

Los monederos digitales ayudan a almacenar de forma segura los bitcoins, o más exactamente, las claves privadas. Los bitcoins en sí siempre se almacenan en la cadena de bloques y no pueden ser transferidos a un monedero. Sólo las claves de acceso a los Bitcoin pueden almacenarse en un monedero.

Por ello, los monederos se crearon para almacenar las claves privadas de forma segura y sencilla. Además permiten enviar y recibir bitcoins con unos pocos clicks. Por lo tanto, los monederos son una valiosa herramienta para el control y uso de Bitcoin.

Monedero Software

Los monederos más comunes son los monederos por software. Los monederos por software pueden configurarse como aplicaciones de escritorio o como aplicaciones para teléfonos inteligentes. Durante la configuración las claves privadas del monedero se enumeran en forma de doce o veinticuatro palabras (frase semilla). Estas palabras son sinónimo de Bitcoin en ese monedero. Quien conoce estas palabras tiene el control de las monedas. Por lo tanto, las palabras deben ser escritas de forma analógica, preferiblemente en papel, en secreto y guardadas de forma segura. Si el ordenador o el smartphone se pierden o son robados, el monedero puede ser restaurado en cualquier momento con estas palabras.

Los monederos por software tienen la ventaja de que se pueden configurar rápidamente y son fáciles de usar. Sin embargo, como los monederos por software son programas informáticos instalados en un dispositivo y conectados directamente a Internet siempre existe el riesgo de ataques de hackers.

Monedero Hardware (Carteras Frías)

Si valoras la seguridad deberías utilizar un monedero de hardware. Estos pequeños dispositivos almacenan los códigos de acceso para Bitcoin en un dispositivo similar a una memoria USB que sólo se conecta al ordenador cuando se necesita. El dispositivo está diseñado de tal manera que incluso un ordenador infectado con software malicioso no puede acceder a los códigos.

Al configurar un monedero hardware se generan doce o veinticuatro palabras (frase semilla), que deben anotarse de forma analógica y guardarse en un lugar seguro. Si alguna vez se pierde el monedero hardware, se puede restaurar con la ayuda de las palabras. Algunos ejemplos de monederos físicos son BitBox , Ledger y Trezor.

