GUÍA BITCOIN 2018

LA GUÍA MÁS PRÁCTICA, COMPLETA Y ACTUALIZADA PARA INICIARSE Y AVANZAR EN EL MUNDO BITCOIN

ALBERTO F. FERNÁNDEZ

Guía Bitcoin 2018

La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo Bitcoin

Alberto F. Fernández

o cualquier otro, sin la previa autorización escrita por parte del autor.

Índice

¿Quién soy?

Hace muchos años, de hecho varias décadas, que soy un apasionado por la tecnología en todos sus aspectos, por cómo está cambiando el mundo y por cómo lo cambiará en el futuro, a una velocidad cada vez mayor. Poco después también empecé a desarrollar un interés por el mundo de la economía y la empresa. Este doble interés me llevó a una doble carrera, en lo tecnológico a estudiar Ingeniería Informática y un Máster en Sistemas de Información, y en lo empresarial a completar un MBA (Master of Business Administration) en una de las más

prestigiosas universidades. Mi carrera profesional ha transcurrido varios años en la consultoría estratégica y tecnológica, actividad que he compatibilizado con ser profesor de finanzas en la universidad.

Hace algún tiempo conocí el mundo de los bitcoins, y desde el principio vi un potencial inmenso para cambiar el mundo y tener un impacto en nuestro futuro. Por otro lado me pareció una tecnología compleja, difícil de comprender y utilizar por personas sin un perfil técnico. Y así nació la idea de escribir un libro que fuera capaz de transmitir el potencial y las capacidades del universo bitcoin de manera sencilla

y práctica a personas que no tienen un conocimientos especifico de informática o de finanzas.

¿Por qué este libro?

La información sobre Bitcoin es prácticamente ilimitada en Internet. Puedes buscar la palabra Bitcoin en Google, y seleccionar únicamente resultados en español:

Aproximadamente 8.870.000 resultados (0,49 segundos)

¿Qué sentido tiene entonces escribir un libro sobre Bitcoin? Creo que el problema hoy en día no es la falta de información, sino el dar sentido a toda esta información, el filtrar aquélla de calidad y convertirla en conocimiento útil, que permita aplicar lo aprendido, desarrollar habilidades que no tenías antes de empezar a leer. Hoy en día el conocimiento que puede encontrar en Internet sobre cualquier materia es inmenso, realmente inabarcable para cualquier persona que no se dedique a eso en exclusiva, incluso con frecuencia también es inabarcable para estas personas. Este conocimiento aparece con mucha frecuencia disperso, desorganizado, falto de rigor,

desactualizado, incorrecto (a veces maliciosamente incorrecto), o directamente no es entendible para una persona no experta en la materia.

Este libro te ofrece lo siguiente:

- **Información útil y práctica,** proporcionándote la información que necesitas para navegar en este nuevo mundo de las criptomonedas, entender lo que son, cuáles son sus ventajas (y desventajas), cómo las puedes utilizar, y cómo pueden cambiar el mundo en el que vivimos
- **Explicaciones sencillas desde el principio,** ya que esta guía no

asume ningún conocimiento previo de informática ni de finanzas

- **Actualizada,** el mundo de las criptomonedas cambiar constantemente, con frecuencia en días o semanas. La información desactualizada en este entorno tan cambiante no tiene sentido
- **Completa,** conteniendo toda la información y los recursos para adentrarte en el mundo de Bitcoin y las criptomonedas
- **Rigurosa,** tanto a nivel de tecnología como financiero, ya que el autor posee formación de y experiencia profesional en ambos ámbitos
- **Sin intereses ocultos,** en Internet

podrás encontrar mucha información “gratuita”, pero como sabes la información gratuita muchas veces no acaba de serlo, y en ocasiones está sesgada al ser proporcionada por empresas que pretenden hacer negocio de las acciones que emprendas con esa información. En mi caso soy un escritor particular, sin afiliación de ningún tipo con ninguna empresa en este ámbito, por lo que siempre te daré la información y los consejos que crea que pueden beneficiarte más, sin ataduras ni condicionantes

Para cualquier comentario o sugerencia

puedes contactarme en este correo electrónico: albertof.fernandez3@gmail.com

¿Estás preparado? ¡Empezamos!

1. Qué es un bitcoin

Concepto de bitcoin

Parece una pregunta tan obvia y sencilla, y sin embargo la respuesta no es tan sencilla a priori. ¿Preguntamos a Wikipedia?

“El bitcoin (signo: BitcoinSign.svg; abr.: BTC, XBT) es una criptomoneda concebida en 2009.▮ El término se aplica también al protocolo y a la red

P2P que lo sustenta, y de forma común se denomina como una moneda digital.▮”

Si has entendido algo, enhorabuena. ¿Qué es una criptomoneda? ¿Y un protocolo? ¿Y una red P2P, es como el emule?

Dicho de una manera directa, el bitcoin es una **moneda virtual, regulada por un complejo algoritmo informático y cuya información de poseedores de estas monedas se recoge de forma anónima en un libro electrónico de actas llamado “blockchain”.** Vamos a entrar a explicar estos conceptos:

Moneda virtual

Nunca verás un billete ni una moneda física de bitcoins. La moneda existe únicamente de forma digital, como información en una red de ordenadores. Bueno, en realidad ya utilizas dinero virtual aunque no te lo cuenten así, cuando utilizas euros. Dirás que los euros existen en la realidad, como billetes y monedas. Pero la realidad es que únicamente alrededor del 8% de los euros, dólares, etc emitidos existe en formato físico. El otro 92% existe exclusivamente en forma electrónica, como puedes ver al hacer transferencias, domiciliar recibos, entregar cheques, etcétera.

Regulada por un complejo algoritmo informático

Este sí es un cambio esencial respecto a las monedas convencionales. Una monedas convencional, como el euro, es emitida por un banco central, en nuestro caso el Banco Central Europeo (BCE). Es él quien regula la cantidad de euros emitida, los tiempos y la forma en que se emiten. Por contra en el caso de Bitcoins no hay ningún banco central ni gobierno ni organismo financiero detrás. ¿Y entonces? Existe un complejo algoritmo informático que regula la cantidad de Bitcoins que se emiten, y cuándo se emiten. Un algoritmo podríamos definirlo como un conjunto de reglas, de

pasos para hacer una tarea o resolver un problema. Por ejemplo el algoritmo para arrancar un coche podría ser introducir la llave en el encendido, girar la llave, pisar el embrague, meter primera marcha, y soltar lentamente el embrague mientras aprietas suave y progresivamente el acelerador. De manera similar el algoritmo Bitcoin regula en detalle cómo se generan los bitcoins, su número, cómo se envían, hasta los más pequeños detalles de su operativa.

Los Bitcoins entraron en circulación en enero de 2009, y desde entonces este algoritmo ha demostrado un funcionamiento tremendamente robusto.

La gran ventaja de la regulación por un algoritmo es que Bitcoin está a salvo de cualquier interferencia por gobiernos, políticos y autoridades económicas. Esto le protege de decisiones de devaluaciones de monedas, corralitos, etcétera. El número máximo de Bitcoins que jamás existirá se definió antes de que existiera el primer bitcoin, y es de casi 21 millones. Actualmente (finales de 2017) existen unos 17 millones de bitcoins en circulación, y el ritmo de creación de nuevos bitcoins por parte de los llamados "mineros" se va reduciendo a medida que el número de bitcoins va aumentando.

Bitcoin surgió inicialmente como una

publicación académica que explicaba el algoritmo y el ecosistema: “Bitcoin, un sistema de dinero electrónico peer-to-peer”, cuyo autor es Satoshi Nakamoto. ¿Quién es Satoshi Nakamoto? Nadie lo sabe (excepto él/ella). Claramente es un seudónimo, algunos dicen que es una persona concreta, otros que un pequeño grupo de personas. Tal vez nunca lo lleguemos a sabe, y esa es parte del misterio.

Información de titularidad anónima recogida en una especie de libro electrónico de actas llamado “blockchain” o “cadena de bloques”

Cuando abres una cuenta en un banco, el

banco realiza una identificación del titular, y crea una cuenta con tu nombre y apellidos, cada euro que pasa por ésta se encuentra asignado a un titular. En el caso de los bitcoins existe un gran libro electrónico que recoge todas las transacciones realizadas en bitcoins desde que éste nació hasta la actualidad. Cada bitcoin minado, cada bitcoin (o fracción) enviado por alguien a otro alguien aparece en este libro, desde el comienzo. Este libro tiene dos características de las al menos una es sorprendente:

1. Es público, cualquier persona puede ver todo lo que contiene, de hecho hay una web que contiene

toda la información de manera accesible https://blockchain.info/es

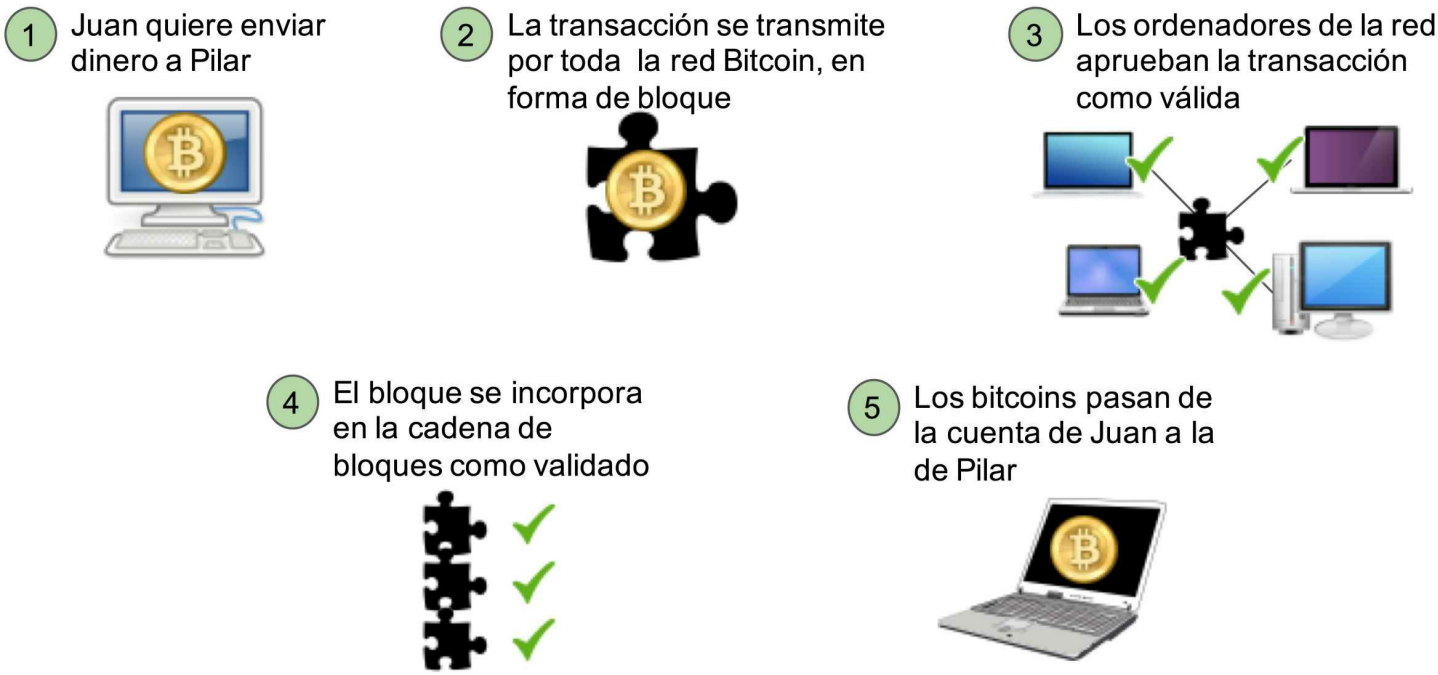
2. Es "anónima". Al contrario del caso de tus cuentas bancarias, tu nombre, apellidos u otro identificador personal no aparecen en ningún lugar. ¿Entonces cómo sé que es mía? Por el código de tu/s cartera/s virtuales que creas cuando quieres poseer bitcoins

Esta blockchain o cadena de bloques está almacenada de manera completa en miles de ordenadores de todo el mundo. No son ordenadores especiales ni están registrados de manera oficial. Cualquiera puede descargarse un

programa en su ordenador y conectar su ordenador a esa red, pasando a ser un nodo más. Esta característica de que no hay un ordenador central, ni siquiera un registro de nodos, sino muchos ordenadores de todo tipo es lo que se conoce como red Peer-to-Peer.

Como podrás imaginar, este registro de todas las operaciones que han ocurrido desde el principio es un archivo muy largo, tanto como de más de 150 Gigabytes (GBs) y creciendo a un ritmo de unos 5 GBs cada mes.

Cómo funciona la cadena de bloques (Blockchain)



¿Qué es poseer un Bitcoin?

Empecemos por algo más sencillo, ¿Qué es poseer un euro? En su forma de dinero físico, poseer un euro es simplemente tenerlo físicamente en nuestra posesión, en una cartera, monedero, etcétera. En su forma digital es un poco más complicado, y supone

ser titular de una cuenta de un banco o de algún otro producto financiero (depósito, fondo, etc.) en el que hay euros depositados o invertidos.

