Material para el curso

“Bitcoin y tecnologías blockchain”

para el Centro de Enseñanzas Virtuales de la Universidad de Granada.

Presentación

Quiero darte la bienvenida a la primera edición de este curso online de Bitcoin y tecnologías blockchain.

En este curso se pretende mostrar una introducción a las tecnologías blockchain usando como ejemplo central Bitcoin.

Aunque hablaremos de otras redes, especialmente de Ethereum, vamos a centrar casi todo el esfuerzo en entender Bitcoin desde el punto de vista económico, técnico y operativo.

Eso significa que va a haber un montón de teoría y de trabajo de documentación, aunque trataremos de que sea lo menos pesado posible.

También habrá una parte práctica, y tendremos que instalar programas y usar nuestros propios monederos para hacer transferencias, recibiendo y enviando bitcoins.

Este curso está orientado a un público muy amplio, por lo que no puede entrarse en profundidad en algunos aspectos, especialmente los más técnicos. Aunque se proveen enlaces y otros recursos para poder investigar, el curso está concebido como una forma de aprendizaje participativa, y te invito a que uses los foros de cada bloque para pedir detalles o explicaciones si lo deseas. También puedes usar esos foros para aportar tus propios conocimientos, experiencia o puntos de vista.

En la medida de lo posible, se ha intentado dejar abiertas todas las opciones para el alumno, no forzándole a usar ningún software o plataforma concretos.

Cuando sean necesarios, los ejemplos de este curso se mostrarán sobre un ordenador con el sistema operativo Linux, y es el que se recomienda por razones de seguridad, estabilidad y confianza, pero el alumno es libre de usar el que prefiera.

Para mostrar el uso del software de monedero se usará el wallet ofical de Bitcoin, que tiene versiones para todos los sistemas operativos pero se hablará también de otros, de nuevo, y el alumno es libre de usar uno distinto (y, probablemente, prefiera hacerlo).

En ningún caso se exigirá o recomendará ningún software, aplicación o plataforma sospechosa de ser insegura o que represente un costo de licencia o uso para el alumno.

Así mismo, tampoco se va aconsejar el uso de ninguna plataforma concreta para la compra o venta de bitcoins u otra moneda aunque, llegado el momento, se pondrá a disposición de los alumnos un foro para que puedan intercambiar opiniones y experiencias al respecto.

El mundo de Bitcoin y las criptomonedas evoluciona a velocidades sorprendentes, y los contenidos de este curso han debido de ser modificados al mismo ritmo en el que se redactaban. Seguramente también haya que actualizarlos durante la duración del curso.

El curso finaliza el 22 de diciembre de 2017. Hasta entonces, cada uno de los módulos se irá activando los lunes al ritmo de uno por semana durante las primeras semanas. El plazo de entrega de los ejercicios y trabajos que se soliciten estará abierto hasta el último día del curso, pero es recomendable no esperar hasta el final e ir haciendo los ejercicios a un ritmo constante.

Los ejercicios no son difíciles, son bastante abiertos en cuanto a su temática y su principal intención es incentivar la investigación individual y la ampliación de contenidos.

Monedas, monedas electrónicas, monedas virtuales y criptomonedas

Historia del dinero

En los siguientes apartados vamos a repasar muy superficialmente la historia del dinero y su funcionamiento. Necesariamente es un resumen impreciso y de trazo grueso, y se han ignorado aspectos que, siendo muy importantes, no son especialmente relevantes en relación a la comprensión del Bitcoin.

Además, se recomienda una breve biografía para quien tenga interés en ahondar más es estos aspectos.

Después veremos qué características tienen y qué usos se les dan a los distintos tipos de monedas hoy día, para luego ver una pequeña introducción a Bitcoin.

La economía familar

Durante la mayor parte de la historia, en la mayor parte de las sociedades, la economía ha funcionado sin dinero, moneda, mercados o, en el sentido técnico, transacción de ninguna clase.

Para empezar, la mayoría de las actividades "económicas" se dan en el seno de la familia. En cualquier sociedad, los miembros de la familia contribuyen a esta en forma de bienes (como, por ejemplo, el producto de la caza en una tribu preagrícola o el sueldo de un trabajador en un país industrial) o servicios (cocina o cuidados, por ejemplo).

En muchas sociedades, además, la familia se hace extensiva, abarcando más allá del la familia nuclear de padre-madre-hijos e incluso alcanzo el nivel de tribu o clan, recurriendo a antiguos y remotos (y, normalmente mitológicos) antepasados comunes.

Economía del don

Cuando un miembro de una sociedad de cazadores-recolectores necesita algo, simplemente se lo pide a su vecino (a un vecino que tenga ese algo, claro), que no tiene más opción que dárselo. Es muy probable que, en el futuro, ese vecino necesite algo y se lo pida al primero, pero eso no es un requisito necesario y, en principio, la reciprocidad no está declarada explícitamente en la solicitud inicial (aunque sí está implícita en el conjunto de valores del grupo social).

No se trata de una transacción en el sentido técnico, porque el bien transmitido no se ofrece como contrapartida a otro (no es un intercambio). Pero sí es una actividad económica porque entraña un redistribución de recursos.

Al describir la llamada "economía del don" de este modo, puede dar la impresión de que se da en algún tipo de ambiente utópico de personas amables y generosas, lo que está totalmente equivocado. Este tipo de intercambios se da en grupos sociales relativamente pequeños, donde las personas se conocen unas a otras y pueden llevar una especie de "registro mental" de la reputación de los demás. Si un miembro de la sociedad tiene fama de no ser lo suficientemente generoso, empezará a recibir menos respuestas positivas a sus solicitudes. En algunas sociedades especialmente violentas, tener mala fama puede ser muy peligroso para una persona. Decimos que la economía del don se basa en la confianza en el sentido de que es necesario que los participantes se conozcan mutuamente y confíen en la reputación del otro.

De estas prácticas nacieron y evolucionaron otras formas más complejas de economía redistributiva, como por ejemplo el potlatch o el kula, la cuales también dependen de un modo u otro de la reputación de los individuos y, por tanto, se basan en la confianza.

Pero todos estos métodos de intercambio no son exclusivos de pueblos antiguos o tribus exóticas, sino que se dan en todas las sociedades: Podemos pensar, por ejemplo, en cómo funcionan socialmente los regalos de cumpleaños para tener un ejemplo en nuestra propia sociedad.

Trueque

La principal limitación de esta forma de economía es que está basada en la confianza y por tanto requiere de un continuo control de la reputación de cada miembro, lo que impide participar a personas ajenas al grupo. ¿Cómo sabe una persona si puede confiar en alguien que no conoce? ¿Por qué hacer un favor a alguien que no has visto nunca y que quizás no vuelvas a ver?

Por eso,las sociedades que basan la gestión de sus recursos en estos sistemas, o bien no intercambian con individuos extraños al grupo o bien tienen sistemas alternativos para hacerlo.

El método más evidente es el trueque: Si se ofrece algo a un desconocido y este, simultáneamente, corresponde con otro bien, ya no es necesario conocerle o confiar en él. pero el trueque tiene sus propios requisitos: Al hacerse de forma simultánea, es necesario que se de la buena suerte de que cada uno de los intervinientes tenga algo que el otro necesita o desea en el mismo momento. Además, el intercambio debe realizarse en un entorno neutral y seguro, para evitar la tentación de robar el bien ajeno sin dar a cambio el propio. Por estas dos razones, el trueque se ha dado más entre grupos que entre individuos: Los miembros de una tribu (normalmente, fuertemente armados) se encuentran en un lugar previamente pactado con los miembros de la otra, y siguen un complejo ritual de ofertas y contraofertas para acabar llegando a un acuerdo. En el trueque, al contrario de lo que hemos visto hasta ahora, siempre está implícito el intento del regateo, de obtener más de lo que se ofrece. El trueque está basado en la desconfianza.

Este punto (el de la desconfianza) es importante y será relevante al hablar de Bitcoin: Probablemente la mayoría de las transacciones son entre personas perfectamente honradas y amables, pero el intercambio no puede basarse en esa premisa.

Dinero

El dinero se inventó en Mesopotamia en torno al 2500 A.E. aunque la moneda no aparecería hasta casi 2000 años más tarde.

Con el surgimiento de los primeros estados las transacciones entre desconocidos se hacen más habituales, y el surgimiento de los templos y los palacios como grandes centros de poder funcionarial permitió llevar registros contables y diarios de la actividad económica (fundamentalmente, entradas y salidas de grano de los almacenes de los templos).

Lo relevante de este cambio es que las mercancías comienzan a tener un precio, un valor normalizado más o menos definido y, a menudo, consignado por el estado en las leyes (que lo hace efectivo al usar ese baremos para cobrar impuestos).

Al principio, las unidades monetarias más habituales eran el grano (cebada o trigo) y la plata, aunque esto no significa que normalmente se usasen físicamente (la gente no llevaba encima puñados de trigo y lingotes de plata para ir al mercado) sino que se empleaban como unidad de referencia. Esto es, como contabilidad. En la práctica, las transacciones (y la deuda consecuente a ellas) se consignaban en tablillas de arcilla que hacían la labor de libros de contabilidad.

Retomaremos esta idea del "Dinero como contabilidad" cuando veamos el funcionamiento de Bitcoin.

Moneda

Las primeras monedas conocidas se empezaron a usar en Lidia, en la actual Turquía, en torno al 600 A.E auqnue es probable que ya se hubiesen usado antes de forma más o menos privada.

Originalmente (y, nominalmente, hasta hace muy poco tiempo) las monedas funcionaban como promesa de pago, de forma parecida a un pagaré. Si el deudor era conocido y de solvencia reconocida, se podían dar esas monedas (y transmitir esa deuda) a cambio de bienes o servicios de un tercero. Naturalmente, los emisores de moneda más conocidos y reconocidos acabaron siendo los monarcas y estados (que además, aceptaban esas monedas como pago de impuestos, por lo que contribuían a mantener su valor). Parece ser que la moneda resultó un invento muy útil, porque su uso se extendió rápidamente después de su invención.

Una característica muy importante del dinero en forma de moneda es que las transacciones son (en principio) anónimas. No hace falta saber el pasado de ese dinero, ni de donde viene, ni para qué lo va a usar el receptor en el futuro. Los intervinientes en una transacción no necesitan conocerse, y la transacción es un acto atómico que se agota en sí mismo. Esta característica en fundamental para la existencia de los mercados tal y como los conocemos.

Hoy día, la fracción de moneda en metálico es muy pequeña en comparación con el dinero circulante, pero sigue siendo la herramienta para la mayoría de las transacciones cotidianas. Además, todo el dinero, incluso el que no está representado por monedas o billetes físicos, está técnica y legalmente regulado deliberadamente para funcionar como si fuera dinero en efectivo. Por ejemplo, cuando se hace una transferencia de un banco a otro, el dinero debe "desaparecer" del banco emisor y "aparecer" en el banco receptor. para hacer esto sin el peligro de errores, accidentes o mala fe, se usan procedimientos muy complejo que requieren de terceros que garanticen el intercambio.