Made in Switzerland

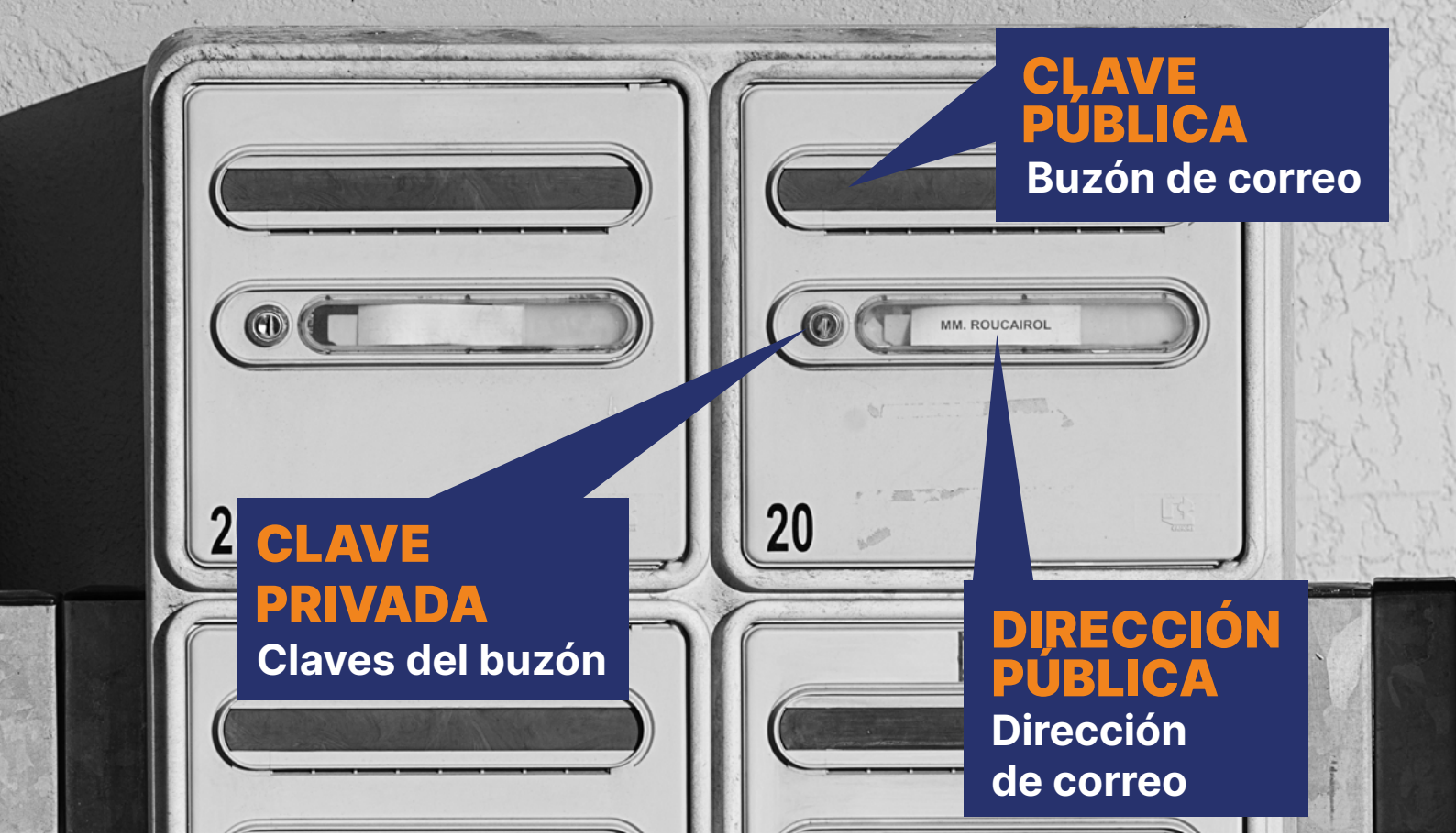
EUROPE'S EASIEST BITCOIN APP

Relai

Download on the App Store

GET IT ON Google Play

Buy bitcoin in 1 minute from as little as 10 EUR/CHF without verification.



Envío y recepción de Bitcoin

Enviar y recibir Bitcoin es muy fácil. Cada monedero Bitcoin tiene su dirección pública generada a partir de la llamada clave pública. Esta sirve como dirección de recepción, similar a un IBAN. Cualquiera que tenga esta dirección puede enviar Bitcoin al monedero correspondiente. La dirección suele mostrarse como un código QR, lo que simplifica aún más el manejo.

Si quieres enviar Bitcoin a alguien tienes que introducir la dirección Bitcoin del destinatario en tu monedero en „enviar“ o escanear el código QR correspondiente. Los gastos de la transacción se deducen automáticamente del monedero del remitente. El importe de las tasas de transacción varía en función de la carga de la red y puede consultarse aquí. La transferencia tarda una media de 10 minutos en llegar al destinatario. Sin embargo, también puede tardar más dependiendo del importe de tasas de transacción que se esté dispuesto a pagar.

Pagos con Bitcoin

Cuando se creó Bitcoin se esperaba que algún día se pudiera utilizar para pagar los productos cotidianos. Y en teoría esto es posible hoy en día. Algunos departamentos fiscales del gobierno, 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 Bitcoin pueden costar varios euros y tardar al menos 10 minutos, esto sólo tiene sentido para transferir grandes cantidades de dinero. Para enviar Bitcoin de forma barata y rápida se necesita una solución alternativa.

La red de Lightning network: “La red relámpago” - más rápida y más barata

Por ello se construyó una capa adicional sobre la red Bitcoin. Esta red, llamada Lightning, permite pagar con Bitcoin en segundos a un coste mínimo. En países como El Salvador la red Lightning ya se utiliza con éxito.

Por lo tanto, en el futuro, el pago de productos cotidianos con Bitcoin se realizará en gran medida a través de la red Lightning. Los desarrollos en este ámbito van a toda velocidad. Twitter, por ejemplo, ha introducido recientemente una función de „propina“ que utiliza la red Lightning. Además, la aplicación Strike ofrece pagos en todo el mundo en varias monedas a coste cero a través de la red Lightning. Por lo tanto es de esperar que en el futuro sólo las cantidades más grandes se liquiden directamente a través de la red Bitcoin, mientras que el resto de las transacciones se ejecutarán a través de la red Lightning.