El bitcoin es una moneda virtual, no física, por lo que la primera forma no aplica. Pero además hemos comentado que los bitcoins no están asignados a un titular identificado de manera personal. ¿Cómo es posible entonces poseer un bitcoin? **En realidad poseer un Bitcoin es poseer una clave muy compleja que identifica una cuenta virtual en la que ese bitcoin está depositado.** Esta clave tiene dos formas, una clave privada que sólo el dueño de esa cuenta debe de tener, y una clave pública, que puede

compartirse con otras personas para que puedan enviar bitcoins a nuestra cuenta.

Una **clave privada** tiene 256 bits o dígitos binarios, es decir sería una secuencia de 256 ceros y unos. Para simplificar un poco el formato, se convierten estos ceros y unos en letras (de la A a la E) y números según un código estándar, y así se puede representar como una secuencia de 64 dígitos hexadecimales (dígitos numéricos y letras A-E). Por ejemplo, esto sería un ejemplo aleatorio de clave privada:

1E99423A4ED27608A15A2616A2B0E9

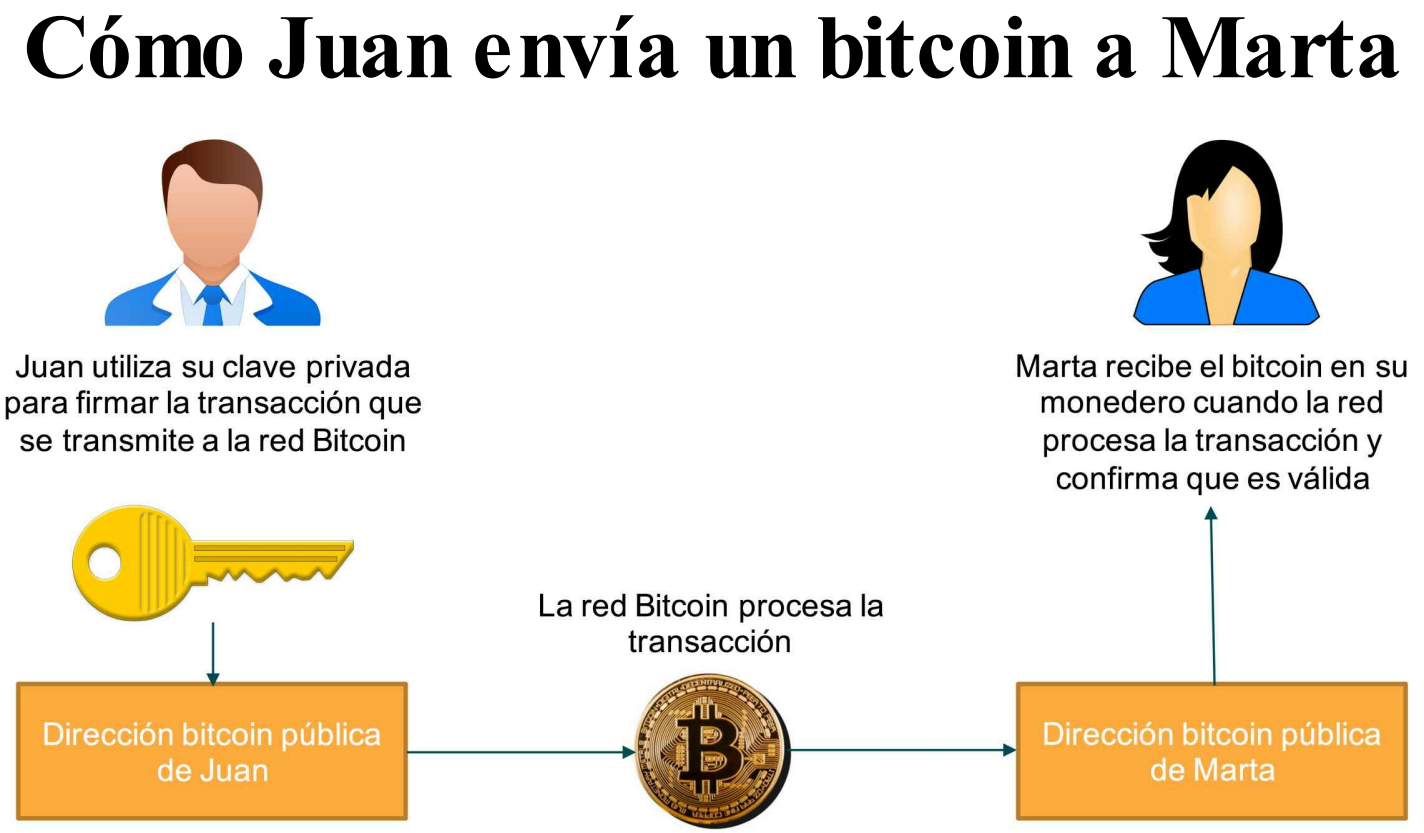
La clave privada es algo así como el usuario y la contraseña de nuestra cuenta del banco, incluso más secreta ya que no existe ninguna información personal que permita identificar al poseedor de los bitcoins si alguien se apropiara de ellos. Nadie debe de saber jamás nuestra clave privada, ya que con esta información podría hacerse pasar por nosotros a todos los efectos, y por tanto disponer de nuestros bitcoins. Pero es que además si en algún momento perdiéramos esta información, no podríamos acceder a nuestra cuenta de ninguna manera, ya que nadie conoce quién es el titular de esa "cuenta", y no es posible conseguir esa información.

A partir de esta clave privada se genera una **clave pública, o dirección bitcoin**, mediante una función matemática muy compleja, que asegura que cada clave pública se corresponde únicamente con una clave privada. He aquí un ejemplo aleatorio de una clave pública o dirección bitcoin:

1J7mdg5rbQyUHENYdx39WVWK7fsLp

La clave pública es parecido al número de cuenta en un banco, es la "dirección" que hay que indicar en una transacción para reflejar el destino de ese bitcoin. La clave pública aparece en cada transacción reflejada en el blockchain, y por tanto es pública y visible por todos.

Lo que no se sabe es quién es el “titular” de esa clave pública.



O sea que la clave privada no la puede saber nadie más que el titular, y la clave pública la puede saber cualquiera que nos vaya a enviar bitcoins. La clave pública deriva a través de un procedimiento matemático de la clave

privada. ¿Hay riesgo de que alguien averigüe nuestra clave privada a partir de la clave pública que cualquiera puede ver? Esta es una pregunta fundamental, y la respuesta es que no se conoce por el hombre ninguna manera que en un tiempo razonable (menos de miles de años) y con los mejores ordenadores disponibles, haga capaz de obtener la clave privada a partir de la clave pública. Esto es esencial para que todo el sistema funcione.

¿Podemos quedarnos sin claves privadas? La respuesta es que no. Dado que una clave privada tiene 256 bits (ceros y unos), el número de posibles claves privadas es 2^256, un número

inimaginablemente grande, ¡cercano al número de átomos en el universo visible!

Los bitcoins son creados a través de un procedimiento en el que los ordenadores conectados a la red bitcoin resuelven unos puzzles matemáticos muy complejos, que permiten seguir incluyendo transacciones en la cadena de bloques. Esto es lo que se llama minería de bitcoins. Cualquier ordenador puede unirse a esta actividad de minería, sin embargo hay que tener en cuenta que el coste en ordenadores y en electricidad para realizar esta actividad es muy importante.

Cuando manejamos euros, sabemos que usamos unidades (1 euro, 2 euros, 100 euros…) y fracciones de 1/100 que llamamos céntimos. Por ejemplo, podemos comprar algo que vale 2,29 euros, 2 euros y 29 céntimos. De manera similar, en el caso de bitcoins podemos manejar unidades enteras (1 bitcoin, abreviado BTC, 5 bitcoins, etcétera). Sin embargo, debido a que el valor de un bitcoin es muy elevado, se utiliza el **Satoshi** como equivalente a los céntimos. De hecho un Satoshi es la fracción más pequeña de un bitcoin que se puede enviar, y equivale a la cienmillonésima parte parte de un bitcoin, es decir 1 Satoshi = 0,00000001 BTC. Si, por ejemplo, 1 BTC valiera

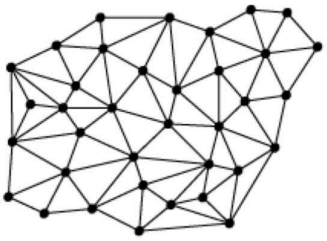
10.000 euros, 1 Satoshi equivaldría a 0,01 céntimos de euros. Un Satoshi por tanto es una unidad muy pequeña actualmente, sin embargo si el valor del bitcoin continúa elevándose, es necesario disponer de fracciones muy pequeñas para poder convertir a cualquier cantidad en euros, inclusive no puede descartarse que en el futuro se actualice el protocolo para permitir divisiones aún más pequeñas.

Características del bitcoin

¿Cuáles son las ventajas y desventajas del bitcoin respecto a las monedas que

usamos habitualmente (llamadas FIAT)?

Principales características de bitcoin



Descentralización

Globalidad

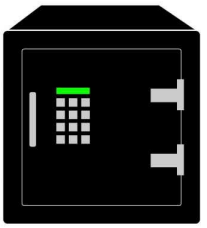
Transparencia

Costes reducidos

Ausencia de control

Anonimidad

Rapidez



Seguridad

Descentralización y ausencia de control por parte de gobiernos

No hay una autoridad central en la red bitcoin. La red bitcoin está formada por miles de ordenadores de todo tipo y características, y no hay un proceso de

registro para ser parte de esta red, cualquiera puede instalarse el software y ser parte de la red en minutos. Cualquier cambio que se propone en el software de esta red, debe de ser aceptado por la mayoría de estos ordenadores para realizarse de manera efectiva, en este sentido es una red democrática.

Esta distribución mundial de la red, la mantiene a salvo de decisiones de gobiernos particulares, como aquellas que llevan a devaluaciones de monedas, corralitos, limitaciones al cambio de unas monedas por otras, etcétera. Por esta razón, el bitcoin está siendo habitualmente utilizado como moneda

reserva en situaciones de crisis financiera (como la de Argentina hace algunos años) o política, y en algunos foros está siendo considerada como el nuevo oro. Por ejemplo, en situaciones recientes de amenaza por parte de Corea del Norte a sus países vecinos, los habitantes de Corea del Sur y Japón se convirtieron en los mayores compradores de bitcoins como moneda refugio ante una posible crisis militar que impactara de manera important a sus monedas locales.

De todas formas una cosa es que no haya control del sistema por parte de gobiernos y otra muy distinta que algunos gobiernos no puedan legislar

sobre bitcoins, actividad que sí está ocurriendo y de manera creciente. Tenemos algunos ejemplos recientes:

- El gobierno de Japón declaró en 2014 que bitcoin no era una moneda. Sin embargo apenas 2 años más tarde declaró el bitcoin una moneda legal en ese país
- El tribunal de justicia europeo decidió en 2015 que bitcoin es una moneda, y que por tanto las transacciones de compraventa de bitcoins con monedas fiat (como el euro) no está sujetas a IVA, como sí lo estarían si bitcoin se considerara un propiedad
- Sin embargo el IRS, la hacienda

estadounidense, decidió en 2015 que bitcoin es una propiedad, sujeta a impuestos de propiedad

- En septiembre de 2017 el gobierno chino decidió prohibir las empresas de compraventa de bitcoins en su territorio

Moneda única a nivel global

Todas las monedas fiat están vinculadas a un país (como el Yen a Japón) o a un conjunto de países (como el Euro en varios países de la Unión Europea). Si quieres utilizar la moneda de un país en otro, tienes que realizar un intercambio de esa moneda por la del país local.

Este intercambio de monedas supone además un coste muy importante.

No es así con el bitcoin. Todos los bitcoins son iguales, y ningún bitcoin está asignado a un territorio concreto. Esto hace que pueda ser una moneda que se utilice directamente como tal en cualquier país sin necesidad de intercambio por otras monedas.

Transparencia

Como hemos comentado todas (sí, absolutamente todas) las transacciones de bitcoins desde el principio están reflejadas en este libro de actas electrónico que es blockchain, y que además es inmutable en lo ya escrito por

una serie de procedimientos criptográficos muy seguros. Por eso podemos saber la secuencia y momentos en los que cada bitcoin ha sido minado o transferido.

Anonimidad

Hemos comentado que no hay ninguna información personal en el libro histórico de transacciones o blockchain. Nadie puede con esa información asignar un dirección privada de bitcoin con una persona concreta. Además una persona u organización puedes crear instantáneamente múltiples direcciones privadas evitando una identificación de movimientos repetidos.

Sin embargo esta anonimidad depende de ti. Si en algún momento difundes información que relaciona tu dirección pública con tu identidad, esta anonimidad desaparece. Por otro lado si un gobierno de verdad te está investigando tiene los medios para poder relacionar a una persona concreta con una dirección bitcoin, por ejemplo revisando el tráfico desde tus conexiones a internet.