La moneda ha sufrido muchos cambios y actualizaciones, pasando por el papel moneda o el dinero electrónico, pero hoy día se reconoce habitualmente que debe cumplir una serie de características básicas:

- Que sea fácil de transportar respecto al valor que representa.
- Que sea fraccionable.
- Que tenga un valor "objetivo", reconocido por todos sus usuarios.
- Que sea difícil de copiar o falsificar.

Aunque algunas de estas características son sólo aplicables en sentido estricto al dinero en metálico, son un buen acuerdo de mínimos, pero permiten que la moneda Pueda usarse como unidad de valor, medio de pago e instrumento de ahorro:

- Unidad de valor: Porque actúa como referencia del valor de vienes y servicios, permitiendo compararlos.
- Medio de pago: Para adquirir bienes y servicios, cancelar deudas, etc.
- Instrumento de ahorro: Porque puede almacenarse sin que, en principio, pierda su valor.

Como podemos ver, el dinero ha cambiado mucho en sus aproximadamente cinco mil años de historia, pero sus características básicas siguen siendo las mismas.

Referencia bibliográfica

Para quien quiera ahondar en estos temas, cualquier libro de texto sobre el tema puede aportar mucho más del escueto resumen que hemos visto.

De todos modos, recomiendo estos tres libros:

El primero trata sobre un tema mucho más amplio, como es la antropología cultural, pero dedica una parte a describir los distintos sistemas económicos históricos o actuales:

Antropología Cultural - Marvin Harris

El segundo es un clásico, aunque está un poco anticuado, y en el se describe la llamada "economía del don":

Ensayo sobre el don - Marcel Mauss

Y el tercero, probablemente el más interesante de los tres, es un repaso a la historia del dinero y la moneda que se sale un poco del relato habitual en los libros clásicos sin dejar de ser riguroso:

En deuda - David Graeber

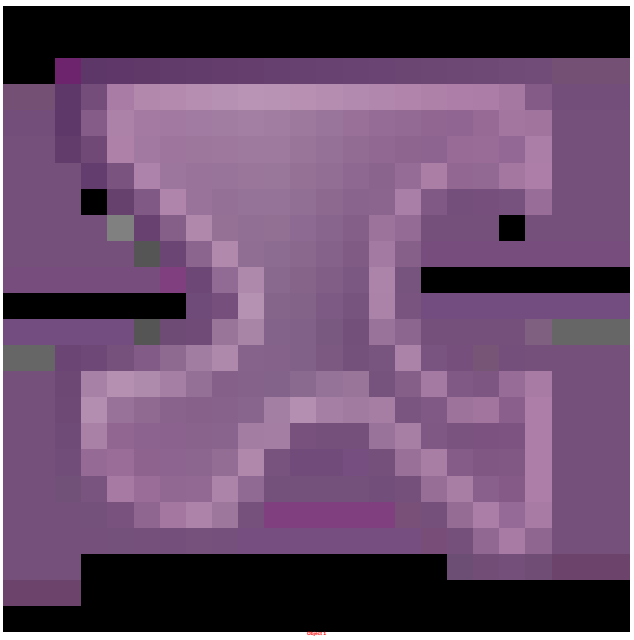
El dinero en la actualidad

El dinero en la actualidad está respaldado por los gobiernos de los países que lo emiten (principalmente, por medio de su aceptación para el pago de impuestos). El dinero en sí no tiene ningún tipo de valor intrínseco más que la confianza de sus usuarios en que pueden obtener cosas con él (se le llama dinero fiduciario o dinero fíat). Por supuesto, el valor en metal de una moneda de un euro es mucho menor que un euro.

En los estados modernos el dinero es creado por los bancos centrales al acuñar moneda. Cuando el banco central de un estado (que, en principio, es una entidad independiente ajena al gobierno) calcula en función de sus parámetros de actuación que hace falta más dinero, manda imprimir la cantidad que estime oportuna de monedas y billetes y "crea" dinero.

Así de simple (en realidad no es ni mucho menos tan simple, pero para nosotros es suficiente).

Los bancos centrales afectan a la economía de otros modos (especialmente, actuando como prestamistas para otros bancos).



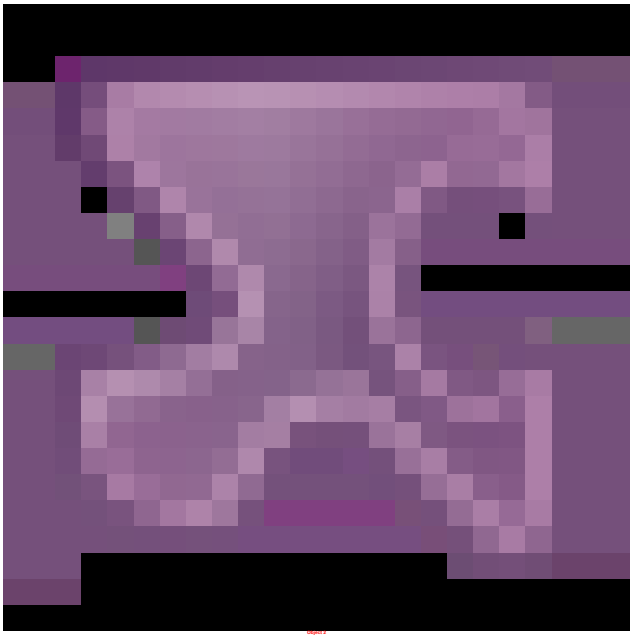
El dinero así creado se llama "dinero legal" o "metálico" y, aunque es la forma de dinero que más solemos ver en el día a día, no es más que una parte de este.

La segunda forma de crear dinero es mucho más importante en su volumen, y está en manos de los bancos privados.

Los bancos crean dinero de forma indirecta al prestar más dinero del que en realidad tienen. Simplificándolo mucho: Los bancos no conservan en sus cajas el dinero de sus clientes, aunque se supone que siempre está a disposición de estos. Si un banco tiene unas reservas de 100 € (el capital de sus clientes) y presta esos 100 € (que luego le serán devueltos con intereses), en la contabilidad aparecerá que el banco tiene los 100 € ingresados más los 100 € que le deben. Acaban de "aparecer de la nada" 100 €.

En realidad, a un banco no se le permite legalmente prestar (usar, invertir) todo lo que tiene, pero sí puede prestar una parte y conservar otra, llamada reserva fraccionaria.

Esta forma de "crear" dinero de la nada se le llama multiplicador bancario, y tiene importantes efectos en la economía.



Algunas personas (especialmente los partidarios de la llamada escuela Austríaca de economía) consideran que estas formas de crear dinero son perjudiciales, y que el dinero debería tener un "valor intrínseco" basado en el respaldo de metales preciosos (normalmente oro). Esta teoría (que cuenta con la oposición de la mayoría de los economistas modernos) tiene, como veremos, un efecto muy importante sobre el diseño del Bitcoin.

Paypal y el dinero electrónico

La conectividad y la frecuencia y velocidad de las transacciones han provocado que, además del dinero electrónico habitual (que es el que usamos, por ejemplo, al pagar con una tarjeta o al hacer una transferencia bancaria), se creen monedas o sistemas de pago alternativos.

Aunque existen multitud de ellos, como Google Wallet, probablemente el más conocido es Paypal.

Paypal, aunque no es una moneda propiamente dicha, puede actuar como moneda en tanto que es un sistema de realizar transacciones y almacenar dinero (para actuar completamente como una moneda le falta el aspecto de "unidad de valor", porque no existe un "paypaldolar" ni nada similar).

Puede que sea "sólo" un medio de pago, pero en el año 2016 Paypal realizó más de seis mil millones de operaciones en todo el mundo.

Un aspecto interesante de los últimos tiempos son las monedas de los juegos de ordenador. El incremento de juegos en red multijugador con sus propios mercados internos ha abierto posibilidades interesantes. El "oro" de juegos como World of Warcraft tiene un uso limitado al propio juego en sus propios términos, pero juegos como EVE Online disponen de mercados internos y monedas con tipos de cambio oficiales y mueven una cantidad apreciable de dinero.

Probablemente el intento más importante (y fallido) de crear una moneda funcional de este tipo sea el linden de Second Life.

Un primer vistazo a Bitcoin

Bitcoin (y sus muchos herederos) pretende darle la vuelta todo esta situación, y cambiar el paradigma del dinero. Si lo conseguirá o no (o si lo conseguirá alguna de las monedas que le han sucedido) es algo que aún está por ver, pero lo cierto es que ahora vive un momento de esplendor y que blockchain, la tecnología que se ha creado para darle soporte, es una idea revolucionaria y que llega mucho más allá de este.

Desde el momento en que Bitcoin apareció surgieron algunos mitos y errores de interpretación que, aunque ahora empiezan a aclararse, aún permanecen en el acerbo común y que veremos a lo largo de este curso. pero, por ahora, vamos a hacer un resumen superficial de qué es Bitcoin.

Bitcoin es una moneda electrónica. No existen billetes impresos ni monedas acuñadas.

Bitcoin (con mayúscula) es una moneda. También es una red de ordenadores, usarios y operadores (que usan el protocolo Bitcoin, también con mayúscula). Cuando hablemos de una cantidad de monedas debemos escribirlo en minúscula (por ejemplo, "0.0004 bitcoins") si el autocorrector nos lo permite. para este último uso se suele usar también BTC o, más raramente, XBT (por ejemplo, "0.0004 BTC").

Bitcoin es una criptomoneda (la primera de su clase) lo que, aparte de sonar muy "tech" y muy rimbombante, significa que su funcionamiento esta basado en la criptografía, como veremos más adelante. Esto, entre otras cosas, significa que es imposible de falsificar. Es importante notar que la criptografía no es un añadido al protocolo Bitcoin para hacerlo más seguro o el motivo que sea, sino que forma parte intrínseca de este. Desde el formato de las cuentas al proceso de "minado" pasando por las transacciones, toda la estructura de Bitcoin se basa en sólidos métodos criptográficos.

Además, está basada en tecnologías distribuidas (la famosa blockchain) y no está centralizada en ningún aspecto. No existe una autoridad o banco central que emita dinero, ni está respaldada por ningún gobierno, ni hay ningún otro tipo de agencia que la controle. Sin embargo, también significa que hay un "libro de contabilidad público". Tanto el valor y parámetros de todas las transacciones como el contenido de todas las cuentas son necesariamente públicos.

Una blockchain, en una primera aproximación, es una base de datos distribuida. Un registro de información (contable, en el caso de Bitcoin) del que existen una gran cantidad de copias iguales (idealmente, una por cada usuario).

Las transacciones son anónimas (pero no secretas, como hemos visto, hablaremos de ello más adelante) y no requieren intermediarios. las cuentas son anónimas en el sentido de que no es necesario dar ningún dato personal a nadie para tener una. De hecho, no es necesario hacer nada, salvo generar un número (aunque un número con propiedades especiales).

Además, las transacciones son irreversibles. Si envías bitcoins a la cuenta equivocada (o, incluso, a una cuenta inexistente), ese dinero está perdido.

No existen medios técnicos para intervenir una transacción o bloquear una cuenta. No es posible dado el propio diseño de la moneda.

Posee por diseño un sistema distribuido (esto es: no centralizado) para evitar el doble gasto.

Los bitcoins se van creando con el tiempo a un ritmo decreciente por medio del proceso conocido como "minado". La cantidad total del bitcoins está limitada por diseño, y nunca superará los 21 millones.