Dado que los importes más pequeños se envían principalmente a través de la red Lightning, se utilizan Satoshis (o Sats de forma abreviada) como unidad de cuenta en lugar de Bitcoin. 1 Bitcoin equivale a 100.000.000 Satoshis.

Para utilizar la red Lightning es necesario crear un monedero Lightning.

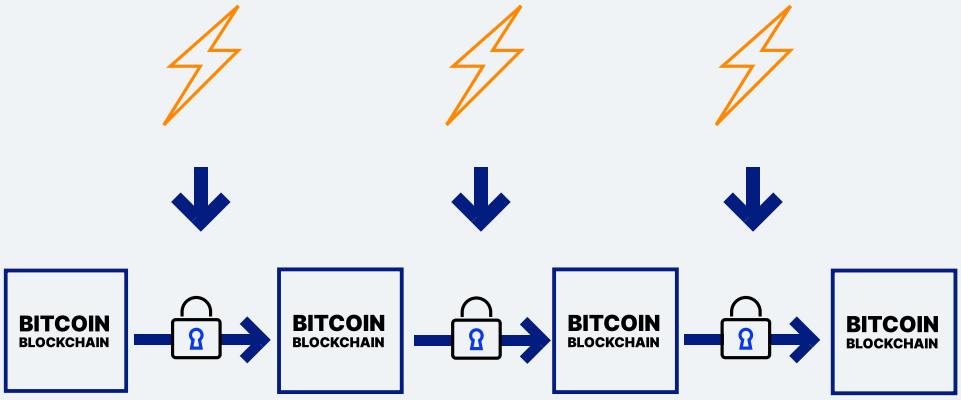
UNA MIRADA HACIA EL FUTURO

En sus más de diez años de existencia Bitcoin ha pasado por muchos altibajos. La criptomoneda fue declarada muerta o sumida en el olvido entre el público en general en varias ocasiones tras fuertes caídas de precio. Sin embargo, Bitcoin se ha extendido inexorablemente por todo el mundo durante la última década.

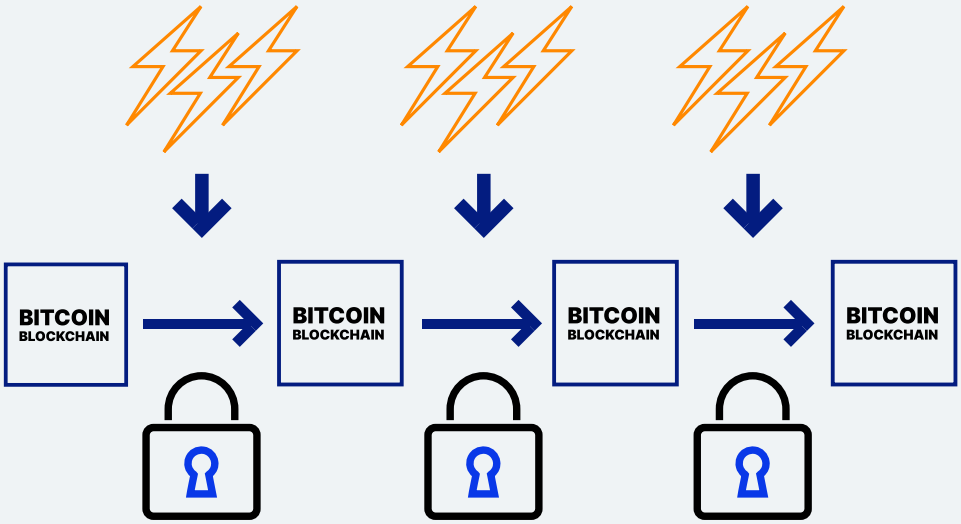
Bitcoin y Energía

Una de las primeras preocupaciones que se plantean a menudo en relación con el desarrollo de Bitcoin es el consumo de energía de la red Bitcoin. La minería de Bitcoin ya 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.