Rapidez de transacción

Cuando realizamos un envío de dinero por transferencia bancaria nacional, el dinero tarda 1-2 días en estar disponible

en la cuenta de destino. Si esta transacción es a otro país tarda varios días. Un envío de bitcoins tarda únicamente unos minutos en estar disponible en la "cuenta" de destino

Costes de transacción reducidos

Cada año muchísimas personas, por ejemplo inmigrantes, envían una cantidad ingente de dinero a sus países de origen. Estos envíos de dinero conllevan unas comisiones muy elevadas, en torno al 7%, incluso más. En el caso del bitcoin los costes de transacciones son reducidos y además no dependen de la cantidad transmitida. Recientemente hubo un ejemplo de una

transacción por 20 millones de dólares con un coste de transacción de ¡5 céntimos de euro!

Seguridad del sistema

El hecho de que todo el historial de transacciones de bitcoin desde que se inició esté almacenado en miles de ordenadores de todo tipo por todo el mundo (también en el tuyo si lo deseas), y bloqueado de posibles modificaciones, hace del bitcoin una moneda segura, casi imposible de intervenir por un gobierno, autoridad o agente malicioso. Los algoritmos en los que se basa han resistido sin problema los más duros tests de seguridad por

parte de matemáticos, hackers, gobiernos, etc. ¿Por qué leemos entonces noticias de robos de bitcoins millonarios? Porque…

…la seguridad de nuestros bitcoins depende de nosotros. Puedes construir la casa más segura del mundo, que dejará de serlo si dejas la puerta abierta y la alarma desconectada. Pasa lo mismo con bitcoin. Si no eres cauto en dónde y cómo almacenas tus bitcoins y la dirección privada, un criminal puede robarlos. Por otro lado si adoptas todas las medidas de precaución que comentaremos, la seguridad es elevada.

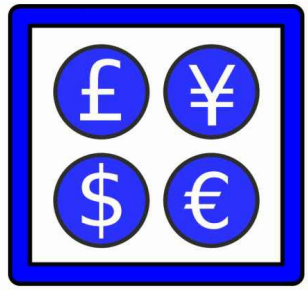
2. Para qué sirve un bitcoin

Una moneda, ya sea física o virtual, tiene valor en la medida en que podemos utilizarla para algo, ahora o en el futuro. Los euros nos permiten comprar comida, vivienda, pagar la electricidad, ahorrar, etcétera.

Algunos usos de bitcoin

Comprar en tiendas

Enviar dinero



Pagos entre empresas

Obtener dinero en metálico

Invertir

Donar

Moneda refugio

Bitcoin ya está cambiando nuestro mundo financiero y lo va a hacer de manera más radical en los próximos años. Ahora mismo en todo el mundo hay miles y miles de personas desarrollando ideas de cómo será el futuro de las finanzas para nosotros. Muchas de estas ideas son incluso difíciles de anticipar en este momento. Por tanto en este capítulo voy a

comentar algunos usos actuales de bitcoin, otros emergentes y apuntar algunos de futuro.

Comprar en comercios

Ésta es una de las más claras utilidades de una moneda, si bien todavía está muy poco extendida por parte de los establecimientos. Pagar en tiendas con bitcoins tiene varias ventajas como la posibilidad de evitar comisiones por pago con tarjeta, o el hecho de que no es necesario cambiar de moneda, pudiendo pagar en cualquier país con mis bitcoins.

Actualmente hay miles de

establecimientos en todo el mundo que aceptan bitcoins como medio de pago, si bien en general se trata de establecimientos individuales, no de grandes cadenas. Este pago lo puedes realizar por ejemplo en una tienda física con una cartera instalada en tu móvil (prácticamente tan fácil como pagar con tu móvil de otra manera), o en una tienda virtual con tu cartera bitcoin del ordenador. Todavía estamos lejos de que cualquier tienda cercana los acepte, pero sí hay ejemplos de tiendas que los utilizan en viajes, comida, casas, grandes almacenes, informática, etcétera.

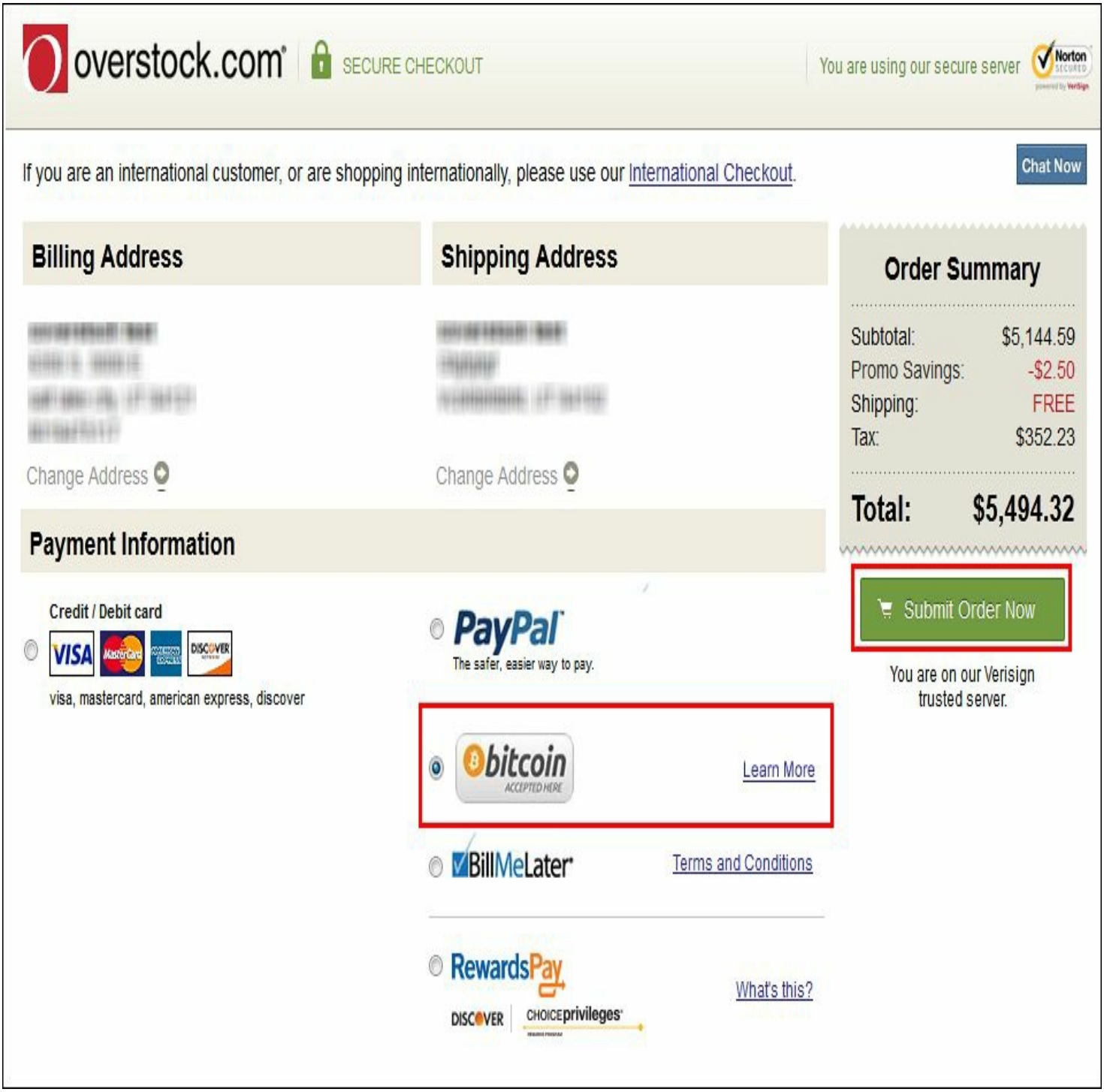
Veamos algunos ejemplos de comercios

que aceptan bitcoins como medio de pago. Overstock.com, es uno de los más populares, se trata de una compañía que vende a precio descontado una amplia variedad de artículos incluyendo mobiliario, electrónica, joyería, o ropa. Newegg.com es otra tienda de comercio electrónico que vende diferentes tipos de artículos, con un peso importante de informática y electrónica. Expedia.com la conocida web de viajes también admite bitcoins como medio de pago. Shopify stores shopify.com es una especie de centro comercial online, donde diversos comerciantes pueden vender sus productos, y también permite el pago en bitcoins. También hay muchos restaurantes que aceptan esta

forma de pago, incluyendo en algunos países cadenas tan populares como Subway y KFC.

Pago con bitcoins en Overstock

(Fuente: overtsock.com)



Transferencia internacional de dinero

Una de las ventajas más importantes de bitcoin es la transferencia de dinero entre personas independientemente del país en el que estén, en minutos, de manera anónima y con unos costes de transacción mínimos, frente a comisiones de hasta un 5-10% que otras empresas ofrecen para este servicio.

Sacar dinero en un cajero

En España ya hay decenas de cajeros bitcoin, que permiten tanto la retirada en euros de nuestra cartera de bitcoins como la compra de bitcoins con nuestros euros.

Pagos entre empresas

Una de las áreas en desarrollo, y que supone un importantísimo volumen de dinero es la posibilidad de realizar pagos entre empresas en bitcoins, independientemente de la localización, evitando comisiones e intermediarios.

Inversión

Uno de los principales usos reales de bitcoin actualmente es la inversión. Los bitcoins han experimentado una revalorización de más del ¡1.000%! en el último año, más que muchas otras

inversiones como fondos, acciones, o bonos. La inversión en bitcoin se considera de elevado riesgo, así que hay que ser muy cauteloso con este uso. Además, la volatilidad (es decir la variación del precio del bitcoin por ejemplo en un día) es muy elevada, pudiendo variar hasta un 10% en un día e incluso más.

Donar

También hay un número elevado de ONGs que aceptan bitcoins en donación, algunas tan conocidas como Save the Children.

Moneda refugio

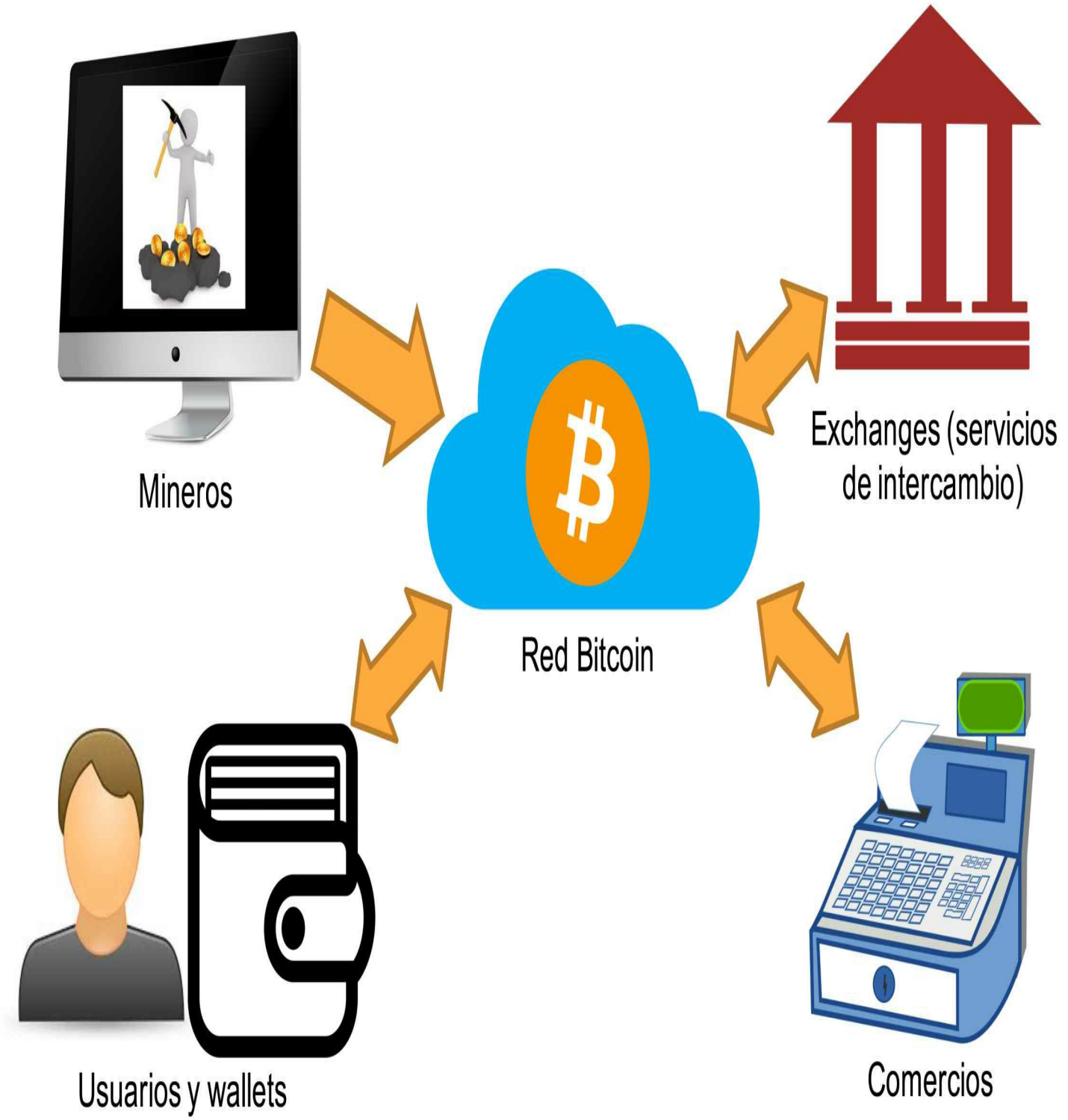
Los atractivos de bitcoin son aún mayores en un país en el que hay restricciones financieras impuestas por el gobierno (por ejemplo limitaciones en cambio de divisas, ya sea limitando la cantidad o interviniendo el tipo de cambio), situaciones inflacionarias, y también crisis políticas o militares. Hace unos años en Argentina el bitcoin se desarrolló tremendamente como moneda por las restricciones financieras impuestas por el gobierno. Más recientemente, la crisis de Corea del Norte ha ocasionado una gran compra de bitcoins por parte de japoneses y

coreanos del sur, teniendo en cuenta que una escalada militar ocasionaría una muy probable pérdida de valor del Yen y del Won.