El protocolo Bitcoin y el software original creado para él es libre y abierto, y cualquiera puede usarlo y/o diseñar su propia implementación.

Historia de Bitcoin, origen, teoría, fundamentos

Historia de Bitcoin

El protocolo Bitcoin fue presentado al público oficialmente el 8 de noviembre de 2008 por medio de un artículo en una lista de correo cypherpunk firmado por Satoshi Nakamoto, un seudónimo que oculta a una persona o grupo (más probablemente lo segundo) desconocido.

Su objetivo era crear una moneda basada en la criptografía que fuese descentralizada y anónima. En realidad no era una idea original, sino la implementación de una idea que, en 1998, Wei Dai ya había descrito: El concepto de "Criptomoneda".

Posteriormente, el 9 de enero de 2009, se liberaría la primera versión del software de Bitcoin, una implementación distribuida como software libre (con licencia MIT) en el conocido repositorio público Sourceforge.

Hal Finney fue, probablemente, la primera persona en usar el cliente de Bitcoin. Lo que sí es seguro es que fue la primera persona en recibir una transacción en bitcoins, cuando Satoshi Nakamoto le transfirió la entonces discreta cantidad de diez bitcoins. Al cambio, ahora serían unos 64.000 Euros.

La primera compra real que se conoce fue obra de Laszlo Hanyecz, un programador de Florida que pagó 10,000 bitcoins por dos pizzas (en realidad, pagó esos bitcoins a otra persona que, a su vez, pagó con su tarjeta).

Oficialmente, Satoshi Nakamoto abandonó el proyecto Bitcoin en 2010. Ese mismo año apareció en la web la primera casa de cambio que operaba con bitcoins.

En 2012 se inició la Fundación Bitcoin. Su misión es "Acelerar el crecimiento global de bitcoin a través de la estandarización, protección y promoción del protocolo de código abierto".

Desde entonces, la red ha crecido, el número de usuarios ha aumentado y el precio del bitcoin se ha disparado.

El precio del bitcoin ha sufrido fuertes variaciones, subiendo y bajando repentinamente pero, en general, su tendencia ha sido de una clara subida. Pese a que no parece que su uso como moneda acabe de funcionar, si se ha mostrado como una potente (y arriesgada) herramienta de especulación.

Bitcoin ha dado lugar a otras muchas monedas, como Monero, Bitcoin Cash o Litecoin. También han aparecido otras herramientas basadas en blockchain pero que pretenden explorar otras posibilidades más allá de la mera moneda, como Ethereum.

Evolución del precio de Bitcoin: https://www.buybitcoinworldwide.com/price/

Información sobre diversas criptodivisas: https://bitinfocharts.com/

Software Libre y su importancia para Bitcoin

Como adelantamos en el tema anterior, tanto el protocolo Blockchain como el programa cliente oficial Bitcoin Core son software libre.

El software libre, cuyo ejemplo más conocido es el sistema operativo Linux, es aquel que garantiza una serie de libertades para el usuario (Copiadas literalmente de https://www.gnu.org/philosophy/free-sw.es.html):

- La libertad de ejecutar el programa como se desea, con cualquier propósito (libertad 0).
- La libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que usted quiera (libertad 1). El acceso al código fuente es una condición necesaria para ello.
- La libertad de redistribuir copias para ayudar a su prójimo (libertad 2).
- La libertad de distribuir copias de sus versiones modificadas a terceros (libertad 3). Esto le permite ofrecer a toda la comunidad la oportunidad de beneficiarse de las modificaciones. El acceso al código fuente es una condición necesaria para ello.

Para que un programa pueda ser considerado software libre, es necesario que tenga una licencia que permita los usos arriba indicados y, lo que es más importante, que el software se distribuya junto con el código fuente de este (o que se disponga de algún modo de acceder a él, como un repositorio en internet).

Esto último es especialmente útil cuando se trata de herramientas en las que sean importantes cosas como la seguridad o la privacidad: Al poder examinarse el código fuente, es posible detectar si contiene errores, puertas traseras o cualquier cosa que pudiera poner en riesgo esta seguridad o privacidad.

Ya se han dado casos de monederos de Bitcoin con puertas traseras o software de minado que empleaba parte del tiempo en trabajar para otros.

Por eso, a la hora de elegir herramientas de seguridad, especialmente cuando se trata de manejar dinero, es más que recomendable escoger herramientas de software libre.

Qué es Bitcoin

Bitcoin es una red peer to peer (p2p) del mismo tipo que Emule o Torrent. Se trata de redes no centralizadas en las que cualquier nodo puede conectarse en igualdad a cualquier otro. No necesitan nodos centralizados que enruten, controlen o gestionen ningún aspecto de esta.

El principal cometido de esta red en mantener sincronizado un fichero (la famosa blockchain) de modo que todos los nodos de la red tengan exactamente la misma versión de ese fichero. La tarea se complica porque ese fichero (la blockchain en adelante), además, va cambiando con el tiempo. El segundo uso es comunicar transacciones.

En el próximo tema entraremos en detalles pero, por ahora, baste decir que la blockchain tiene una serie de salvaguardas para asegurar su validez (nunca se elimina nada de ella, sólo se agrega, y los cambios que se hacen deben estar firmados criptográficamente de modo que, cada vez que se agrega un bloque de datos, se validan todos los datos anteriores (por eso se le llama "cadena").

En el tema anterior, cuando vimos el origen del dinero en Mesopotamia, ya apuntamos a la idea de "Dinero entendido como contabilidad".

La blockchain es precisamente eso. Al fin y al cabo, no es más que un inmenso libro de cuentas digital donde se consigna cada transacción que ha habido desde el inicio de la red Bitcoin, mostrando quién tiene cada bitcoin, y quién lo ha tenido en cada momento de la historia.

Esto es importante porque, sobre todo al principio, en la prensa se dieron informaciones erróneas relativas al anonimato en Bitcoin: Todas las transacciones y todos los estados de cuentas son públicos. Todas las cuentas son anónimas en el sentido de que no consta en ninguna parte ningún dato del propietario, pero tanto el la cantidad de bitcoins que tiene un cuenta como el historial de transacciones son perfectamente públicos. Por eso se recomienda encarecidamente usar cuentas diferentes o, incluso, utilizar de cuentas de un solo uso en la medida de lo posible.

Una cuenta en Bitcoin no es más que un número un tanto peculiar asociado a una cantidad de bitcoins. Este número se llama "hash" y, aunque ya hablaremos en detalle de eso más adelante, se trata de un número que se obtiene usando métodos criptográficos a partir de una clave secreta.

Por ejemplo, esto es una cuanta de bitcoin: **1CeEBLRF2Ki284MU9gEn6uCjmSPNydZstq**

Y, dado que es completamente pública, cualquiera puede examinar la blockchain, buscar ese número, y ver fácilmente tanto su contenido en bitcoins como las transacciones en las que ha participado. Por ejemplo, en blockchain.info se puede buscar el estado actualizado de todas las cuentas de Bitcoin, y podemos ver la que hemos visto arriba:

https://blockchain.info/address/1CeEBLRF2Ki284MU9gEn6uCjmSPNydZstq

Como curiosidad, aquí hay un artículo intentando calcular, en base a la información que hay en la blockchain, la fortuna de Satoshi Nakamoto

Una transacción no es más que un número de cuenta de salida, una cantidad a transferir, y un número de cuenta de ingreso.

Entonces, para realizar una transacción, sólo es necesario emitir un mensaje en la red Bitcoin diciendo "Quiero que se agregue a la blockchain una transacción de X bitcoins de la cuenta AAA a la cuenta BBB" (Naturalmente no se trata de un simple mensaje de texto, el protocolo articula el formato exacto de ese mensaje, pero la idea es esa).

Pero, entonces, ¿Cómo se hace para que sólo el propietario de la cuenta pueda enviar dinero?

Toda transacción en Bitcoin debe estar firmada electrónicamente con la misma clave secreta que se usó para crear el hash de la cuenta de la que salen los bitcoins.

Como veremos en el tema siguiente, Bitcoin utiliza un sistema de criptografía de clave pública por medio del que se puede determinar si algo ha sido firmado con una clave concreta aunque no se conozca esa clave. De este modo, se puede comparar el número de la cuenta emisora con la firma de la transacción para validarla (No es necesaria firma del receptor, se pueden ingresar bitcoins en cualquier cuenta sin permiso del propietario).

De este modo, sólo la persona que tiene esa clave puede realizar una transacción. Por otro lado, si se pierde la clave asociada a una cuenta, es acuenta queda completamente anulada. Nunca se podrá usar los bitcoins que contenga.

Estas claves no son una simple contraseña de ocho caracteres, un dígito, una letra en mayúscula y una letra en minúscula. Se trata de números de 256 bits generados automáticamente por un sofisticado algoritmo matemático y son prácticamente imposibles de recordar por una persona.

Por ejemplo: una de estas claves (codificada de forma que sea "comprensible por humanos" sería la siguiente:

"7b7aa3c2e9eee3fd2cdde66f377c3aaf81202adf914f765d726d65d9fc88cafa"

Normalmente, los monederos electrónicos son los que se ocupan de recordar y utilizar esas claves sin que el usuario tenga que hacer nada. Recordad hacer copia de seguridad de vuestros monederos.

Puedes (y debes) poner una contraseña a tu monedero electrónico. No hay que confundir la contraseña que usas para tu monedero (y que no debes olvidar) con las muchas claves que usa tu monedero para acceder a tus cuentas (y por las que no debes preocuparte).

Minería

La minería es el procedimiento por el que se construye la blockchain.

Veremos los detalles en el tema siguiente, pero consiste en invertir potencia computacional en resolver un problema criptográfico de dificultad variable.

Un minero reúne propuestas de transacciones de otros miembros de la red, las valida, y las reúne en un "bloque". Luego añade ese bloque a la blockchain y procede a calcular un hash, un número único que debe cumplir ciertos requisitos. Para ello debe usar una serie de cálculos que exigen mucha potencia computacional. Al tener que calcular este hash sobre el nuevo bloque añadido a la cadena anterior, se asegura que hay un orden cronológico lineal. Cada bloque está validando a todos los anteriores y, si se intentara introducir un bloque entre dos anteriores, ninguno de los hashes posteriores sería válido.

La dificultad de esta prueba se actualiza periódicamente (cada dos semanas, aproximadamente) para que, independientemente del volumen de mineros que haya y su capacidad de cómputo, se calcule un nuevo bloque cada diez minutos aproximadamente. Eso significa que, si hay más mineros con más capacidad de cómputo, la llamada "prueba de trabajo" será más difícil.

Cuando el minero ha calculado ese hash publica su nuevo bloque, compartiéndolo con el resto de la red.

Cada usuario aceptará como válido ese bloque si no tiene uno más reciente (es decir, si su blockchain es más corta) y lo compartirá a su vez, de modo que se va transmitiendo por la red. Como hay muchos mineros trabajando a la vez, a veces, hay varias versiones distintas de la blockchain distintas, creadas por distintos mineros, que se distinguen sólo por sus últimos bloques.

Esto quiere decir que es posible minar un bloque válido, compartirlo y que sea aceptado por muchos clientes en un principio, pero que acabe siendo rechazado porque ya había circulando otra versión de la blockchain con más bloques.