Cuanta menos energía en forma de potencia de cálculo se utilice para crear la Blockchain de Bitcoin, más fácil será alterarla posteriormente.



Cuanta más energía en forma de potencia de cálculo se utilice para crear la Blockchain de Bitcoin, más difícil será alterarla posteriormente



Cuando se habla de Bitcoin y energía es importante entender que la cantidad de energía que fluye en la red Bitcoin es crítica para la seguridad de la red. Cuanta más energía fluya en la red, más segura será. Esto se debe a que, para que la "blockchain" de Bitcoin sea alterada, la misma cantidad de potencia de cálculo - y por lo tanto de energía - que se invirtió para crear la cadena de bloques en primer lugar debe ser gastada de nuevo. Sin embargo, con millones de ordenadores en todo el mundo proporcionando potencia de cálculo a la red Bitcoin, es casi imposible que un individuo, una organización o un estado pueda reunir suficiente potencia de cálculo para realizar incluso los más pequeños cambios en la blockchain. Por lo tanto, el "hashpower" y el consumo de energía asociado es una importante característica de seguridad de la red Bitcoin.

Además, los ordenadores de minería de Bitcoin tienen la ventaja de que pueden estar ubicados en cualquier parte del mundo. Dado que los mineros necesitan la electricidad más barata posible para ser rentables, suelen ubicarse en lugares donde hay muchos excedentes, y por lo tanto ener-

gía barata. A largo plazo, es probable que esto ocurra en lugares donde hay mucha energía renovable, ya que ésta produce la electricidad más barata.

Según el Consejo de Minería de Bitcoin, los mineros de Bitcoin utilizan actualmente un 56% de energía renovable y la tendencia va en aumento. Muchos expertos en Bitcoin creen que la minería de Bitcoin se alimentará de hasta el 100% de energía renovable en el futuro.

Sin embargo, hasta que esto ocurra, el consumo de energía de Bitcoin se reduce a la cuestión de si un dinero y un depósito de valor seguros e infalsificables merecen o no este gasto de energía.

El Salvador - Bitcoin como Moneda Nacional

Hace unos años los visionarios ya pensaban que era posible que Bitcoin fuera reconocido algún día como moneda de curso legal por los Estados. En el verano de 2021 llegó el 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 el pago no solo puede hacerse con dólares estadounidenses, sino también con Bitcoin. Para ello, se proporcionó a los ciudadanos un monedero de Bitcoin personalizado que permite realizar pagos a través de la red Lightning en cuestión de segundos y a un coste mínimo.

Otros países como Ucrania, Brasil y Panamá están debatiendo actualmente proyectos de ley similares. Si otros países siguieran el ejemplo de El Salvador, esto aumentaría, por un lado, la demanda de Bitcoin y, por otro, reforzaría la credibilidad de Bitcoin como „dinero“. La aceptación de Bitcoin como moneda de curso legal en más y más países, por lo tanto, representa una fase decisiva en el proceso de adaptación global de Bitcoin.

Leyes y Regulaciones

Esta evolución ha hecho que los Estados, los bancos centrales y las empresas tengan que ocuparse intensamente de las criptomonedas. Varios Estados, entre ellos Suiza, han publicado reglamentos y directrices sobre las criptomonedas. Este hecho es bien recibido por muchos participantes en el mercado, ya que crea seguridad jurídica tanto para los proyectos de criptomonedas como para los inversores implicados.

Las regulaciones también están en el horizonte en los EE.UU., que hasta ahora ha adoptado un enfoque de laissez-faire. La comunidad global de criptomonedas está siguiendo de cerca la forma exacta que tomarán estas nuevas leyes de regulación en los Estados Unidos, ya que tendrán un gran impacto en todo el sector de las criptomonedas.

Otras criptomonedas

El Bitcoin no es ni mucho menos la única criptodivisa actual. Actualmente existen más de 16.000 criptomonedas y activos diferentes. Estas monedas y tokens tienen diferentes características y funcionalidades y no todas han sido diseñadas como „monedas“ o dinero. Algunas se parecen más a las acciones, en el sentido de que su valor refleja el éxito de un cripto-proyecto. Otros son necesarios para hacer uso de un servicio concreto. Y otros - los llamados tokens meme - son principalmente monedas de diversión.