3. El ecosistema bitcoin

El ecosistema Bitcoin está formado por distintos tipos de participantes que comparten entre sí la utilización del protocolo bitcoin.

El ecosistema Bitcoin


Mineros
Exchanges (servicios de intercambio)
Red Bitcoin
Usuarios y wallets
Comercios

Los mineros

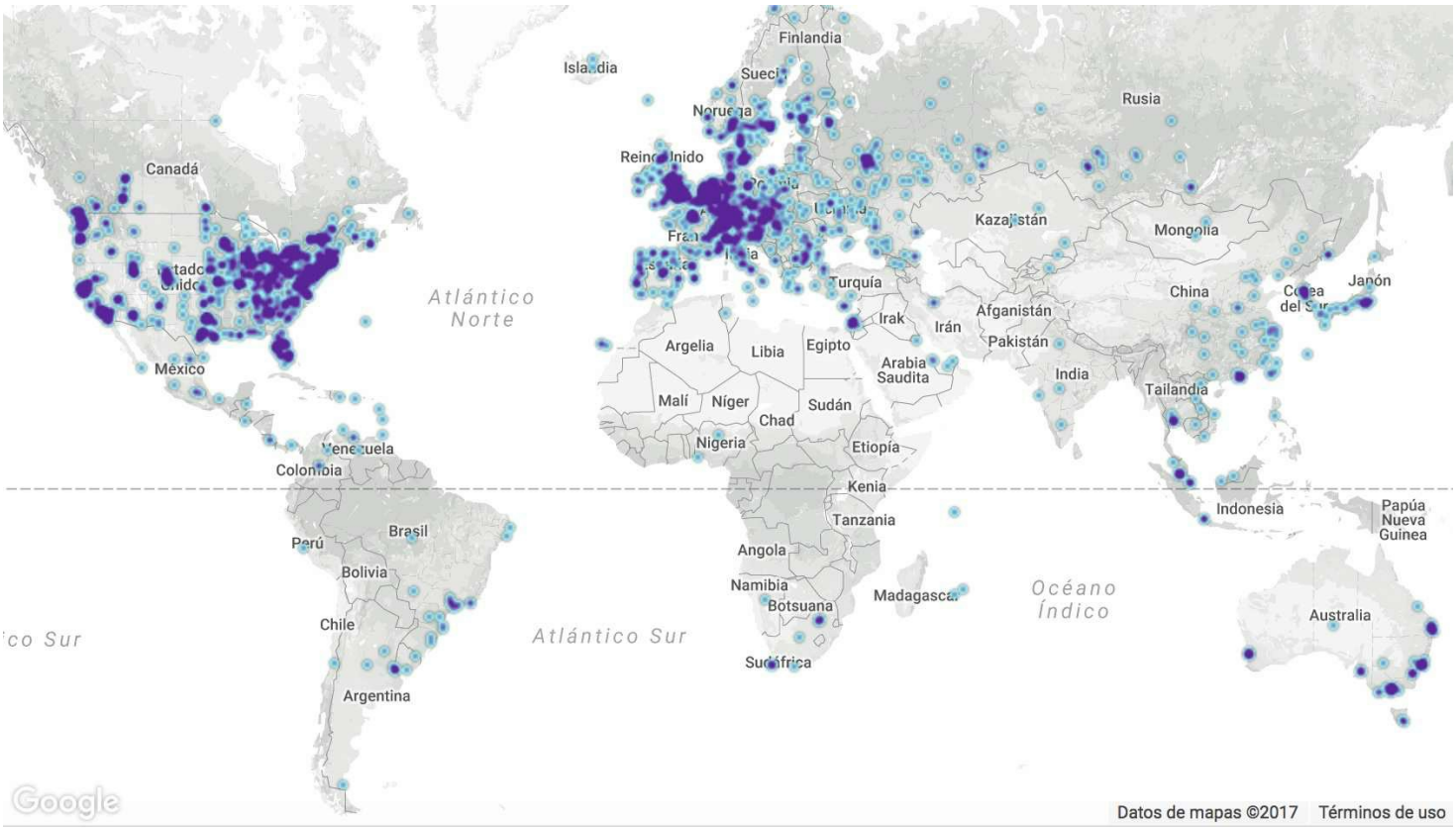
En primer lugar del ecosistema tenemos el origen de los bitcoins, y éste se sitúa en los mineros. No es sólo el origen de los bitcoins, en realidad los mineros constituyen el corazón de la red bitcoin, ya que **almacenan la cadena de bloques y procesan las nuevas transacciones en la red.** Un minero es un ordenador con un software específico instalado, que está conectado a la red bitcoin, que almacena la cadena de bloques (blockchain) sincronizada, y que trabaja resolviendo puzzles criptográficos para añadir nuevas transacciones a la cadena de bloques cada 10 minutos.

En este trabajo de resolución de puzzles

compite con todos los demás ordenadores de la red Bitcoin, y el ganador de esta competición que ocurre cada 10 minutos, reciben una compensación en forma de bitcoins. Esta compensación es, de hecho, la manera de generar nuevos bitcoins en el sistema, ya que el que gana cada competición además de escribir en la cadena de bloques las transacciones de esos 10 minutos, escribe una transacción en la que se auto-asigna una cantidad de bitcoins, actualmente 6 bitcoins.

Mapa de distribución global de nodos Bitcoin

(Fuente: Bitnodes https://bitnodes.earn.com/)



¿Qué tipo de ordenadores son mineros? Hay actualmente miles de ordenadores de este tipo, y en realidad se trata de una red tremendamente abierta. Tu propio ordenador podría ser un nodo bitcoin en unos minutos, sólo necesita un mínimo de potencia y espacio para almacenar la cadena de bloques, además de conexión a Internet. Bastaría con instalarle el

software y dejarlo funcionando.

Granja de equipos informáticos para minería de Bitcoin
(Fuente: Wikimedia Commons, Autor: Marco Krohn)

¿Y cómo verifica la red Bitcoin que tu ordenador es un participante bienintencionado en la red, que no

pretende cambiar ilícitamente la cadena de bloques? Lo interesante del protocolo Bitcoin es que implícitamente asume que habrá participantes bienintencionados y otros no tanto, y el protocolo está preparado para eso. No hay un proceso de verificación de los ordenadores o nodos que se incorporan a la red. Lo que hay es un protocolo de mayorías, de tal manera que cuando cada 10 minutos se escriben las nuevas transacciones en la cadena de bloques, sólo aquéllas que cuentan con un apoyo mayoritario, más del 50% de los ordenadores conectados a la red, pasan a ser incluidas en la cadena de bloques.

Esto significa que si un atacante

intentara añadir transacciones fraudulentas, o alterar la cadena de bloques entera, tendría que hacerse con el control miles de ordenadores de la red Bitcoin de todo el mundo para hacer que esas transacciones o esas modificaciones en la cadena de bloques fueran asumidas como las correctas, o bien incluir tantos ordenadores en la red bitcoin que asumiera más del 50% de la red con sus propios ordenadores. Estas dos posibilidades son prácticamente imposibles, es lo que se llama ataque del 51%, nunca ha ocurrido hasta ahora y parece prácticamente imposible que ocurra al continuar creciendo la red Bitcoin y mantenerse los máximos estándares de seguridad en la misma.

Los servicios de intercambio o exchanges

Los exchanges **facilitan el intercambio entre monedas convencionales (fiat) y bitcoins.** Lo hacen facilitando una plataforma electrónica de intercambio, que pone en comunicación a personas o instituciones interesadas en comprar bitcoins con otras interesadas en vender bitcoins.

Una plataforma recibe ofertas de compra de 1 bitcoin con, por ejemplo, por hasta 7.050 euros, y por otro lado recibe

ofertas de venta de bitcoins, por ejemplo 1 bitcoin por hasta 7.050 euros. Y se encarga de emparejar esas ofertas para que las transacciones tengan lugar. En este ejemplo el precio máximo al que el comprador quiere comprar y el mínimo al que el vendedor desea vender coinciden, por lo que la transacción irá adelante. El exchange recibe una comisión por esta compra-venta, que puede estar alrededor del 0,25% del importe.

Pantalla ilustrativa de trading
(Fuente: Pixabay)

Como puedes imaginar, un exchange maneja un volumen muy elevado de dinero y de transacciones, necesariamente son empresas con inversores significativos detrás, y la seguridad es fundamental ya que son objeto de ataques múltiples por parte de hackers que desean hacerse con los fondos. Es importante entender que las

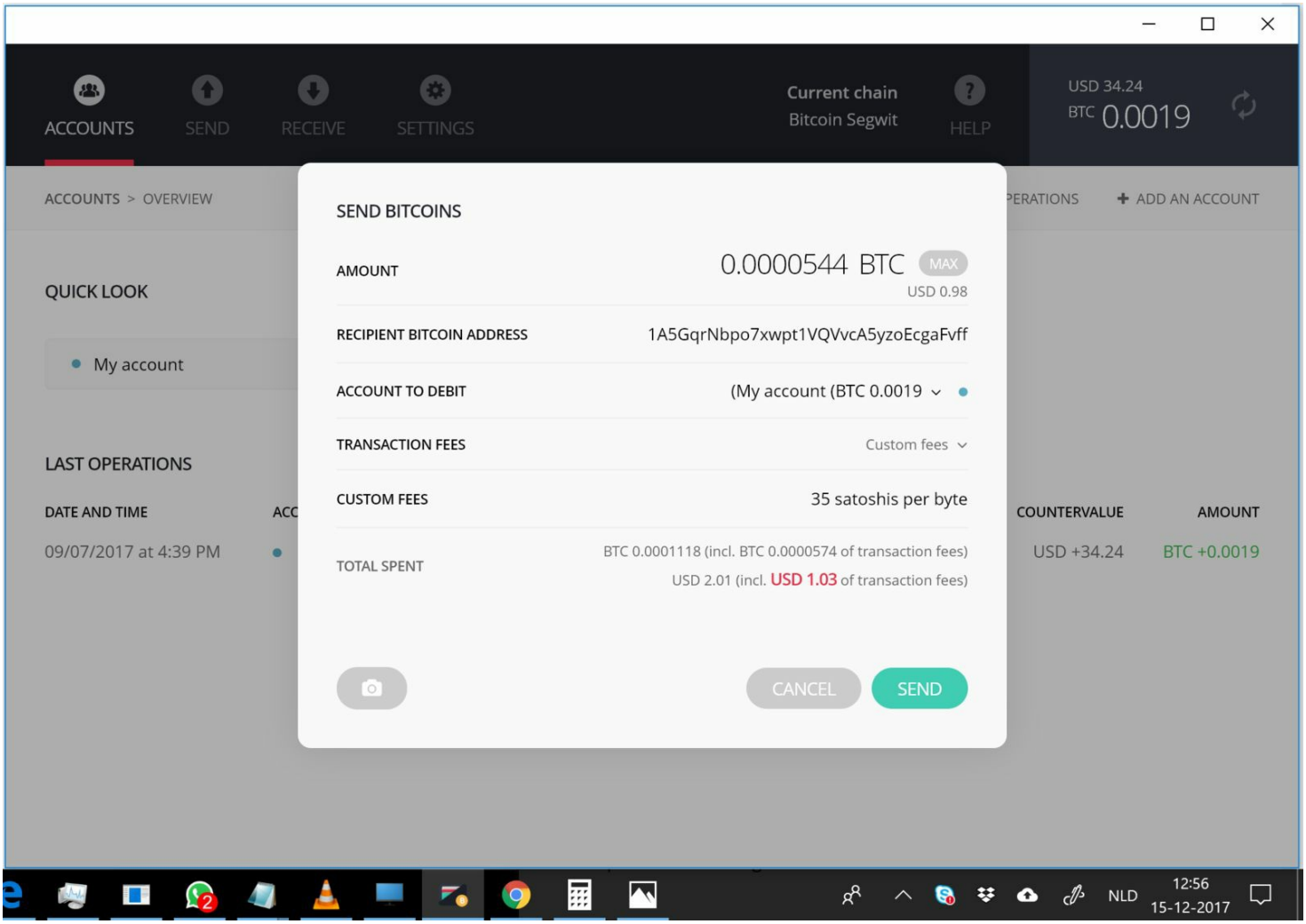
transacciones que ocurren en un exchange no se ven reflejadas en la red bitcoin como tales, sino únicamente en los sistemas informáticos del exchange, que maneja un conjunto muy grande de cuentas de bitcoin que organiza entre ellos.