Por eso no se acepta un transacción hasta que obtiene tres o cuatro "confirmaciones". Cada vez que un bloque se añade a la cadena se "confirman" los anteriores, porque hace más probable que ese bloque de la cadena esté en rodas las versiones de la blockchain y, por tanto, esté "fuera de dudas".

Cuando se habla de que una transacción tiene "cuatro confirmaciones", esto quiere decir que se han agregado cuatro bloques después del que contiene esa transacción.

Adicionalmente, cuando un minero añade un bloque, incluye un número de cuenta en el que se ingresan automáticamente tanto el número de bitcoins generados con ese bloque (un número que se va reduciendo con el tiempo hasta que se alcance el límite previsto de 21 millones de bitcoins) y los "feeds" que hubiera añadidos a las transacciones de ese bloque. Este es el beneficio del minero. No se obtiene nada por casi conseguirlo, no hay premio para el segundo. Cada minero consigue el pago si calcula un nuevo hash y, además, tiene la suerte de imponerlo ante los que puedan haber calculado otros.

Al principio, cualquier persona podía minar bitcoins con un simple ordenador personal. Había pocos competidores y la prueba de fuerza era relativamente sencilla.

Actualmente, el minado de bitcoins está monopolizado por los grandes mineros con enormes instalaciones de cálculo especializadas. Usan harware diseñado especialmente para esto y se emplazan en lugares donde la energía es barata.

Limitaciones de Bitcoin

Existen algunas limitaciones propias de Bitcoin que ponen en aprietos su utilidad presente y futura:

El tamaño de cada bloque está limitado a 1M por razones de seguridad. Durante la mayor parte de la historia de Bitcoin eso no ha sido un problema, porque el número de transacciones era pequeño y no se llegaba a ese límite (los bloques eran muy pequeños). Pero en los últimos años el número de transacciones ha aumentado, y el límite del bloque empieza a ser problemático.

Dado el límite del tamaño de bloque y que se genera un bloque nuevo cada diez minutos, el número máximo de transacciones de la red Bitcoin se reduce a una media de unas seis o siete por segundo. A modo de comparación, VISA hace, de media, unas 2000 operaciones por segundo.

El que se llegue al límite de transacciones hace que el pago por transacción a los mineros aumente: SI quieres que tu transacción sea incluida en un paquete debes pagar para incentivar al minero. Si no lo haces, preferirá incluir en su bloque la transacción de alguien que le pague más. Por eso, en los últimos tiempos, el feed por transacción está aumentando.

La red Bitcoin es lenta. Suponiendo un seguridad de cuatro confirmaciones, eso significa que se debe esperar, en el mejor de los casos, cuarenta minutos para que una transacción sea válida. En la práctica, la confirmación de una transacción pude demorarse horas.

La red Bitcoin es costosa. La energía usada simplemente para mantener la red en marcha es enorme. Todos esos mineros procesando información par construir bloques empelan una cantidad energía equivalente al consumo de un país pequeño. Una cantidad brutal, sobre todo si tenemos en cuenta que la inmensa mayoría de ese trabajo es redundante, ya que sólo uno de ellos acabará creando realmente su bloque.

La blockchain ocupa mucho espacio. No es algo relevante para los grandes sistemas y para la minería (aunque la dificultad de la minería se incrementa con el tamaño de la blockchain), pero sí es una dificultad añadida para el usuario común. La blockchain de Bitcoin actualmente pasa de los 160 GB, lo que es un requisito bastante exigente para un ordenador portátil, pero supera completamente las posibilidades de un teléfono móvil.

Existen wallets (monederos) que sortean esa limitación manteniendo versiones reducidas de la blockchain o dependiendo de servicios on-line que son los que realmente mantienen la blockchain. Esto representa un ahorro de espacio y una mejora en la eficiencia, a costa de perder en seguridad, al depender de la confianza en otros.

Además, al ser un archivo exhaustivo de todas las transacciones realizadas en la historia, el tamaño de la blockchain sólo puede crecer, y más rápido cuanto más se use.

Criptografía de clave pública y fundamentos de la blockchain

Criptografía

Dice el diccionario que la criptografía es el arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

Pero al diccionario le falta aclarar que hablamos de técnicas matemáticas.

Dado que, en realidad, un ordenador sólo trabaja con números (con unos y ceros, en concreto), cualquier cosa con la que opere un ordenador son es más que números. De este modo, en realidad, podemos operar con un texto, un archivo o una foto como si no fuera más que un número.

Así que, en lo que sigue, conviene recordar que hablar de funciones que hacen lo que sea con "un número" implica que lo pueden hacer también con un texto, una foto, un archivo o lo que sea.

NOTA: Existe en la comunidad criptográfica hispanohablante cierta polémica sobre el uso de palabras como "encriptar" o "cifrar", cual debe usarse y cuando. En lo que respecta a este tema, ambas (y sus variaciones) se usan indistintamente con el mismo sentido.

Cuando algo está oculto usando técnicas criptográficas decimos que está "cifrado" o "encriptado". Cuando algo no está oculto de este nodo, decimos que está "en claro".

La criptografía puede ser un tema un tanto árido, pero es la base fundamental de la blockchain y hay que entender sus rudimentos para comprender esta.

Funciones hash

En un sistema informático al que puedan tener acceso varias personas (lo que, hoy en día, significa casi cualquier sistema informático) es necesario controlar el acceso por medio de contraseñas.

La idea es muy simple: cada usuario tiene una contraseña que debe escribir al acceder al sistema. Si la clave coincide con la que hay almacenada se le permite el acceso. Simple ¿no?

Este modelo tiene un problema: La clave debe estar almacenada en el sistema para poder hacer la comparación. Si alguien accede al archivo donde se almacenan las claves, puede saltarse toda la seguridad.

Para resolver este problema haría falta una forma de verificar una contraseña sin tenerla almacenada. Y eso se consigue con las llamadas funciones hash.

(No vamos a entrar en detalles pero, para los que quieran profundizar más, aclararemos que aquí nos referimos conretamente a funciones hash criptográficas)

Una función hash (también llamadas "funciones resumen") es una función matemática que toma una cifra cualquiera con un número arbitrario de dígitos y retorna una cifra de un número predeterminado de dígitos.

Normalmente, al resultado de aplicar una función hash se le llama, también, "un hash", de modo que se habla de "calcular un hash" u "obtener un hash".

Las funciones hash tiene algunas características interesantes:

El valor resultante de aplicar una función hash concreta está determinado sólo por el valor inicial. Es decir, que siempre que aplique la misma función hash al mismo valor obtendrás el mismo resultado.

Aplicar una misma función hash a dos números distintos dará dos resultados distintos. Se dice que no hay "colisiones". Esto no es cierto para todas las funciones hash, pero basta con que la probabilidad de colisiones sea suficientemente pequeña.

Dado un subconjunto cualquier de valores iniciales, los valores finales están uniformemente distribuidos en el conjunto de posibles resultado. Es decir, que no existen patrones (del tipo, por ejemplo, "un número pequeño dará un resultado pequeño") que permitan predecir ni siquiera aproximadamente el resultado. Números muy parecidos, tras aplicarles la función hash, darán resultados muy distintos (esto va a ser muy importante cuando hablemos de minería).

Por ejemplo, este es el resultado de aplicar la función hash MD5, una de las más utilizadas, a tres textos muy parecidos:

"Hola mundo" -> "f822102f4515609fc31927a84c6db7f8"

"hola mundo" -> "0ad066a5d29f3f2a2a1c7c17dd082a79"

"Hola mundo." -> "9a385be5ce59d3953a3e764cd099cce9"

Como puede verse los valores resultantes, aunque de la misma longitud, son completamente distintos, a pesar de que las cadenas originales son muy parecidas.

Como comparación, la función hash SHA256 (similar a la que se usa en la minería de bitcoins) dará los siguientes resultados para los mismos textos:

"Hola mundo" -> "9797b1e9be5a424f3f94392a8102a6c247a533d2d6e287d038c104f325e84fdb"

"hola mundo" -> "41d85e0b52944ee2917adfd73a2b7ce3d3c8368533a75e54db881fac6c9ad176"

"Hola mundo." -> "300d95a6ab2537d939f0e134a889470d7bd4e4cab00b6f5e82b06df13cbe69c6"

Los hash obtenidos con SHA256 son más largos (256 bits frente a 128 de MD5), por lo que son más resistentes a ataques de fuerza bruta.

La función inversa de una función hash (esto es: la que, dado el resultado de aplicar la función hash, retorna el valor original) es computacional mucho más costosa. Muchísimo. En la práctica, se puede considerar impracticable.

Técnicamente no todas las funciones hash cumplen esta propiedad. Aquellas que sí lo cumplen (y que son las que nos insertan aquí) son las llamadas "Funciones hash de un solo sentido".

Esto es justo lo que necesitábamos para solucionar nuestro problema con el almacenamiento de las contraseñas: Ahora sólo hay que almacenar el resultado de aplicar una función hash a nuestra contraseña de modo que, cada vez que queramos comprobar si la que ha introducido un usuario es válida, sólo hemos de aplicarle a esa la misma función y comparar con el valor almacenado.

Como siempre que hablamos de estas cuestiones criptográficas, hay que tener en cuenta que "deshacer" un hash (o sea, obtener la clave original a partir del hash almacenado) no es imposible, en teoría. Sólo es enormemente difícil.

De todos modos, en la práctica y usando una función hash razonablemente segura, se puede considerar imposible.

Pero estas propiedades de las funciones hash nos van a resultar útiles en muchos otros contexto donde se requieran cosas como un identificador único o comprobar fácilmente la integridad de un archivo.

Árboles de Merkle

Algo interesante en relación a los hashes (y que va a ser muy relevante para notros en la blochain) son los llamados árboles de Merkle.

Un árbol de Merkle (también llamado, a veces, árbol de hashes) es una estructura de datos en árbol la que cada nodo es el resultado de aplicar una función hash sobre el valor de los nodos hijos.

De este modo, tenemos que cada par de elementos en los extremos finales del árbol está descrito por un hash que los engloba, y cada par de estos hashes tiene a su vez otro hash que los engloba a ellos, etc.

La raíz de este árbol (el hash final único que engloba a todos los demás) se llama raíz de Merkle (Merkle root)

Lo bueno de esta estructura es que puede servir para verificar rápidamente que los valores de las ramas finales no se han modificado, porque toda la estructura de hashes cambiaría ante cualquier modificación y, por tanto, la raíz de Merkle cambiaría. Además, pueden servir para localizar fácilmente dónde está ese cambio, siguiendo la ruta de cambios en los hashes.

Criptografía de clave simétrica

El método más clásico de criptografía, y la forma en que la gente entiende normalmente que funciona: Se usan una clave para encriptar el texto, y se vuelve a usar la misma clave para desencriptarlo.

Si se usa para enviar mensajes plantea el problema de que la clave debe ser conocida tanto por el emisor como por el receptor, por lo que hay que enviarla también. Y, en la mayoría de los casos, si es posible enviar la clave por un canal seguro entonces es posible enviar el mensaje por ese mismo canal.

El único sistema criptográfico que está demostrado que es absolutamente seguro desde el punto de vista algorítmico es un sistema de clave simétrica: El llamado "cuaderno de un solo uso", que requiere claves de un solo uso, que sean aleatorias y que tengan, al menos, la misma longitud que el mensaje.