Por lo tanto, para evitar pérdidas, es aconsejable examinar detenidamente la moneda en cuestión y el proyecto que la respalda antes de realizar cualquier inversión.

Monedas Digitales de Bancos Centrales (MDBC - CBDC en inglés)

Las criptodivisas están actualmente en transición, pasando de una fase de Salvaje Oeste no regulada a un mundo de cripto-finanzas regulado. Esta evolución no ha dejado indiferentes a los bancos centrales, y se ha planteado la idea de que estos emitan sus propias criptodivisas. Estas „monedas digitales de los bancos centrales“, o CBDC en sus siglas en inglés, combinarán, según sus defensores, la estabilidad de una moneda estatal con los beneficios de una moneda basada en blockchain. En resumen, crearían dinero digital, por así decirlo.

Sin embargo, dependiendo de su diseño, una CBDC puede adoptar formas fundamentalmente diferentes.
Varios países han puesto en marcha pruebas piloto con diferentes tipos de CBDC. Sin embargo, se espera con impaciencia si las zonas monetarias económicamente fuertes, como EE.UU, la UE o China lanzarán sus CBDC y de qué forma.

Competencia por el dinero

Nuestra sociedad se ha acostumbrado tanto a las monedas estatales en las últimas décadas que hasta hace poco era difícil imaginar otros tipos de dinero para muchos. Pero no hace tanto tiempo formaba parte de la vida cotidiana la circulación paralela de diferentes tipos de dinero. Había billetes de varios bancos, monedas de diferentes metales y otros valores monetarios que podían utilizarse como medio de pago.

Con Bitcoin las monedas no estatales vuelven a estar disponibles como alternativa a las estatales. Hasta ahora la mayoría de los gobiernos han tolerado Bitcoin. Hasta cierto punto, esto podría ser gracias a su naturaleza descentralizada, que hace que Bitcoin sea difícil de atacar. Para los ciudadanos esto significa que ahora existe una alternativa digital al dinero estatal junto con el oro y la plata. Será interesante observar los efectos de esta competencia monetaria adicional en el futuro.

BITCOIN, ¿Y AHORA QUÉ?

Si te estás preguntando qué deberías hacer con toda esta información, permíteme hacerte una sugerencia. Entrar en el mundo de Bitcoin no cuesta nada, ni tiempo ni dinero, pero conocerás una tecnología que está a punto de cambiar nuestro mundo y el futuro.

Por lo tanto: crea una cuenta en una casa de cambio de criptomonedas, descarga un monedero en tu smartphone y compra Bitcoin por 50 euros, o haz que un colega te envíe Bitcoin a tu monedero, pero intenta tener en tus manos Bitcoin al menos una vez.

Porque si Bitcoin da el salto y se convierte en algo tan omnipresente como Internet, no sólo lo conocerás teóricamente, sino que habrás utilizado Bitcoin tú mismo. A veces esto marca la diferencia, ya que te da una visión y una experiencia de la tecnología, lo que te pone por delante de la mayoría de la gente.

SOBRE EL AUTOR

Daniel Jungen es un economista y periodista financiero experto en criptoactivos. Daniel es cofundador de InsightDeFi, una boutique de investigación especializada en todo lo relacionado con las criptomonedas. Junto con sus socios en InsightDeFi publican un informe quincenal (en alemán) sobre Bitcoin, DeFi y Crypto.

RELAI

Fundada en Suiza por Julian Liniger y Adem Bilican después de luchar por encontrar un espacio seguro y sin complicaciones para comprar bitcoins, Relai está haciendo que el ahorro y la inversión en bitcoins sean accesibles para todos. La aplicación para bitcoins está diseñada para ser sencilla e intuitiva, y permite a cualquier persona en Europa comprar y vender bitcoins en cuestión de minutos sin necesidad de registro, verificación o depósitos. Auditada de forma independiente y con más de 35 millones de francos suizos invertidos a través de su plataforma, Relai ofrece a los consumidores la posibilidad de acceder a nuevos medios de ahorro e inversión.

Aprende más en Relai.app.

Gracias a @la_cryptonita que tradujo este libro electrónico del inglés al español. Encuentra su canal de YouTube sobre Bitcoin aquí