Los servicios de cartera virtual (wallet)

La minería y los servicios de intercambio (exchanges) proporcionan dos maneras de obtener bitcoins. Una vez obtenidos es necesario **guardarlos, enviarlos y recibirlos de una manera**

segura. Esto es posible con una cartera de papel en la que anotamos de manera física la dirección de nuestra cuenta bitcoin, sin embargo la gran mayoría de usuarios decide utilizar un servicio de cartera que simplifica el almacenamiento, el envío y los pagos con bitcoins. Existen servicios que funcionan en la web, otros que son aplicaciones a instalar en un ordenador o dispositivo móvil, e incluso dispositivos físicos destinados a almacenar bitcoins.

Aplicación de cartera virtual para Bitcoin
(Fuente: Wikimedia Commons, Autor: FlippyFlink)



Los comerciantes

La utilidad de una moneda se relaciona en parte con las cosas que puedes comprar con ella. En este sentido

tenemos los comerciantes que **admiten bitcoins como forma de pago**. Pese al éxito en la adopción y revalorización de bitcoins, todavía hay un número reducido de comercios que admiten bitcoin como forma de pago. Sea estima que de los 500 principales comercios en Internet, únicamente 3 aceptan bitcoins. Esto tiene que ver con la poca utilización para compras por parte de usuarios, las complejidades tecnológicas que supone, y la gran variabilidad en el precio de la moneda, que supone riesgos y oportunidades.

Los procesadores de pagos

Muchos comerciantes tienen interés en aceptar bitcoins como forma de pago, y lo pueden hacer directamente a través de carteras virtuales con las que pueden recibir los pagos. Sin embargo, a menudo los comerciantes encuentran más sencillo y seguro utilizar un servicio de procesamiento de pagos profesional, al que pagan una pequeña comisión. Es un concepto similar a utilizar la red de Visa o MasterCard para aceptar pagos.

Una de las ventajas de estos servicios es el poder **convertir instantáneamente los pagos en bitcoin a la moneda fiat local** (euros en nuestro caso). Esto

puede ser importante, ya que en la mayoría de los casos los comerciantes tendrán que pagar abonar mercancías a sus proveedores y pagar sus gastos en moneda fiat, y una conversión directa a moneda fiat en el momento evita el riesgo de que el tipo de cambio baje y obtengan menos euros cuando vayan a cambiar la moneda. Otra ventaja de estos servicios es que proporcionan herramientas e informes para simplificar el aceptar el pago en bitcoins de manera más sencilla, como avisos cuando el pago se ha realizado, almacenamiento de recibos, y otros.

Los inversores y consumidores

Teniendo en cuenta la todavía limitada cantidad de comercios que admiten pagos en bitcoins, y la revalorización de bitcoin, actualmente la mayoría de **usuarios de bitcoin** piensan en esta moneda como forma de inversión que como moneda para realizar compras. Además todavía es muchas veces más incómodo realizar la compra en bitcoins que utilizar, por ejemplo, una tarjeta de crédito.

El protocolo bitcoin

El protocolo Bitcoin es el elemento

fundamental para el funcionamiento del bitcoin como moneda. En ausencia de autoridad regulatoria, el protocolo bitcoin es quien regula absolutamente todos los aspectos, desde la seguridad hasta la emisión de nueva moneda, desde el sistema de cuentas hasta el funcionamiento de la cadena de bloques. Los principales componentes del protocolo Bitcoins son:

La cadena de bloques (blockchain) y las transacciones

En última instancia un bitcoin es una cadena de firmas digitales. Desde que ese bitcoin se generó, cada propietario que ha habido ha firmado con su clave

privada cada transacción al siguiente propietario, de manera que cualquiera que reciba un pago con ese bitcoin puede trazar el registro de transacciones y verificar la propiedad actual. El problema principal a resolver es cómo asegurar que algún propietario no ha gastado dos veces ese bitcoin, y Bitcoin lo resuelve haciendo que toda la red tenga un registro público de todas las transacciones que han ocurrido, en la que llamamos cadena de bloques. Cada transacción se anuncia públicamente y todos los ordenadores en la red acuerdan por mayoría la transacción que llegó primero. Cualquier transacción posterior de ese mismo bitcoin ya "gastado" por su propietario no será

válida.

Proof-of-Work o Prueba-de-trabajo

Los ordenadores conectados a la red Bitcoin compiten cada ciclo de 10 minutos resolviendo un puzzle matemático muy complejo, cuya dificultad se va ajustando por el número y la potencia de ordenadores en la red. La resolución de este puzzle es lo que se denomina Proof-of-Work. El ordenador que gana escribe la primera transacción del nuevo bloque y se auto-adjudica un número de bitcoins determinado, suponiendo un incentivo para participar en la red Bitcoin. Este número de bitcoins asignado en cada transacción se

va dividiendo por dos cada cierto tiempo, de tal manera que supone una regulación del número de nuevos bitcoins emitidos y del número total que puede haber de bitcoins.

Funcionamiento de la red Bitcoin

Las transacciones nuevas se difunden por todos los ordenadores (nodos) de la red. Esta red es descentralizada, no hay una autoridad central, cualquier ordenador con el software de Bitcoin en ejecución se convierte en parte de esta red. Cada nodo recoge las transacciones nuevas en un bloque nuevo y trabaja en encontrar el "Proof-of-Wok" para su bloque. Cuando un nodo encuentra este

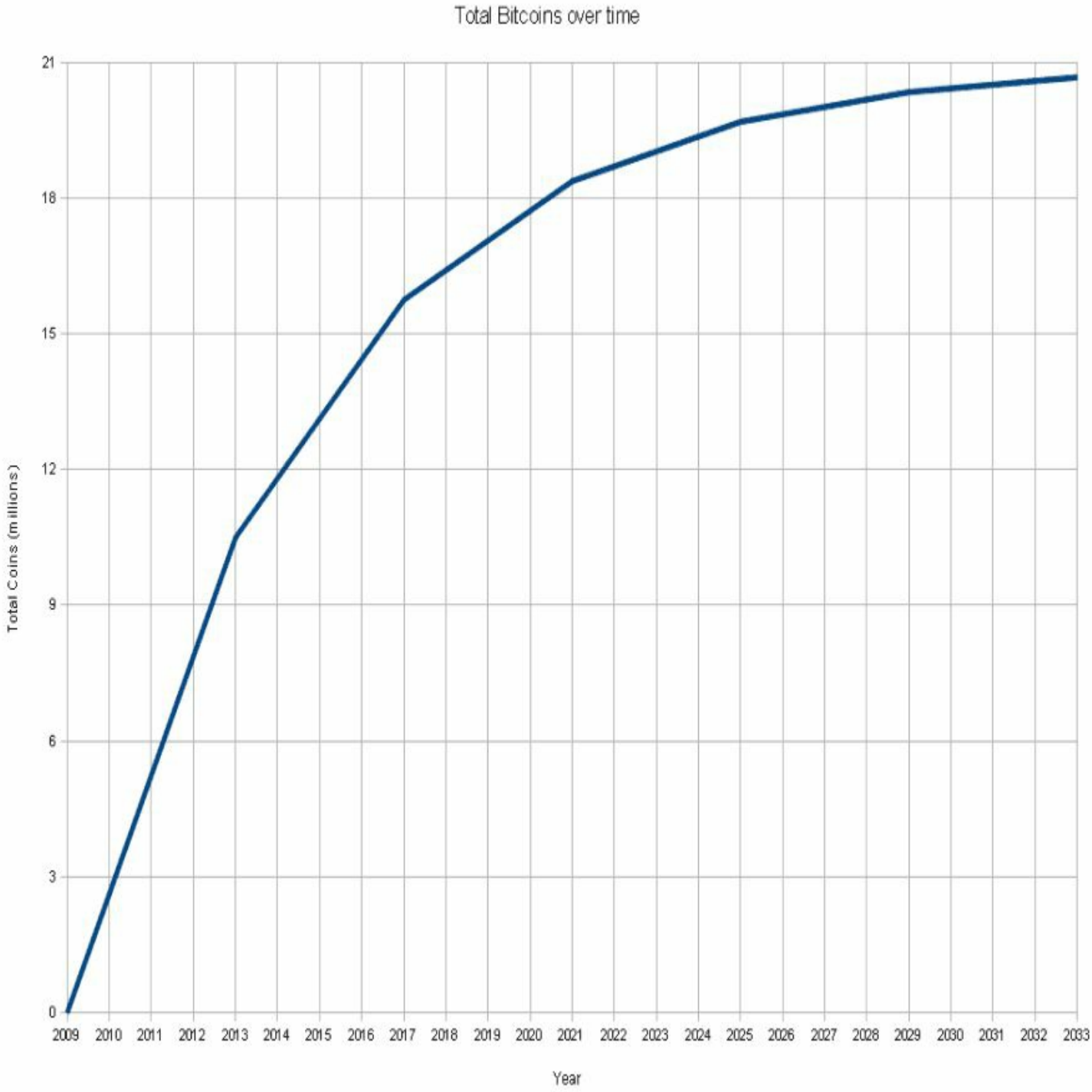
“Proof-of-Work” lo difunde a todos los nodos, y los nodos aceptan el bloque únicamente si todas las transacciones de ese bloque son válidas y no se han gastado ya ninguno de los bitcoins incluidos. Los nodos aceptan por mayoría el bloque y comienzan a crear el siguiente bloque de la cadena. Es importante tener en cuenta que los nodos siempre consideran la cadena más larga como la correcta y trabajan en extenderla con nuevos bloques.

Privacidad y claves

La clave privada es la que permite al propietario firmar una transacción en la que envía bitcoins a otra persona. Sólo

el propietario la conoce. La clave pública aparece reflejada en la cadena de bloques y por tanto todos los ordenadores la conocen, sin embargo esta clave es anónima, no recoge ninguna información del propietario, y por tanto es un elemento muy importante de la privacidad.

Evolución del número de bitcoins a lo largo del tiempo
(Fuente: Wikimedia Commons, Autor: Insti)



¿Qué es un fork?

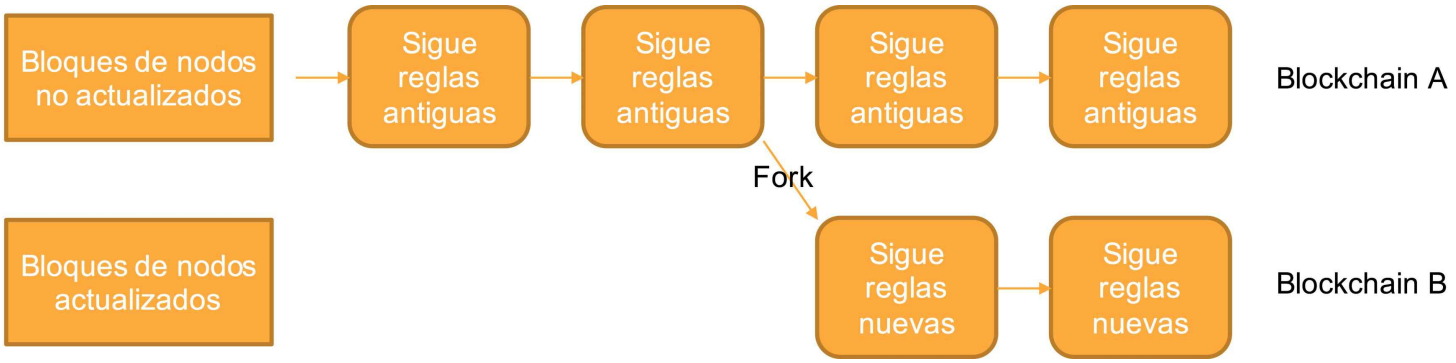
Un fork, que se podría traducir como bifurcación, es una **actualización del protocolo, o conjunto de reglas, por el que funciona bitcoin.** Sería un poco parecido a cuando actualizamos el sistema operativo de nuestro ordenador para conseguir nuevas funcionalidades. Como sabemos, un requerimiento del protocolo bitcoin es la sincronización de la información de acuerdo a unos tiempos y parámetros muy definidos, en toda la red bitcoin, por lo que es crítico que las reglas sean las mismas en todos los ordenadores de la red (nodos).