Criptografía de clave asimétrica

Supongamos que nos dicen que el número 847342423169694469 es el producto de dos números primos (lo es), y que debemos descubrir cuáles son con lápiz y papel.

Se trata de una tarea larga y tediosa que requiere un montón de operaciones matemáticas. No es un número muy grande y cualquier ordenador puede hacerlo en un instante, pero la dificultad se dispara con el número de dígitos.

Sin embargo, si nos piden que descubramos el producto de multiplicar 920469379 y 920554711 (que es, precisamente, el número de arriba) el trabajo es muchísimo más fácil, requiere menos operaciones y, lo que es más importante, la dificultad no crece tan rápidamente con el número de dígitos.

Esto es muy interesante, porque podemos buscar un par de números primos tales que calcular su producto sea una tarea asequible a un ordenador tanto en tiempo como en capacidad de cómputo, pero el resultado no se pueda factorizar a menos que se usen grandes supercomputadores durante millones de años.

Al igual que este ejemplo de la factorización de números, existen operaciones matemáticas que son muy simples y fáciles de calcular en un sentido, pero enormemente difíciles en sentido opuesto.

Los sistemas criptográficos de clave asimétrica (también llamados "de clave pública") usan este tipo de cálculos para generar pares de contraseñas que cumplen la interesante propiedad de que lo que se cifra con una de las claves del par sólo puede descifrarse con la otra, y viceversa.

Concretamente, en estos sistemas una de las claves del par se difunde públicamente de modo que pueda ser usada por cualquiera, mientras que la otra es guardada en estricto secreto por su propietario.

Esto tiene dos utilidades fundamentales:

Criptografía: Cualquier persona puede encriptar un mensaje usando la clave pública de alguien, de modo que sólo ese alguien (que posee la clave privada) pueda acceder a su contenido.

Firma: Una persona puede enviar un mensaje encriptado usando su clave privada para que cualquiera pueda desencriptarlo usando su clave pública, de modo que certifique sin lugar a dudas que el mensaje lo ha enviado él (que posee la clave privada).

El único problema es cómo asegurarse de que la persona que usa una clave sea realmente quién dice ser, para eso se usan redes de confianza, pero eso va más allá de la criptografía y no tiene demasiada relevancia en lo que respecta a Bitcoin.

Transacciones

Una transacción puede estar formada por una o varias cuentas de entrada y una o varias cuentas de salida. De este modo, una transacción entre dos usuarios podría consistir, en realidad, en la emisión de diversas cantidades desde muchas cuantas distintas y el ingreso en muchas otras cuentas distintas.

Las transacciones no tienen un periodo de validez explícito y, en principio, son válidas desde el momento en que se emiten a la red Bitcoin hasta siempre (no caducan).

Una transacción debe estar firmada con la misma clave que está firmada la cuenta desde la que se emiten los bitcoins.

El concepto fundamental en una transacción de bitcoins es el de UTXO ("Unspent Transaction Outputs" o algo así como "Transacciones de Salida no Gastadas").

Dado que la blockchain nunca se modifica, no hay algo como un estadillo de cuentas que indique quién tiene qué cantidad de dinero en cada momento.

Para verificar que una transacción es válida, es necesario comprobar que la cuenta de salida tiene ese dinero, y que no ha sido gastado en anteriores transacciones. A ese dinero no gastado es a lo que se le llama "UTXO". Cuando se hace una transacción, lo que la red bitcoin está haciendo en realidad es marcar una cantidad de bitcoins de la blochain como UTXO para ese usuario. Tu dinero puede estar realmente diseminado por toda la blochain, aunque tu monedero, simplemente, indicará que tienes la cantidad de bitcoins que sea.

De todo esto se deduce que transacción es simplemente una cadena de bits con un formato determinado, y que puede ser creada por cualquier medio; no hace falta que se hecha por ningún software en concreto (se podría escribir a mano, si eres capas de darte ese trabajo).

Pero, naturalmente, alguien debe comprobar que esa transacción es válida.

Propagando Transacciones

Como acabamos de ver, una transacción puede ser creada offline, sin conexión internet. Pero no tendrá ningún efecto hasta que se propague por la red y llegue a inscribirse en la blochain.

Recordemos que la red Bitcoin es una red P2P en la que no hay nodos privilegiados. Cualquier usuario de la red es (en principio) un nodo exactamente igual que cualquier otro.

Como dijimos en el capítulo anterior, cuando un usuario crea una transacción, esta es transmitida a través de toda la red Bitcoin.

Cada nodo que recibe la transacción la transmite a su vez a los demás, pero antes comprueba su validez. Esto es muy importante, porque todos los nodos están validando que es transacción sea correcta (válida).

¿Y qué es lo que hace que una transacción sea válida?

Además de lo visto al describir las transacciones, el primer requisito es que la transacción debe estar bien formada: su sintaxis y estructura de datos deben ser correctas, su tamaño no puede superar el máximo definido en el protocolo, no puede tener vacíos los campos de la(s) cuenta(s) de emisión ni la(s) de recepción, el valor debe ser menor que 21 millones de bitcoins y mayor de cero, etc.

Además se comprueba, lógicamente, que las cantidades emitidas sean iguales a las cantidades ingresadas, que las cuentas de salida existan y tengan fondos, etc.

Si una transacción llega a un nodo y no cumple alguno de los requisitos para ser válida, o cumple alguno para no serlo, es descartada y no se transmite a los demás nodos. De este modo, se consensúa la validez de las transacciones. Si un software intenta "colar" una transacción falsa o malformada, será descartada por el resto de nodos. Si un nodo descarta maliciosamente una transacción, está se propagará de todos modos por el resto de nodos.

Añadiendo la transacción a la blockchain

Todos los nodos de la red blochain son iguales, y se dedican a las tareas habituales de un nodo: Propagar transacciones y mantener actualizada su copia de la blochain.

Pero ya vimos que hay nodos que, además, se ocupan de construir la blockchain. Estos nodos son los que en el tema anterior llamábamos "mineros".

Cualquiera puede decidir ser minero usando cualquier software disponible o con su propio software personal. No es necesario ningún tipo de registro ni control, ni advertirlo de ningún modo, Un minero es un nodo como otro cualquiera de la red.

Lo que diferencia al minero es que, en lugar de transmitir la blochain tal y como le llega desde otros nodos, antes intenta añadirle un nuevo bloque.

Pero para ello debe construir ese bloque primero, y eso no es un trabajo fácil.

Para crear un bloque, un minero debe superar la llamada "prueba de fuerza" (proof-of-work), que es un desafío de computación de dificultad variable que asegura que el minero ha invertido unos recursos computacionales y, además, se ajusta para que los bloques sean creados en la red a un ritmo medio constante de un bloque cada diez minutos.

Pero, antes de ver en qué consiste esta prueba, debemos ver cómo está formado un bloque.

Estructura de un bloque

La estructura de un bloque de la blockchain puede ser bastante compleja, pero esencialmente consiste en una serie de transacciones empaquetadas precedidas por una cabecera que las describe.

Las transacciones de un bloque deben ser válidas (los mineros, como cualquier otro nodo de la red, validan las transacciones), pero la parte interesante es la cabecera.

La cabecera de un bloque está formada por los primeros 80 bytes, según una estructura definida:

Primeros 4 bytes | Número de versión

Siguientes 32 bytes | Hash del bloque anterior

Siguientes 32 bytes | Raíz de Merkle de las transacciones del bloque

Siguientes 4 bytes | Marca de tiempo

Siguientes 4 bytes | Target

Últimos 4 bytes | Nonce

Los primeros cuatro bytes corresponden simplemente al número de versión del software / protocolo usado para crearlo.

Los siguientes 32 bytes son más importantes, y contienen el hash del bloque anterior a este (o "bloque padre").

Después, otros 32 bytes contiene la raíz del árbol de Merkel de las transacciones de ese bloque. Como vimos al principio de este tema, este árbol es una estructura de hashes que sirve para validar las transacciones contenidas en este bloque. Si se cambiara el valor de cualquier parámetro de alguna de ellas, el valor de este campo también debería cambiar.

La marca de tiempo (timestamp) es la fecha y hora de creación del bloque en formato Unix Epoch. Este formato es, simplemente, el número de segundos transcurridos desde el 1 de enero de 1970.

Esta marca de tiempo tiene valor informativo, y NO se usa para comparar la antigüedad de la blockchain de un minero con la de otro (sería muy fácil mentir poniendo una fecha anterior a la real), aunque sí se usará, como veremos después, para estimar el ritmo de creación de bloques.

El Target es el valor que hace que sea difícil crear el bloque, y además cómo de difícil será hacerlo. Se trata (junto con el "nonce") del parámetro fundamental al hablar de minería, así que lo veremos con más detenimiento un poco más adelante.

El Nonce es el número que se usa, incrementándolo iterativamente, para encontrar un hash que sea menor que el target. También lo veremos más adelante con más detenimiento.

Después de la cabecera, el resto del bloque contiene las transacciones.

Los primeros 50 kilobytes de este espacio de transacciones está reservado para las transacciones prioritarias.

La primera transacción de cada bloque es muy importante, ya que es la que "genera" bitcoins de la nada, que van a a parar al minero.

La cantidad de bitcoins que genera esa transacción está predefinida según un patrón decreciente, de forma

que se reduce a la mitad cada 210.000 bloques (unos cuatro años). Actualmente está en unos 18.5 BTC y se reducirá a cero en torno al 2140.

El minero, además, ingresa las comisiones (feeds) que se añadan a las transacciones. Las comisiones son voluntarias, y puede decidirse no añadirlas. Cuando había pocas transacciones estas comisiones no eran necesarias pero, hoy día, una transacción pude demorarse mucho tiempo si no ofrece una comisión.

Dado que la blochain es pública, todos los detalles de cada uno de los bloques puede ser examinado por cualquier software, ya sea en el propio ordenador como en internet. EL sitio más conocido es blockexplorer.com

Hashcash

El algoritmo hashcash es el procedimiento que usa bitcoin para asegurar una prueba de trabajo que garantice que la creación de bloques sea al mismo tiempo costosa para el minero y fácil de comprobar para el resto de nodos y, además, que la dificultad pueda ser ajustada en función de las necesidades de la red.

Todo el brutal esfuerzo computacional (y el consiguiente gasto de energía) que requiere el mantenimiento de la red Bitcoin se basa en lo costosa que resulta la resolución de esta prueba matemática y, por tanto, la minería.

Como hemos visto, crear un bloque de blockchain es algo en principio muy simple: Sólo hay que validar las transacciones que llegan por la red, unirlas en un paquete de formato determinado, añadirlo a la blockchain y compartirlo. Todo ello son tareas computacionalmente poco costosas, tanto en tiempo como en energía. Cualquiera podría crear montones de bloques nuevos cada segundo e invadir la red con ellos.

Pero el protocolo Bitcoin añade una dificultad adicional, con el objetivo primario de mantener el ritmo de creación de bloques limitado y constante, para que la red sea operativa.