¿Para qué sirve un fork? Bitcoin es un protocolo que ha demostrado su gran

seguridad y robustez a lo largo de varios años. Sin embargo también se han mostrado algunas carencias en sus funcionalidades, y es esto lo que pretende mejorarse con los forks. Por ejemplo, al crecer el número de usuarios y multiplicarse el número de transacciones, se está poniendo de manifiesto que el protocolo llega a un estado de saturación, hay más transacciones que procesar que la capacidad que soporta el protocolo. Lógicamente esto sólo puede empeorar al aumentar la utilización de bitcoin y el número de posibles usos. En este sentido, una de las principales mejoras, llamada SegWit, permite aumentar el número de transacciones que se pueden

procesar.

División de la cadena de bloques (blockchain) en un hard fork



Hay dos tipos de forks. Por un lado un **soft fork o bifurcación suave**, es un cambio de reglas, y por tanto del código informático que regula su operativa, que es compatible hacia atrás, es decir, el nuevo protocolo que surge del fork funciona de manera compatible con la versión previa del protocolo. Un soft

fork origina una divergencia o separación temporal en la cadena de bloques, cuando algunos nodos de se actualizan y otros no en el momento en el que la actualización ocurre. De hecho, como funciona es que en cuanto se produce un soft fork, muchos de los nodos bitcoin se empiezan a actualizar a la nueva versión. Si la mayoría de los nodos se actualizan, el soft fork vence, y la nueva cadena, apoyada por la mayoría de los nodos, seguirá las nuevas reglas. Si únicamente una minoría actualiza, el soft fork falla y la cadena de bloques previa continúa. Para los nodos que se actualizan tarde no es problema, pueden volver a copiarse la cadena de bloques mayoritaria y continuar funcionando con

normalidad.

El **hard fork o bifurcación dura** es una disrupción de la cadena de bloques en la que los nodos que no se actualizan no pueden trabajar con la cadena de bloques actualizada, y no hay por tanto compatibilidad con la versión previa. La ventaja del hard fork es que permite un cambio importante en el protocolo de operación de bitcoin de manera más rápida. Un hard fork ocasiona una divergencia o separación permanente en la cadena de bloques, ya no hay compatibilidad con la previa. En este caso la cadena de bloques previa y la nueva siguen avanzando en paralelo, pero cada una sigue un conjunto

diferente de reglas, no compatibles. Los usuarios no pueden enviar bitcoins de una cadena a otra.

Cuando ocurre un hard fork, todos los usuarios que poseían bitcoins en la cadena de bloques anterior al fork, ahora tienen las monedas de las dos cadenas de bloques resultantes de la disrupción. Si, por ejemplo, tenías 3 bitcoins antes del fork, pasas a tener 3 bitcoins en la nueva cadena de bloques y otros 3 bitcoins en la previa, ya que toda la información previa al fork está ahora en dos cadenas de bloques. Esto ha ocurrido recientemente con la aparición de Bitcoin Cash (Agosto 2017) y Bitcoin Gold (Octubre 2017). Todas las

personas que poseían un número de bitcoins en la blockchain, ahora siguen teniendo el mismo número de bitcoins en la cadena bitcoin, y además el mismo número de bitcoins cash y bitcoin gold en las nuevas cadenas de bloques de bitcoin cash y gold. Evidentemente no vale lo mismo cada bitcoin (actualmente a alrededor de 7.000 euros) que cada bitcoin cash (alrededor de 1.000 euros) o bitcoin gold (actualmente alrededor de 200 euros).

Hay algunas **medidas que debes de tomar antes, durante y después de un fork**. Lo primero es asegurarte de que 1-2 días antes tienes todos tus bitcoins en una cartera tuya, en la que controlas las

claves privadas. De esta manera aseguras que en la cadena que se va a bifurcar estarán tus bitcoins, e identificados con tus claves y, por tanto cuando la cadena se bifurque tus bitcoins estarán en las dos cadenas bifurcadas. Si tus bitcoins están, por ejemplo en tu cuenta en un exchange, puede haber problemas si hubiera alguna incidencia o bien el exchange podría no darte tus correspondientes bitcoins en una de las cadenas resultantes de la bifurcación. Además estos servicios de intercambio suelen interrumpir los depósitos y retiradas de fondos alrededor de un fork, y también pueden interrumpir el trading. Por otro lado debes de evitar cualquier tipo de

transacción con bitcoins entre 1 día antes y 1-2 días después del fork, ya que se trata de un momento particularmente vulnerable a errores e incluso ataques maliciosos al traspasarse mucha información en un proceso muy complejo. Después del fork continuarás teniendo tus bitcoins en la cadena principal, como al principio, sin embargo deberás de reclamar con tus claves privadas los bitcoins de la nueva cadena. Dependiendo del tipo de cartera que utilices, las instrucciones de cómo realizar esto diferirán, pero en general es un proceso sencillo, si bien normalmente deberás esperar algunas semanas hasta que la cartera que utilizas implante la nueva moneda bifurcada.

Muchos usuarios gustan de ver de repente sus bitcoins duplicados y tener así nueva moneda, sin embargo cada ramificación de la cadena de bloques resta fortaleza a la original, y origina dudas sobre la robustez del concepto. Si esto ocurriera de manera continua, podríamos acabar con demasiados hijos, nietos y sobrinos de bitcoin, y esto creo que no sería bueno para nadie. Un hard fork sólo debería de ocurrir cuando sea absolutamente necesario y con un apoyo muy mayoritario de usuarios y nodos. Sería algo aplicable a situaciones en la que hubiera funcionalidades críticas o temas de seguridad que requieren una medida tan drástica.

4. Cómo conseguir bitcoins

Ya sé que es un bitcoin, para qué lo puedo utilizar y conozco el ecosistema general de bitcoin, y llegó el momento de la verdad. ¿Cómo consigo bitcoins? Hay fundamentalmente cuatro maneras de conseguir bitcoins:

1. Minarlos a través de ordenadores que resuelven estas funciones matemáticas tan complejas
2. Comprarlos en una plataforma electrónica de intercambio (los famosos exchanges)

3. Comprarlos a un particular directamente
4. Comprarlos en un cajero automático de bitcoins

Vamos a ir revisando cada una de estas formas.

Minando los bitcoins

Hemos comentado como en un sistema monetario tradicional, el banco central (por ejemplo el Banco Central Europeo) decide una política monetaria y en función de eso crea la moneda (por

ejemplo euros) a un mayor o menor ritmo. En el caso de bitcoins el proceso de creación está regulado por unas leyes matemáticas y un proceso transparente.

Cada 10 minutos empieza un "torneo" en el que miles de ordenadores de todo el mundo, que juntos constituyen la red informática global más potente, compiten resolviendo un mismo problema matemático. Este problema sólo puede resolverse probando cientos o miles de millones de números al azar hasta dar con el resultado correcto. Este puzzle matemático resulta en la verificación de la blockchain, y por tanto la validación de las transacciones que se incluyen en ella. El primer

ordenador que consiga resolverlo se lleva la recompensa, en forma de nuevos bitcoins que son creados por el sistema. Esta recompensa actualmente es de 6 bitcoins por ciclo, que a un precio de unos 8.000 euros, supone 48.000 euros de premio potencial en esos 10 minutos, o un premio diario total de 6,9 millones de euros, equivalente a un premio total anual de ¡2.500 millones de euros! Este premio acaba siendo distribuido entre muchísimos equipos diferentes, pero está claro que si eres capaz de competir con un buen equipo y un coste bajo de electricidad, merece la pena participar.

Cualquier **ordenador** puede participar en este "torneo", instalando un programa

especial. Sin embargo la minería genera importantes rendimientos económicos, y esto ha hecho que muchas empresas se hayan especializado en ello, montando auténticas granjas de ordenadores tremendamente potentes y especializados en minería de bitcoins. Además debido al intensísimo trabajo que realizan, estos ordenadores tienen un consumo energético muy elevado, por lo que estas granjas de ordenadores se suelen ubicar en zonas donde el precio de la electricidad es muy bajo (por ejemplo en la cercanía de centrales eléctricas). Estos es lo que se conoce como Proof-of-Work, que podríamos traducir como prueba de trabajo, que significa que la creación de un nuevo

bitcoin ha requerido una actividad (el minado) que implica un consumo de recursos (equipos informáticos, electricidad).

Equipo de minería de Bitcoin
(Fuente: Wikimedia Commons, Autor: Youwei-han)

Imaginemos que quiero minar bitcoins. **¿Dónde empiezo?** En primer lugar puedes usar tu ordenador de casa, instalar este programa y comenzar a minar. El problema es que el rendimiento que vas a obtener es muy muy bajo compitiendo contra tantos gigantes, y además los requerimientos de potencia que vas a hacer a tu ordenador son tantos y tan continuados que pueden llegar a dañar al propio ordenador. Por otro lado el consumo de electricidad va a resultar muy elevado. El siguiente escalón sería comprar un equipo especializado de minería de bitcoins, que requiere una inversión de alrededor de 500-5.000 euros. Son equipos con forma tipo caja de zapatos grande,

ruidosos y poco atractivos, generan bastante calor y únicamente sirven para minar bitcoins. Además el consumo eléctrico es el de una estufa (unos 500-1.500 watios), por lo que tu factura eléctrica teniéndolos enchufados 24 horas al día constantemente, se va a disparar. Si te interesa aún así, mira algunas marcas como AntMiner.

Otra opción es incluir tu, probablemente modesto equipo, dentro de un **pool de minería**. En este caso tu equipo pasa a formar parte de una red mucho más potente que aprovecha mucho mejor los recursos conjuntos (por ejemplo, no probando los mismos números en varios equipos) y que distribuye luego los

bitcoins obtenidos entre los integrantes en proporción a la capacidad de cálculo que han aportado.

Hay una opción adicional que es el **cloud mining**. En este caso, hay empresas que instalan granjas de ordenadores, y puedes participar simplemente pagando una cantidad de dinero (por ejemplo mensual) para "alquilar" cierta capacidad de procesamiento para generar bitcoins. La empresa te da los bitcoins que ha generado el procesamiento que has contratado.

¿Y todo esto merece la pena? En España tengo muchas dudas. Por un lado el

elevado coste de la electricidad hace menos rentable utilizar un equipo para minería de bitcoins. Por otro lado, el cloud mining puede ser una opción pero no tengo claro que tenga mejor rentabilidad que, por ejemplo, la inversión directa en bitcoins esperando a su revalorización. Además, ha habido casos de timos basados en servicios de cloud mining.

Comprando bitcoins en una plataforma electrónica de intercambio (exchange)

La **manera más sencilla, accesible,**

rápida y segura de conseguir tus bitcoins es a través de plataformas electrónicas de intercambio (o "trading") de criptomonedas, los llamados "exchanges". Aquí puedes comprar y vender tus bitcoins u otras monedas virtuales, y el pago lo puedes realizar habitualmente a través de una transferencia a tu cuenta personal en un "exchange" o bien a través de tarjeta de crédito o incluso PayPal. También puedes almacenar en ellos tu moneda habitual (euros), aunque sólo tiene sentido temporalmente en espera de adquirir bitcoins.

¿Qué exchange utilizar? Es muy importante un exchange seguro y

consolidado, que ofrezca la garantía de llevar tiempo operando. Además debe de permitir operar en euros. Por otro lado debe de ser un exchange con un volumen de operación elevado para asegurar que no habrá problemas en la liquidez de tus bitcoins depositados y que los precios de compra son acordes con mercado. Algunos exchanges que cumplen estos requerimientos son Kraken (EE.UU.), Coinbase (EE.UU.), CEX.IO (Reino Unido), GDAX (EE.UU.), BitStamp (Luxemburgo). Todos los exchanges permiten operar en bitcoins. Por otro lado, hay cientos de criptomonedas disponibles que no son bitcoins (las llamadas altcoins), y cada exchange sólo permite operar en algunas

de ellas. En el caso de que quieras operar en otras criptomonedas que no puedas encontrar en estos exchanges, y si estos exchanges no operan en euros, tienes la opción fácil de comprar tus bitcoins en uno de estos, y transferirlos como bitcoins a casi cualquier otro exchange en el que puedas cambiar tus bitcoins por otras criptomonedas. Otros exchanges interesantes por variedad de criptomonedas son Bitfinex (Hong Kong), Poloniex (EE.UU), o Bittrex (EE.UU.).