Como hemos visto al describir la estructura de un bloque, es necesario que en la cabecera consten tanto la dificultad como el "nonce". La dificultad es un número que calcula la red distibuídamente (cada nodo la calcula independientemente según unos parámetros objetivos que veremos un poco más abajo), pero el nonce es un número que debe averiguarse en base a esa dificultad.

Los detalles del algoritmo concreto han cambiado en diferentes versiones de Bitcoin, pero son cambios menores (aunque con implicaciones para la seguridad del protocolo) y no nos afectan demasiado. Aquí describiremos sólo el funcionamiento general.

Para crear un bloque, un minero comienza probando con un nonce cualquiera (lo normal es un cero e ir incrementando en cada prueba) para crear un hash del paquete usando ese nonce.

Para calcular ese hash se usa la función SHA256 dos veces consecutivas, por lo que se le llama "SHA256 al cuadrado".

Si el hash obtenido es menor que la dificultad, enhorabuena: Hemos creado un bloque válido.

Pero la dificultad, aunque puede variar, siempre es un número muy bajo (lo que implica que necesitamos encontrar un hash que empiece por un montón de ceros),así que, en la inmensa mayoría de los casos, el hash creado es mayor que el valor de la dificultad

No queda otra que que cambiar el nonce (increméntándolo) y volver a hacer la prueba.

Es necesario repetir la operación las veces que haga falta (y esos son muchas veces) hasta dar con un hash que sea menor que el valor de la dificultad.

Recordemos que, al hablar de las funciones hash, dijimos que los valores finales estaban uniformemente distribuidos en el conjunto de posibles resultados. Esto quiere decir que no hay forma de predecir el orden de un hash a partir del nonce y que dar con un nonce que nos construya un bloque válido es una lotería.

Pero, como todas las loterías, el único factor determinante es el número de boletos que tengamos. Y, en computación, numero de boletos quiere decir capacidad de cómputo.

Si mi ordenador personal hace calcula un hash en el tiempo en el que la instalación de supercomputación de un minero profesional encuentra varios millones, es posible que yo tenga suerte y lo encuentre primero, pero tengo las probabilidades en mi contra.

¿Cómo se establece la dificultad?

La dificultad es, como hemos visto, un número que se pone como objetivo de la función hashcash, de tal modo que el hash del bloque debe ser menor que este.

En realidad, el Target (el número que aparece en la cabecera del bloque) no es la dificultad en sí, sino que se calcula a partir de ella. Pero el matiz es una pequeña complejidad que vamos a ignorar porque no afecta demasiado a la explicación que sigue. Quien quiera conocer los detalles, puede ver la descripción detallada del algoritmo concreto aquí: https://en.bitcoin.it/wiki/Difficulty

En lo que a nosotros nos interesa, la dificultad es un parámetro que se calcula de forma distribuida e independiente en todos los nodos de la red.

Es simplemente un número que se ajusta periódicamente para hacer que el ritmo de producción de bloques sea lo más constante posible, en torno a uno cada diez minutos. Dado que la producción de un hash válido es un proceso aleatorio, este ritmo de producción es siempre un valor promedio, pudiendo variar arriba o abajo.

Pero, lo importante, es que la entrada o salida de mineros afecta a este ritmo. Al principio, cuando Bitcoin no era famoso y sólo minaban unos pocos crypto-nerds con sus ordenadores personales, el cómputo total dedicado a bitcoin era mínimo.Hoy en día, como montones de grandes instalaciones de computación especializadas, la capacidad de cálculo de hashes ha crecido radicalmente.

Y, sin embargo, se sigue creando un bloque cada, aproximadamente, diez minutos.

El protocolo Bitcoin especifica que se debe recalcular la dificultad cada 2016 bloques, lo que viene a ser, aproximadamente, una vez cada dos semanas.

Este cálculo se hace usando las marcas temporales de los bloques anteriores para estimar el ritmo de producción: Si se han creado a un ritmo demasiado rápido, se incrementa la dificultad (el Target se hace más pequeño para que sea más difícil encontrar un hash menor). Si se han creado a un ritmo menor de lo esperado (esos 10 minutos por bloque), se baja la dificultad de la prueba (haciendo el Target más grande, para que se a más fácil encontrar un hash que sea menor).

Validando bloques.

Como hemos visto, las transacciones sólo se propagan por la red una vez validadas, de forma que se eliminan de la circulación las que sean inválidas por errores o deliberadamente.

Lo mismo ocurre con la propia blochain.

Cada nodo de la red comparte su versión de la blockchain con el resto de nodos de forma muy parecida a como lo hacen programas como emule o torrent.

Si un nodo encuentra entre sus "vecinos" una versión más actual que la suya (con más bloques), reemplaza la que tiene por esa. Naturalmente, dado el protocolo de transmisión, normalmente sólo es necesario importar la parte correspondiente a los últimos bloques, no la blockchain completa (que es igual en todos los nodos).

Pero antes de importarla (y, lógicamente, antes de compartirla) se comprueba su validez.

Básicamente, un bloque es válido si cumple los siguientes criterios:

- Sus transacciones son válidas.
- El valor de la dificultad es correcto (recordemos que todos los nodos de la red calculan la dificultad independientemente).
- Usando el nonce se obtiene un hash válido (menor que la dificultad).

Este último punto es muy importante: Mientras que encontrar un nonce válido es una operación tremendamente costosa en capacidad de cómputo, tiempo y energía, comprobar que ese nonce es válido es algo fácil y simple, porque sólo hay que calcular un hash una vez. De este modo, encontrar un bloque válido es muy difícil, pero comprobar la validez de un bloque es muy simple.

Un detalle importante es que, como en la cabecera del bloque se guarda el hash del bloque anterior, cada bloque "certifica" el anterior, de modo que se hace imposible modificar bloques antiguos.

Una vez que se ha validado el bloque, se acepta y se comparte con el resto de la red.

Clientes, monederos y transacciones

Bitcoin práctico. Los wallets.

Wallets, monederos, carteras. Se trata de el software fundamental para operar en bitcoins. Hay muchos y de muchos tipos, y su utilidad relativa depende del gusto, las necesidades y del interés de cada uno.

Es una buena idea tomarse con un poco de calma la elección del monedero.

Empecemos con algunos consejos y recordatorios.

Software libre

Como ya comentamos, es una muy buena idea que cualquier monedero de Bitcoin que utilicemos sea software libre. Es bastante fácil (y bastante tentador) crear un wallet con una puerta trasera (es decir, un sistema por el que el creador del software pueda acceder a los datos del monedero), o uno que transmita todas nuestras claves a un servidor remoto, o que contenga algún tipo de troyano o, en general, cualquier sistema que ponga en peligro la privacidad de las transacciones o los propios fondos. El software libre es público y verificable, por lo que su seguridad en este sentido es mucho mayor.

Naturalmente, el software del monedero no es el único problema: Si nuestro monedero cuenta con todas las garantías pero el sistema operativo en el que está instalado es inseguro, hemos solucionado más bien poco. Como se suele decir, "Cualquier sistema de seguridad informática es tan fuerte como el más débil de sus eslabones".

Por eso los sistemas Linux (que también son software libre) son los más recomendables pero, si no podemos elegir o simplemente preferimos usar Windows, es conveniente seguir unos consejos básicos de seguridad, como mantener el equipo actualizado, usar un antivirus, usar contraseña de sesión, etc.

Programas de escritorio y servicios online

Los monederos que se instalan en el propio ordenador son siempre más seguros que aquellos que se usan remotamente, a través de páginas web o similares. Especialmente si son "nodos completos" y tienen una versión completa de la blockchain. Por otro lado, un wallet que sea nodo completo requiere de mucho más espacio en disco y es mucho más lento de instalar y de sincronizar con la red Bitcoin.

Hay monederos que se instalan en el ordenador pero no son nodos completos y, por tanto, no tienen una copia completa de la blockchain. Estas carteras necesitan menos espacio en disco pero son más inseguras, ya que usan servidores externos para validar las transacciones.

A menudo, los monederos online en páginas web y similares no están bajo el control del usuario (que no puede acceder a las claves de las direcciones de sus bitcoins) si no que son, en realidad, monederos controlados por otros.

Adicionalmente, los monederos online suelen cobrar comisiones (además de las propias comisiones a los mineros del sistema Bitcoin) por realizar transacciones.

Por otro lado, los monederos online son más cómodos, se puede acceder a ellos desde muchos dispositivos, y no requieren de tanto espacio en disco.

Seguridad

Recordemos que una cartera electrónica no es más que un conjunto de claves criptográficas que nos permiten acceder a direcciones de la blockchain. Si se pierden esas claves, se pierde el acceso a las direcciones. Sin esas claves no existe ninguna posibilidad de recuperar esos bitcoins. Desaparecen para siempre (en realidad no desaparecen, siguen ahí, pero es imposible gastarlos).

Todos los monederos tienen algún sistema de backup que nos permite guardar una copia de seguridad de nuestro monedero. Es muy conveniente usarlo para hacer una copia y guardarla en algún lugar seguro (y, preferentemente, lejos del ordenador donde está instalado el wallet). Las copias en la nube, como carpetas de Dropbox y similares, no son una buena idea. Si, a pesar de todo, se opta por guardar una copia en la nube, es muy recomendable utilizar algún tipo de herramienta criptográfica para asegurarla.

Si tienes tu monedero electrónico en tu ordenador portátil y te roban el portátil, te roban el monedero. Casi todos los wallets permiten limitar el acceso al programa o a partes de él mediante una contraseña. Es una buena idea usarla.

Muchas personas optan por usar un sistema de "cuenta caliente" y "cuenta fría" para separar bitcoins "corrientes" de bitcoin "de ahorro". La cuenta caliente es la que se usa normalmente para las transacciones que sea necesario efectuar, y la cuenta fría (también hay quién opta por usar más de una cuenta fría) se usa para guardar los bitcoins que no se piensan usar en breve y que es preferible mantener seguros.

Para ello se pueden usar varios sistemas, aunque lo más normal es usar dos carteras distintas instaladas en dos dispositivos distintos. Lo ideal es que el dispositivo que tiene la cuenta fría esté desconectado de internet.

Aspectos básicos de las transacciones

Recordemos que una transacción no está efectuada hasta que está incluida en la blockchain.

Además, en un momento dado puede haber en la red Bitcoin varias versiones de la blockchain que sólo se distingan en los últimos paquetes. Conforme vayan creciendo, una versión se acabará imponiendo a la otra.

Algunos monederos permiten decidir el feed que se quiere asignar a una transacción. Mayores feed harán que aumente las probabilidades de que la transacción se incluya en un bloque. Se trata de una cuestión estadística: Feed más altos hacen que la transacción sea más "apetitosa" para los mineros, que tendrán más incentivo para incluirla en su bloque.

Normalmente estos monederos calculan cual es un feed adecuado para un plazo de tiempo determinado (que normalmente se puede ajustar) en base a los promedios de bloques anteriores. Es una medida aproximada y se calcula en bitcoins por kilobyte (es menos importante la cantidad de bitcoins transferidos que el espacio que ocupa la transacción en la blockchain).

En cualquier caso, hay que tener siempre en cuenta que las transacciones en bitcoins son lentas. para empezar, dado que no se genera más que un bloque cada diez minutos, hay que esperar como mínimo en torno a ese tiempo para que alguien mine un bloque que contenga nuestra transacción. Si hay muchas transacciones con feeds mayores, probablemente haya que esperar más. A menudo horas.