Listado de principales exchanges de Bitcoin por volumen de operación en 6 meses

(Fuente: Bitcoiny

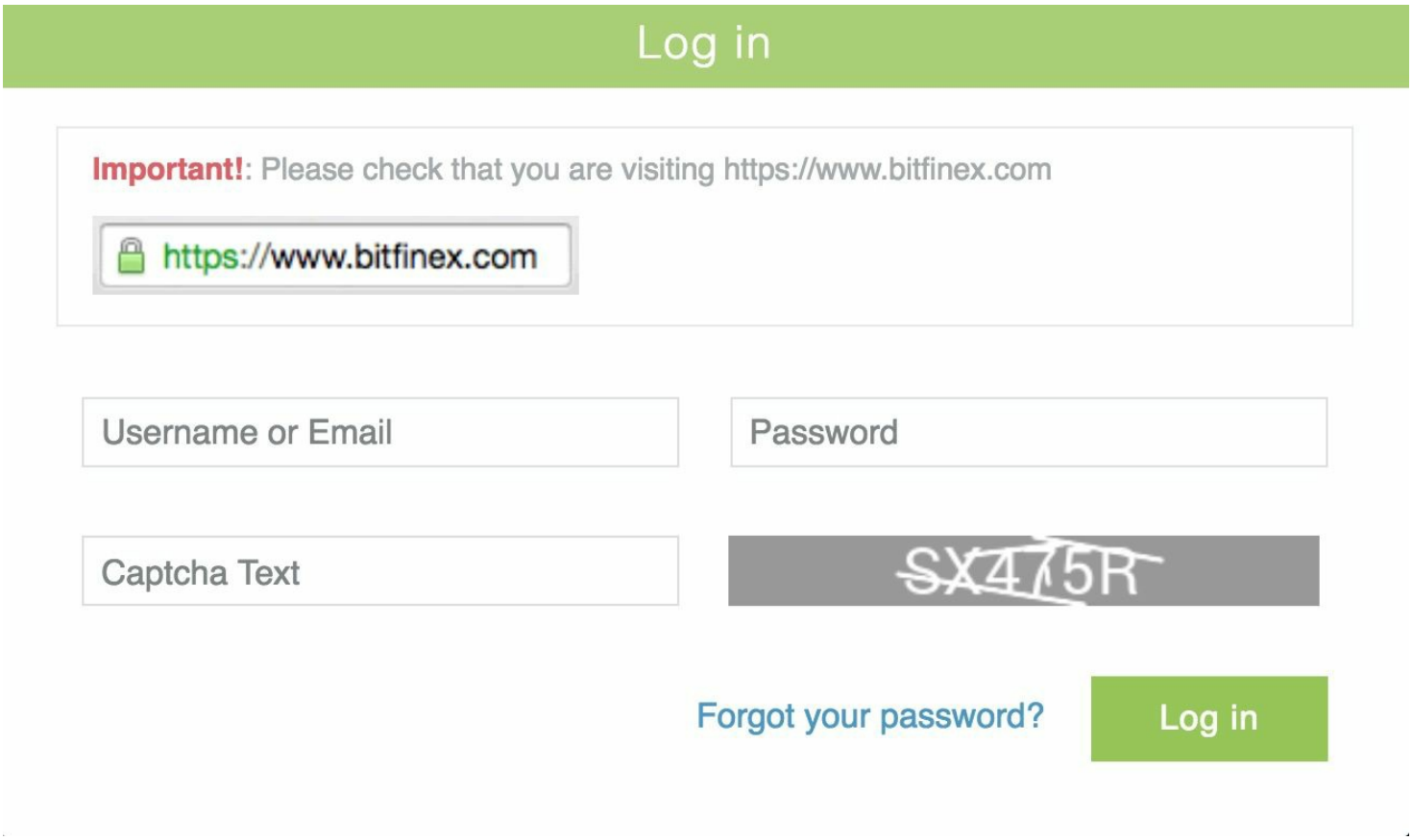
https://data.bitcoinity.org)

Exchange	Volume [BTC]	Market share ▾
bitfinex	9.03M	28.89%
coinbase	4.03M	12.91%
bitflyer	3.50M	11.21%
bitstamp	3.28M	10.49%
others	3.08M	9.84%
kraken	2.85M	9.11%
gemini	1.87M	5.99%
okcoin	1.69M	5.40%
btcchina	1.15M	3.68%
bit-x	777k	2.49%

El primer paso es **crear una cuenta** en el exchange que elijas, se trata de un proceso que puede realizarse en 5 minutos con tu nombre, correo electrónico, y contraseña. Como en otros servicios de internet confirmas recibiendo un email en tu cuenta de correo sobre el que tienes que hacer click. Es muy importante que elijas una contraseña muy segura, evitando contraseñas fáciles de adivinar (una palabra o secuencia de números fácil), y estableciendo combinaciones largas de letras, números y símbolos. Ten en cuenta que cualquier persona que pueda adivinar tu contraseña podrá disponer ilegalmente de tus fondos depositados en

el exchange.

Pantalla de acceso al servicio de intercambio Bitfinex
(Fuente: Bitfinex https://www.bitfinex.com/)



Hasta aquí muy sencillo, sin embargo una cuenta básica no te permite operar, sino que es necesario pasar por un

proceso de verificación e identificación que es semejante en los diferentes exchanges. Normalmente un primer paso requiere nombre y apellidos, país y dirección. Esto suele permitir un primer nivel de operativa con un límite de alrededor de 3.000 euros. Un segundo nivel de verificación permite elevar este nivel hasta alrededor de los 30.000-50.000 euros, y requiere que escanees tu DNI o pasaporte y una foto tuya sosteniendo ese DNI o pasaporte. Este paso suele tardar unos días ya que el exchange tiene que validar estas fotos y suele ser un proceso manual. Además hay un tercer nivel de verificación para instituciones o personas que quieran operar con un

volumen aún mayor.

Niveles de verificación en el servicio de intercambio Kraken

(Fuente: Kraken https://www.kraken.com/)

Get Verified

Kraken requires additional user information before any deposits or withdrawals can be made in order to meet KYC/AML legal requirements. There are multiple tier levels of funding limits, each with increasing amounts of deposit/withdraw limits.

	Daily limits	Monthly limits	Margin	Requirements	Verify Status
Tier 0 Deposits and withdrawals are not available.	Deposit (fiat) ..... $0.00 Deposit (crypto) ..... $0.00 Withdraw (fiat) ..... $0.00 Withdraw (crypto) $0.00	Deposit (fiat) ..... $0.00 Deposit (crypto) ..... $0.00 Withdraw (fiat) ..... $0.00 Withdraw (crypto) $0.00		Account signup	✔ Verified
Tier 1 You can trade between all currencies, but account funding is limited to digital currencies only.	Deposit (fiat) ..... $0.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $0.00 Withdraw (crypto) $2,500.00	Deposit (fiat) ..... $0.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $0.00 Withdraw (crypto) $20,000.00		• Full name • Date of birth • Country of residence • Phone number	Processing
Tier 2*	Deposit (fiat) ..... $2,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $2,000.00 Withdraw (crypto) $5,000.00	Deposit (fiat) ..... $10,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $10,000.00 Withdraw (crypto) $50,000.00		• All of the above • Address verification	Processing
Tier 3	Deposit (fiat) ..... $25,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $25,000.00 Withdraw (crypto) $50,000.00	Deposit (fiat) ..... $200,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $200,000.00 Withdraw (crypto) $200,000.00	Enabled	• All of the above • Government issued ID • Verified proof of residence (e.g., utility bill no	Not submitted

El siguiente paso es **depositar tus euros en el exchange.** Para ello el proceso más habitual es realizar una transferencia desde tu cuenta bancaria.

Entrando en la opción de depósitos, el exchange te indica el número de cuenta al que realizar la transferencia, debería de ser una cuenta dentro del sistema SEPA para agilizar y simplificar la transferencia desde España. Además en el campo de comentarios de la transferencia debes de indicar cierta información incluyendo tu código de usuario en el exchange. Esta transferencia la puedes realizar habitualmente desde tu banco a través de banca online. Al cabo de pocos días tendrás tus euros depositados en el exchange y podrás comenzar el trading. Otras opciones es depositar tus euros a través de una tarjeta de crédito, introduciendo los datos como en otras

compras de comercio electrónico. También puedes utilizar PayPal en algunos exchanges, de manera similar a como realizas otras compras por ese medio.

Llegamos ahora al momento en el que puedes, por fin, **comprar tu primer bitcoin.** Para ello entras en el apartado de trading y selecciona el par que te interese, en este caso el par bitcoin (abreviado BTC) / Euro. Ahí podrás ver la evolución del precio actual, la evolución del precio en el periodo que selecciones (última hora, 12 horas, 24 horas, 1 semana, 1 mes, 3 meses…) el precio máximo y mínimo, y el volumen de operativa, además de otra

información de interés dependiente de cada exchange.

Veamos ahora **cómo funciona un exchange** en realidad. El exchange no vende ni compra bitcoins, sino que conecta a compradores y vendedores. Supongamos en un instante de tiempo, tres vendedores quieren vender bitcoins, el primero está dispuesto a vender 1 bitcoin a 8.200 euros como mínimo, el segundo está dispuesto a vender 3 bitcoins a 8.400 euros o más, y el tercero está dispuesto a vender 2 bitcoin a 8.600 euros o más. Además hay tres compradores, el primero quiere comprar 1 bitcoin a no más de 8.500 euros. Un segundo quiere comprar 2 bitcoins pero

no a más de 8.400 euros. Un tercer comprador quiere comprar 2 bitcoins al mejor precio que haya en ese momento en el mercado. El sistema del exchange coloca las órdenes de esta manera:

Vender		Comprar	
1 BTC	8.200	1 BTC	8.500
3 BTC	8.400	2 BTC	8.400
2 BTC	8.600	2 BTC	Mercado

En este caso la primera orden de compra y de venta se ejecuta, comprándose 1 bitcoin a 8.200 euros. La segunda orden de compra de 2 bitcoins se ejecuta a 8.400 euros, y la tercera orden de compra de 2 bitcoins se ejecuta, comprando 1 bitcoin a 8.400 euros

(quedaba 1 bitcoin a ese precio) y otro bitcoin a 8.600 euros.

A continuación hay que generar una orden nueva de compra de bitcoins. En ese caso hay que indicar cuántos bitcoins quieres comprar, te calcula un estimado en euros de cuánto supone. Además hay que indicar el tipo de orden.

Principales tipos de órdenes

Tipo de orden	**Mercado**	**Límite**
Definición	Compra/venta al mejor precio	Compra/ven al precio especificad

	disponible	o mejor
Control del precio	Ninguno	Completo

Mercado

Una orden a mercado se ejecutará **de inmediato al precio de mercado en ese momento.** Por ejemplo, supongamos que es 14 de marzo a las 14:00. Si el precio del bitcoin está a 8.750 euros en el momento de ejecución de la orden, y compras 1 bitcoin, el coste en euros será esos 8.750 euros. El precio del mercado fluctúa constantemente, a veces de

manera brusca, por lo que aunque veas a qué precio está, ese precio puede variar justo cuando tu orden está en ejecución. Por esta razón suele aconsejarse utilizar órdenes a mercado con precaución e inclinarse más por órdenes con límite. Una orden de mercado no puede ser cancelada ya que se ejecuta inmediatamente, si bien por supuesto puedes elegir vender tus bitcoins inmediatamente después de su ejecución. En ocasiones una orden a mercado será completada parcialmente a varios precios, por ejemplo, supongamos que el precio está a 8.750 euros, pero al ejecutarse el volumen no es suficiente para cubrir toda la cantidad, podría ocurrir que, por ejemplo, compraras

medio bitcoin a 8.750 euros y otro medio a 8.800 euros. Una orden de venta a mercado funciona de la misma manera. Supongamos que el 14 de junio tu bitcoin vale 9.300 euros y quieres venderlo, en ese momento generas una nueva orden de venta de 1 bitcoin a mercado. Esta orden se ejecutará al precio del momento justo de la ejecución.

Límite

Es una orden para **comprar a un precio menor o igual que el límite indicado o bien vender a no menos del límite especificado**, por tanto implica que la orden se ejecutará sólo cuando se

alcance el límite indicado o mejor. Supongamos que, nuevamente el precio del bitcoin es de 8.750 euros. Viendo la tendencia y la volatilidad, crees que el bitcoin en algún momento va a bajar y quieres aprovechar ese momento para comprar un poco más barato. Podrías establecer una orden con límite de 8.600 euros el 14 de marzo a las 14:00, y se puede definir hasta cuando está vigente la orden, digamos que estableces hasta el 21 de marzo de las 14:00. Si, digamos, el 16 de marzo el bitcoin ha bajado hasta los 8.600 euros, la orden se ejecutará. La ventaja de las órdenes a límite es, precisamente, que puedes pagar menos por tu bitcoin en base a la volatilidad que tiene su precio,

aprovechando una bajada de precio en un momento determinado, y sin tener que estar pendiente de seguir la cotización constantemente. Si el precio del bitcoin hasta el 21 de marzo nunca baja hasta 8.600 euros, la orden nunca se ejecutará. Es posible dejar abierta la orden indefinidamente, y una orden a límite se puede cancelar en cualquier momento antes de su ejecución. Normalmente puedes ver las órdenes abiertas, pendientes de ejecución, en la sección de órdenes abiertas.