Como, además siempre es posible que la versión de blockchain en la que está nuestra transacción sea reemplazada por otra más larga en la que no esté, es necesario esperar a que se vayan añadiendo bloques tras el que contiene nuestra transacción. Cada uno de estos bloques añadidos es lo que se llama "una confirmación" de la transacción. Cuantas mas "confirmaciones" tiene una transacción, más improbable es que aparezca una versión mas larga de la blockchain que no contenga el bloque de nuestra transacción.

Lo habitual es esperar cuatro confirmaciones pero, si es una transacción importante, es conveniente esperar cinco o seis confirmaciones (o incluso más) antes de darla por efectuada.

Dado que el bitcoin (BTC) tiene un valor de mercado tan alto, normalmente se opera en fracciones de este:

El milibitcoin (mBTC), que equivale a la milésima parte de un bitcoin.
El microbitcoin (µBTC), que equivale a la millonésima parte de un bitcoin.

Un pequeño error al indicar la moneda en una transacción puede ser desastroso.

Obteniendo bitcoins

Existen montones de páginas y servicios que ofrecen bitcoin, desde vendedores privados a páginas webs, pasando por entidades bancarias perfectamente legítimas o sospechosas ofertas en la red Tor.

La mayoría de legislaciones exigen que, para este tipo de transacciones (especialmente cuando son de un monto elevado) que podrían ser usadas para blanqueo de capitales y actividades similares, el comprador esté debidamente identificado (normalmente, enviando una fotografía en la que se vea una fecha escrita, el rostro del comprador y un documento identificativo.

Es posible encontrar lugares en los que las exigencias sean menores. En general, cuanto menores son las exigencias más caro resulta el cambio para el comprador, y más arriesgada la compra.

Una forma más fácil de obtener una (pequeña) cantidad de bitcoins es esperar al último módulo de este curso, en el que haremos un par de ejercicios prácticos de transacciones.

La mejor guía para elegir dónde comprar o vender bitcoins es la experiencia de otros usuarios. En este curso no se recomienda ningún sitio de compraventa de bitcoins, pero hay un foro abierto para que los alumnos puedan intercambiar opiniones.

Bitcoin Core

Bitcoin Core es el wallet oficial de la fundación Bitcoin, y es el wallet de referencia para el resto de monederos.

Es un programa que se instala en el propio ordenador del usuario y, como hemos visto, es software libre (con una licencia MIT) y tanto el programa como su código fuente están disponibles en internet para su uso, distribución, o para comprobar su seguridad y confianza.

Bitcoin Core actúa como un nodo completo, de modo que mantiene una versión completa de la blockchain y valida por sí mismo todas las transacciones.

Dado que es un nodo completo, bitcoin Core necesita descargar toda la blockchain para operar. Esto hace que la primera instalación del programa sea un proceso muy lento (puede tardar incluso días, si la conexión a internet es lenta). Además, cada vez que se inicia el programa, necesita actualizar la blockchain con los nuevos paquetes creados desde que se usó por última vez. Si hace varios días de esto, puede tardar un buen rato.

No depende de ningún servicio o web externos.

Bitcoin Core es, además, una cartera jerárquicamente determinista (hierarchical deterministic o HD). Esto significa que todas las claves que usa parta crear las cuentas son generadas a partir de una clave maestra única de un modo determinista, lo que significa que, en caso necesario, las claves de acceso a todas las cuentas pueden ser generadas de nuevo a partir de esa clave maestra, ya sea para recuperar un backup o para tener acceso al mismo monedero en otro dispositivo.

Bitcoin Core gestiona las direcciones de forma transparente al usuario, brotándolas para incrementar la privacidad, aunque permite al usuario controlar qué dirección quiere usar en cada momento.

Es compatible con la red Tor, y puede usarla para aportar un nivel mayor de privacidad.

A la hora de hacer una transacción, Bitcoin Core sugiere al usuario el feed adecuado para que la transacción se efectúe aproximadamente en un plazo determinado, basándose en los promedio de los últimos bloques. El usuario puede cambiar ese valor poniendo el feed que prefiera.

Al ser el monedero de referencia, Bitcoin Core puede ser usado para minar bitcoins. En la práctica, hoy día es imposible competir con los grandes mineros, pero el software está preparado para hacerlo y es perfectamente posible generar bloques (aunque, con toda seguridad, para cuando consiga crear un bloque, ya haya un montón más añadidos a la blockchain).

Bitcoin Core tiene también utilidades avanzadas, como consola de comandos, logs, gráficas de uso de red, visualizador de pares a los que está conectado, etc.

Tiene versiones para los sistemas operativos Windows, Mac y Linux.

Electrum

Electrum es uno de los monederos de Bitcoin más populares. Está basado en Bitcoin Core y es muy parecido a este.

Como Bitcoin Core, es un programa de escritorio que se instala en el propio ordenador. También es software libre y su código está disponible.

Electrum no mantiene una copia completa de la blockchain (no es un nodo completo), si no que sólo guarda las cabeceras de los bloques y usa una lista de servidores (que se puede configurar) y un algoritmo SPV (Simplified Payment Verification) para validar las transacciones. Esto, unido a que usa servidores centralizados, hace que sea más inseguro que Bitcoin Core, pero mucho más rápido y ligero.

También como Bitcoin Core, permite al usuario decidir el feed que quiere asignar (o si no quiere asignar ninguno) a cada transacción, aportanado sugerencias.

También permite usar la red Tor y rota las direcciones de las transacciones para mejorar el anonimato.

https://bitcoin.org/en/developer-guide#simplified-payment-verification-spv

Simple Bitcoin Wallet

Simple Bitcoin Wallet es un monedero para sistemas Android.

Al ser para dispositivos móviles, está enfocado a la ligereza, y no es un nodo completo. Esto hace que no pueda comprobar transacciones y necesite recurrir a otros nodos (usa un algoritmo SPV, como el de Electrum) para validar las transacciones, lo que lo hace menos seguro. Es también software libre y su código está disponible.

Como Bitcoin Core o Electrum, aconseja y permite al usuario decidir el feed que quiere asignar.

Armory

Armory es un wallet avanzado, con muchas más opciones que los que hemos visto anteriormente, pero también más complejo de usar.

Tiene muchas opciones de seguridad y backup, con opciones criptográficas avanzadas.

Armory es un nodo completo, por lo que valida todas las transacciones por sí mismo (a cambio de tener que mantener una copia completa de la blockchain).

También permite al usuario decidir el feed que quiere asignar a cada transacción, aportando sugerencias.

Armory rota las direcciones y puede usar Tor.

Bither

Bither es un pequeño wallet multiplataforma (lo hay en versiones para iOS, Android, Windows, Mac y Linux).

Es software libre (licencia Apache) y no es un nodo completo, por lo que usa un algoritmo SPV para validar las transacciones.

Bither reutiliza las direcciones de las transacciones, por lo que tiene menos privacidad que otros monederos. Además, no soporta Tor.

BitGo es un monedero web que puede ser accedido desde cualquier dispositivo. Para asegurar que las transacciones están exclusivamente bajo el control del usuario usa un sistema de doble firma (una de las cuales está en manos del propietario).

A pesar de todo, al ser un servicio web, todas las transacciones y validaciones se efectúan en un ordenador fuera del control del usuario. A cambio, no es necesario instalar ningún software.

Aunque no es tan seguro como una aplicación de escritorio, tiene bastantes controles de seguridad para ser una herramienta web.

Otros wallets

Algunos fabricantes venden wallets por hardware, con diseños que van desde pendrives a sofisticados aparatos con complejas medidas criptográficas.

También se pueden crear "wallets de papel", que consisten básicamente en QR-codes, con algunas aplicaciones y páginas web.

En definitiva, existen infinidad de wallets y aquí hemos visto sólo unos ejemplos más representativos. A pesar de ello, no es recomendable instalar cualquier wallet sin asegurarse antes de que es de cierta confianza.

Además de los vistos aquí, en la página oficial de la Fundación Bitcoin hay una amplia cloección de monederos.

No es ninguna mala idea darles un vistazo antes de elegir.

Enlaces de Descarga:

- Bitcoin Core
- Electrum
- Simple Bitcoin Wallet (Bitcoin Monedero)
- Armory
- Bither
- BitGo

Ejemplo de Wallet: Bitcoin Core

Aunque cada alumno puede decidir el software de wwalet que prefiera, y debería dar un vistazo a las opciones que se han visto, nostros vamos a usar bitcoin Core como ejemplo, dado que es el monedero de referencia y la mayoría de los demás lo imitan en mayor o menor medida.

La instalación de Bitcoin Core es como la de cualquier otro programa.

Para empezar, es necesario descargarlo de la página oficial de la Fundación Bitcoin.

La principal diferencia es que el programa debe descargarse la blockchain para poder operar (el programa nos permite elegir el directorio donde se almacenará). Esta descarga suele tardar horas y, si la conexión a internet es muy lenta, puede tardar incluso días. No es necesario hacer toda la descarga de una sola vez. Es posible cerrar el programa y continuar la descarga en otro momento, aunque es importante recordar que no debe apagarse el ordenador hasta que el programa se cierre completamente para evitar que los datos se corrompan.

Es posible acelerar este proceso descargando mediante Torrent el bootstrap.dat, un archivo con parte de la blockchain.

Bitcoin Core comienza a sincronizar la blockchain desde los bloques más antiguos a los más modernos. Hay que tener en cuenta que Bitcoin Core no sólo está descargando la blockchain, sino que también la está validando completamente.

En adelante, como cada vez que se inicie el programa habrá bloques nuevos, Bitcoin Core tendrá que descargar y validar también esos bloques.

La primera vez que se usa el programa, una vez actualizada la blockchain, tiene una pinta como esta:

En la esquina inferior derecha nos indica alguno detalles sobre el estado (si pasamos el puntero del ratón por encima, nos dará mas detalles): La unidad que estamos usando (BTC, mBTC o µBTC), si estamos usando claves HD (hierarchical deterministic), a cuántos pares estamos conectados y una marca de check verde si la copia local de la blockchain está actualizada.

En la Vista General podemos ver nuestro saldo. Es importante recordar que, en realidad, este saldo puede estar repartido en montones de direcciones dentro de bloques distintos de la blockchain. El monedero abstrae esa información y nos lo muestra como si fuera una sola cuenta.

En el cuadro de la derecha nos muestra las últimas transacciones realizadas, y indica si son de entrada, salida o entre nuestras propias cuentas.

Si queremos ver detalles de alguna transacción, podemos hacer clic sobre ella en el panel de la derecha o pulsar en el icono "Transacciones", en la barra superior.

Para enviar dinero sólo hay que usar el botón "Enviar" de la barra superior. En la ventana que se muestra tenemos un campo para insertar la dirección a la que vamos a enviar los bitcoins, y podemos elegir el feed que deseamos pagar seleccionándolo de una lista de feeds recomendados o escribiéndolo notros mismos directamente.

Abajo hay un botón para añadir destinatarios: Una transacción puede ser de un número indeterminado de direcciones a un número indeterminado de direcciones.

En caso de que tengamos bitcoins almacenados en varias direcciones, el programa se ocupa de rotarlas, de modo que no usemos siempre la misma, para hacer más difícil el rastreo de las operaciones.

En la barra de botones también hay un botón para "Recibir bitcoins". Usando este se manda a través de la red Bitcoin un mensaje a la cuenta que le indiquemos solicitándole la cantidad de bitcoins que hayamos puesto. Este mensaje va encriptado con la clave pública de la cuenta a la que se dirige, por lo que sólo el propietario de esa cuenta puede leerlo. Esto es un simple mensaje, como un correo o cualquier programa de chat, y no es una transacción ni se almacena en la blockchain.

Por defecto, Bitcoin Core creará una dirección distinta cada vez que se solicite dinero. Aunque es posible obligarle a reutilizar direcciones, es una buena política no hacerlo para hacer más difícil el rastreo de movimientos en nuestras cuentas.

Las transacciones, tanto de entrada como de salida, pueden etiquetarse con un nombre o una descripción. En cualquier caso, se trata de una etiqueta privada e interna al programa que no se transmite a la red bitcoin.

Si queremos ver las direcciones que estamos usando para enviar o recibir bitcoins, debemos ir al menú "Archivo". Allí tenemos un apartado para las direcciones de envío (en el que podemos agregar nuevas direcciones, pero que raramente se usa) y otro para las direcciones de recepción (donde podemos crear nuevas direcciones para que nos envíen bitcoins). En las tablas que nos muestra aparece la etiqueta que les hayamos puesto (que es privada, informativa y sólo la vemos nosotros) y la dirección de la transacción. Esta dirección es pública y cuando, por ejemplo, queramos que nos envíen bitcoins, es la dirección que debemos dar para que nos puedan ingresar la cantidad que sea en ella.

Bitcoin Core guarda todas las claves e información en el archivo wallet.dat, en el directorio que le indicamos durante la instalación. Por defecto, este archivo está en "C:\Users\Nombredeusuario\Appdata\Roaming\Bitcoin" en sistemas Windows, "~/.bitcoin/" en sistemas tipo Linux o "~/Library/Application Support/Bitcoin/" en Mac.

Si ese archivo se borra o se corrompe, lo perderemos todo. Es. por tanto, muy importante hacer una (mejor dos, o varias) copia de seguridad.

Para ello podemos simplemente copar ese archivo a mano, pero también tenemos la opción "Guardar copia del monedero" del menú "Archivo".

Una opción interesante es firmar mensajes con alguna de nuestras direcciones de bitcoin. Esto se usa para asegurar que el mensaje está enviado por el propietario de esa cuenta.

Por ejemplo: Sabemos que Satoshi es el propietario de los bitcoins creados en el primer bloque de la blockchain (el llamado "bloque génesis"). Si yo quisiera demostrar que en realidad soy Satoshi, sólo tendría que firmar con la clave de esa dirección un mensaje diciéndolo, y publicarlo en cualquier sitio (una página web, facebook...).

El siguiente elemento del menú Archivo sirve para verificar la validez de las firmas que recibamos.

Recordemos que cualquiera que tenga acceso a nuestro ordenador (ya sea de modo físico como remotamente) tiene acceso a nuestro monedero. En el menú Configuración tenemos opción a cifrar nuestro monedero, de modo que sólo quién conozca la frase de paso (sí, una frase es mucho mejor que una sola palabra) pueda acceder a nuestros bitcoins.

Bitcoin Core tiene más opciones, e incluso un potente interfaz de línea de comandos que, entre otras cosas, nos permite minar. Pero estas que hemos visto son las herramientas principales que, de un modo u otro, comparten todos los monederos.

Tecnologías blockchain más allá de Bitcoin

Las hijas de Bitcoin

EL nacimiento y, sobre todo, el éxito de Bitcoin ha dado lugar a multitud de monedas que tratan de segur su estela.

Muchas son copias de la idea original con más o menos variaciones, pero otras muchas son "forks", es decir, modificaciones de la moneda original

En bitinfocharts.com pueden verse y compararse más de cuarenta de ellas.

Vamos a ver unos ejemplos.

Bitcoin Cash

Surgido en agosto de 2017, Bitcoin Cash (BCH) es el último fork de Bitcoin.

Bitcoin Cash ha sido ideado para resolver los problemas de escalado más inmediatos de Bitcoin, aumentado el tamaño de bloque hasta los ocho megabytes (ocho veces más que bitcoin).

Aunque en el momento de su implantación comenzó con bastante éxito y parecía que iba a imponerse sobre su antecesor, actualmente parece que no acaba de convencer a usuarios y mineros, que siguen prefiriendo el viejo Bitcoin. Aunque se trata de un fork muy reciente que tuvo mucho empuje, y aún puede levantar cabeza.

Litecoin

Litecoin (LTC) fue lanzado en 2013, y es probablemente el fork de Bitcoin con más éxito (aunque sigue teniendo mucha menos popularidad que su predecesor).

Nacido para tratar de resolver algunos de los problemas de Bitcoin, Litecoin tiene algunas características que lo hacen más flexible y escalable, como un mayor número de unidades totales (84 millones en lugar de 21), una mayor frecuencia de generación de bloques (uno cada dos minutos y medio) y una prueba de trabajo que reduce la ventaja de los grandes sistemas de hardware de minería.

Aunque no soluciona todos sus problemas, Litecoin es una moneda más funcional que Bitcoin. De todos modos, no parece que vaya a imponerse sobre este.

Monero

Monero (originalmente BitMonero) es una interesante criptomoneda enfocada explícitamente a la privacidad.

Cuando se hizo notar que las noticias originales sobre la privacidad de Bitcoin estaba bastante exageradas, se vio la necesidad de una moneda que sí fuese realmente anónima, con un mecanismo que enmascarase las transacciones y protegiese la privacidad de los intervinientes.

La primera moneda en tener este objetivo fue Bytecoin, de la que nació Monero como fork.

Las transacciones en Monero (XMR) están protegidas por varias firmas criptográficas (ring signatures), de las cuales sólo una pertenece realmente al propietario, mientras que el resto sólo existen para dificultar el rastreo de las transacciones.

Además, Momero usa un algoritmo de minado que trata de paliar la ventaja de los grandes mineros, y no tiene límite máximo a la cantidad de moneda minada.

Ethereum

Ethereum nació en 2013 y es, probablemente, el heredero más famoso y exitoso de Bitcoin. Y lo es por buenas razones.

Como Bitcoin, se basa en una blockchain para operar (que como toda blockchain, es pública y puede examinarse) pero, al contrario que este, su objetivo principal no es actuar como una moneda.

El objetivo del proyecto Ethereum es construir una red de computación distribuida.

El ritmo de creación de bloques en la blockchain de Ethereum es unas cuarenta veces mayor que el de Bitcoin, creándose aproximadamente uno cada quince segundos. Además, los bloques no tienen un tamaño máximo.

En Ethereum, la creación de "moneda" (el Ether) durante el proceso de minado es constante, creándose la misma cantidad fija (5 eth) en cada bloque, independientemente del tiempo, con lo que no hay un límite superior a la cantidad de Ether que puede existir (recordemos que hay un tope máximo de bitcoins). Es decir, que el Ether, al contrario que el Bitcoin, es inflacionario en lugar de deflacionario.

Esto es así porque,como veremos, el Ether está concebido como "combustible" para el procesamiento más que como herramienta especulativa o recurso de inversión. Es más importante para el buen funcionamiento de la red incentivar su uso que su ahorro.

Ethereum usa un algoritmo de Prueba de Trabajo propio, llamado Ethash especialmente diseñado para evitar uno de los mayores problemas de Bitcoin: El monopolio de los grandes mineros. Se supone que Ehash es mucho más independiente a la potencia de cálculo que la Proof of Wrok de Bitcoin, de modo que un pequeño minero independiente tiene más posibilidades de éxito aunque se enfrente a competidores con una gran capacidad de cómputo.

Contratos inteligentes

Como apuntábamos antes, el objetivo de Ethereum no es crear una moneda, sino una plataforma de computación distribuida. Y, para ello hace uso de los llamados "contratos inteligentes" (smart contracts).

Un contrato inteligente es un programa informático que ejecuta una serie de acciones cuando se cumplen ciertos requisitos preestablecidos. Un contrato inteligente, una vez creado, es inmodificable e incancelable, y se ejecutará o no en función de las condiciones que se le hayan programado.

Las acciones que efectúe un contrato pueden ser de todo tipo (es posible incluso vincular dispositivos de hardware para que lean la blockchain y actúen de un modo determinado cuando se active un programa concreto) pero, normalmente, suelen consistir en la ejecución de transacciones. Del mismo modo, las condiciones que hacen que un contrato inteligente se active pueden ser de todo tipo.

No hay que caer en el error de pensar en los contratos como en un mero texto firmado por dos partes o algo así de simple. Un "contrato" puede ser un programa muy complejo. Algunos ejemplos de posible aplicaciones de los contratos inteligentes en ethereum son crear nuestra propia criptomoneda, sistemas de votación, apuestas, sellos de tiempo, plataformas de crowfunding, juegos, etc.

Se puede ver una lista de más de ochocientas aplicaciones que están funcionando actualmente en Ethereum en esta página.

Los contratos en Ethereum deben ser "alimentados" con una cantidad de ether que depende de su complejidad, y que es el modo de pagar por el tiempo de procese dedicado a la ejecución del contrato por parte del minero que lo incluye en la blockchain de Ethereum (al ether con el que se alimenta un programa se le llama "gas).

(Bitcoin tiene soporte para contratos inteligentes muy simples, como cuentas multi-firma o sellos de tiempo, pero es muy limitado y apenas se usa)

Solidity

Para ejecutar los contratos, el software de Ethereum dispone de una máquina virtual llamada Ethereum Virtual Machine (EVM). Por seguridad, la EVM ejecuta el código de forma totalmente aislada del la red o del sistema de archivos del usuario.

El lenguaje que usa Ethereum para codificar los contratos se llama Solidity, y es un lenguaje "Turing completo", lo que básicamente significa que no está limitado y se puede usar para escribir cualquier programa imaginable.

Se trata de un lenguaje no demasiado complejo, parecido a javascript, aunque puede ser algo difícil de aprender para los que no estén demasiado familiarizados con la programación. En cualquier caso, pueden verse todos los detalles de este lenguaje en su página.

Si alguien quiere comenzar a programar en Solidity, existen montones de entornos de programación y complementes para los IDEs y editores más conocidos (hay una lista aquí).

También existe una página para programar Solidity de modo online sin necesidad de instalar nada.

Instalar Ethereum

Naturalmente, el cliente oficial de Ethereum es software libre, y puede descargarse gratuitamente en su página web.

Un detalle internaste de Ethereum es que dispone de una blockchain aparte para tests, en la que se puede minar ether muy fácilmente y usarlo para experimentar sin riesgos.

Nuestra propia blockchain

Como hemos visto, Ethereum es mucho más que una moneda, y eso es lo que ha hecho dispararse su popularidad.

Aunque se puede usar como moneda igual que Bitcoin y, de hecho, se cotiza en los mismo mercados, la idea detrás de Ethereum es la de servir de plataforma universal que pueda dar soporte a otras herramientas basadas en blockchain.

El atractivo de Ethereum es que se presenta como una forma fácil y simple de construir nuestra propia tecnología blockchain.