Stop

Una orden de stop **especifica un precio al que una orden será ejecutada, y en**

ese momento se ejecuta como una orden de mercado. Se utiliza en estrategias con stop loss, es decir, en las que quiero vender mis bitcoins si caen por debajo de un cierto precio. Veamos un ejemplo. Supongamos que has comprado un bitcoin a 8.600 euros. Supongamos que 3 meses después el precio del bitcoin ha llegado a a 9.300 euros. Piensas que esa inversión ya te ha dado una buena rentabilidad y aunque estás abierto a aumentar esta rentabilidad, quieres asegurar que proteges la mayoría del valor que tienes ahora. Entonces estableces una orden de venta stop loss a 9.100 euros. Si tu bitcoin sigue subiendo, no se ejecutará la orden. Sin embargo, en el momento en

el que el precio caiga a 9.100 euros o por debajo, la orden se ejecutará al precio de mercado. Esto quiere decir que si ha caído por debajo de 9.100 euros, pero la tendencia en ese momento es más bajista y al cruzarse con las órdenes compradoras el precio es de 9.090 euros, será ése el precio al que se ejecute en realidad

En cuanto a las comisiones, los exchanges se llevan una comisión por cada operación, en función de la cantidad y a veces del momento. Esta comisión viene a estar en el entorno del 0,25% de la cantidad comprada o vendida.

Las transacciones en un exchange se realizan instantáneamente. La razón de esto es que en realidad estas transacciones no se reflejan en la red bitcoin y no necesitan ser confirmadas por ésta, sino que se realizan en el sistema local del exchange. Por tanto no requiere esperar los 10-60 minutos de confirmaciones por la red bitcoin de la transacción, pero por otro lado esos bitcoins aparecen en una cuenta del exchange en la red bitcoin, no en una cuenta bitcoin nuestra en esta red. Cuando se ejecuta la orden, los bitcoins depositados aparecen como nuestros en la plataforma del exchange, como un apunte en nuestra cuenta. Sin embargo las características principales de los

bitcoins per se, la clave privada sobre todo, no son nuestros. A diferencia de los bancos, los exchanges no tienen o tienen muy limitado un seguro que proteja al cliente si el exchange deja de operar o es robado por hackers. Algunos exchanges grandes han compensado las pérdidas de clientes por un robo, pero no tienen obligación legal. Por eso es importante elegir exchanges grandes y con una trayectoria consolidada. Para hacer esos bitcoins más “nuestros” debemos de transferirlos a una cartera de bitcoins.

Comprando bitcoins a un particular directamente

Sabemos que una de las ventajas de los bitcoins es la descentralización y la independencia de entidades financieras. Por tanto podemos comprar bitcoins directamente a otro particular sin pasar por un exchange. Esto ofrece las ventajas a priori de menores comisiones y mayor anonimidad. Digo a priori porque todo dependerá del precio de compra que suele estar algo más elevado por parte del vendedor, y mientras que en un exchange con un volumen de operación elevado el precio de compra es un reflejo del precio de mercado, en el caso de particular a particular habrá que ver si el precio refleja la realidad del mercado. Hay

distintas modalidades.

Servicios para encontrar compradores y vendedores particulares

Algunos ejemplos son **Local Bitcoins, BitQuick o Bitcoin-OTC**Se parece un poco a algo tipo eBay. Indicas cuántos bitcoins quieres comprar y te aparecen los usuarios que quieren vender, a qué precio, y qué medio de pago admiten, que incluyen en metálico, transferencia, PayPal, entre otros. Las operaciones se pueden realizar totalmente online (la mayoría) o como operaciones locales que pueden realizarse cara a cara en Local Bitcoins. Al ser transacciones entre particulares directamente, hay un

riesgo de estafa, que ese reduce al habilitar un servicio de depósito en garantía. Esto significa que al acordarse una operación, los bitcoins que se transfieren se bloquean en un depósito en la cartera del servicio web del vendedor. Por tanto si el pago se ha realizado pero el vendedor no ha transferido los bitcoins al comprador, pueden reclamarse los bitcoins del depósito.

En el caso de este servicio las transacciones de una cartera del servicio web a otra son instantáneas (al no requerir confirmaciones por la red bitcoin), si bien aquí debemos hacer consideraciones similares a las de los

exchanges, si algo pasa con la empresa no tenemos protección. Es más adecuado que la transacción transfiera esos bitcoins a nuestra cartera personal (no la de la web), y en ese caso sí pasa por la red bitcoin y requiere varias confirmaciones por lo que el tiempo para que se procese suele ser de 10 a 60 minutos, a veces más (hasta algunas horas) si hay congestión en la red bitcoin. Como hemos comentado anteriormente, no debemos de mantener una cantidad importante en moneda nacional o bitcoins en el servicio web ya que podría cerrar y que no pudiéramos recuperar la cantidad. Bitcoin-OTC es un canal IRC, no una web. Por tanto requiere instalar un

cliente IRC en nuestro ordenador, y seguir las instrucciones que aparecen en la web https://bitcoin-otc.com/

Pantalla de compra/venta rápida de LocalBitcoins

(Fuente: LocalBitcoins.com)

Comprar bitcoins en persona

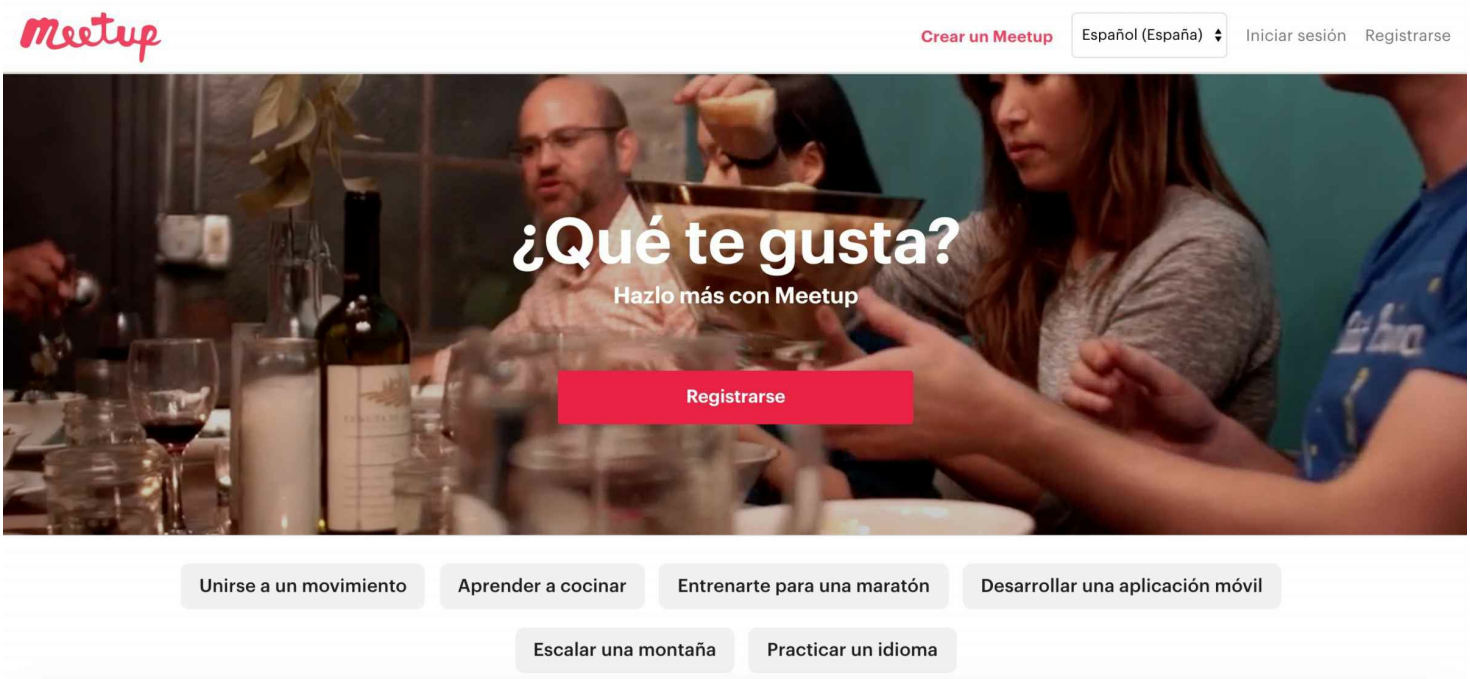
Ofrece una serie de ventajas. Una de las más valoradas es la anonimidad ya que, a diferencia de los exchanges, no se requiere habitualmente ninguna información, documentación ni verificación, y no deja rastro electrónico en plataformas de intercambio. Además, es un proceso rápido y que puede realizarse de manera sencilla. Simplemente es que el vendedor escanee el código QR de la clave pública del comprador en la aplicación cartera de su teléfono y le entreguemos el dinero. Hay que tener en cuenta que hay que acordar un precio, normalmente basado en el de algún exchange o el CoinDesk Bitcoin Price Index. Por supuesto si el intercambio de dinero es una cantidad

significativa, hay que aplicar las precauciones básicas, o bien realizar la compra con alguien conocido o bien en sitio público y con las precauciones de seguridad básicas.

Además hay quedadas de grupos de bitcoins por todo el mundo, en las que puedes intercambiar con otras personas en un ambiente más cómodo. Una manera de encontrarlos es la web Meetup https://www.meetup.com/es/ buscando por palabra clave bitcoin. Ya hemos mencionado que plataformas como Local Bitcoins permiten contactar con vendedores para comprar en persona, con la ventaja de que son personas que ya habrán participado en

otras transacciones y tendrán valoraciones de usuarios previos con los que han intercambiado bitcoins. Es conveniente elegir a los vendedores no sólo con un feedback bueno, sino también con un número alto de operaciones realizadas. Es conveniente tener en cuenta que lo habitual es negociar el precio antes del encuentro cara a cara. Además muchos vendedores cobran un precio algo superior (5-10%) al del mercado.

Pantalla de inicio de Meetup
(Fuente: Meetup España
https://www.meetup.com/es-ES/)



Comprando bitcoins en un cajero de bitcoins

Otra manera de conseguir bitcoins, si bien todavía no muy extendida son los cajeros de bitcoin. Hay un tipo de cajeros automáticos, que pueden ser dedicados a bitcoin. Puedes localizar

los cajeros en webs como https://coinatmradar.com/. El funcionamiento es sencillo, pueden comprarse bitcoins introduciendo el dinero en el cajero, o bien venderse bitcoins y obtener la contraprestación en euros en efectivo. Servicios como Bit2me https://bit2me.com/inicio permiten crear una cuenta y a través de ella enviar tus bitcoins a un cajero incluido en el sistema Halcash para retirarlos en efectivo. Los cajeros automáticos suelen requerir algún método de identificación, y tienen un límite determinado y no demasiado elevado (por ejemplo 1.000 euros). Ellos mismos general una cartera personal en el momento para almacenar

tus bitcoins, y te facilitan la clave privada y pública de esta cartera en el momento.

Cajero automático de bitcoins
(Fuente: Steemit)

También están los llamados cajeros

humanos. Son localizaciones, en muchos casos comercios de diferentes actividades, que permiten entrar, pagar en euros y te los cambian por bitcoins dándote la clave privada y pública de la cartera. El comercio se lleva un porcentaje de la transacción.

En conclusión, ¿dónde consigo mis bitcoins?

Para la mayoría de personas interesadas, creo que comprar los bitcoins en plataformas electrónicas de intercambio (exchanges) es la mejor opción. Es un método seguro (si se tiene la precaución

de no dejar dinero ni bitcoins almacenados), con unas comisiones bajas y que permite comprar a un precio ajustado a mercado. Además es un método razonablemente ágil, si bien el proceso inicial de verificación puede ser un poco tedioso, y las transferencias de dinero algo lentas.

En el caso de valorar particularmente la rapidez, los cajeros de bitcoins no requieren esperar a que se efectúe una transferencia de dinero que tarda unos pocos días. Por otro lado, las transacciones entre particulares permiten en general una mayor anonimidad.

Finalmente, la minería de bitcoins requiere un planteamiento diferente, incluyendo una inversión en equipamiento que funcione de manera continuada, así como un consumo eléctrico muy elevado, sobre todo a precios españoles. Por tanto creo que sólo tiene sentido si este coste eléctrico puede reducirse notablemente.

5. Cómo almacenar bitcoins

La respuesta a la pregunta de cómo almacenar bitcoins es probablemente la más importante relacionada con la seguridad de nuestro dinero. Hemos comentado ya que, en realidad, nosotros no guardamos los bitcoins en ningún lugar. Los bitcoins están almacenados en la red, y sólo las personas que conocen la clave privada de cada cartera pueden acceder a ellos. Por tanto, en la práctica, la clave privada es equivalente a nuestro dinero. Si alguien la llega a conocer, puede disponer ilegalmente de todo

nuestro dinero. Por otro lado, dado que es imposible de reconstruir, si la perdemos perdemos nuestros fondos. En este capítulo vamos a comentar algunas de las opciones para almacenar nuestros bitcoins, así como estrategias para incrementar la seguridad del almacenamiento.

Hay diferentes formas de almacenar los bitcoins, una es directamente dejar los bitcoins en nuestra cuenta de una plataforma de intercambio electrónico, una opción nada aconsejable para cantidades significativas de dinero. La mejor opción son las carteras bitcoin, si bien hay diferentes tipos: online, móviles, ordenador, en papel y

dispositivos hardware especializados.

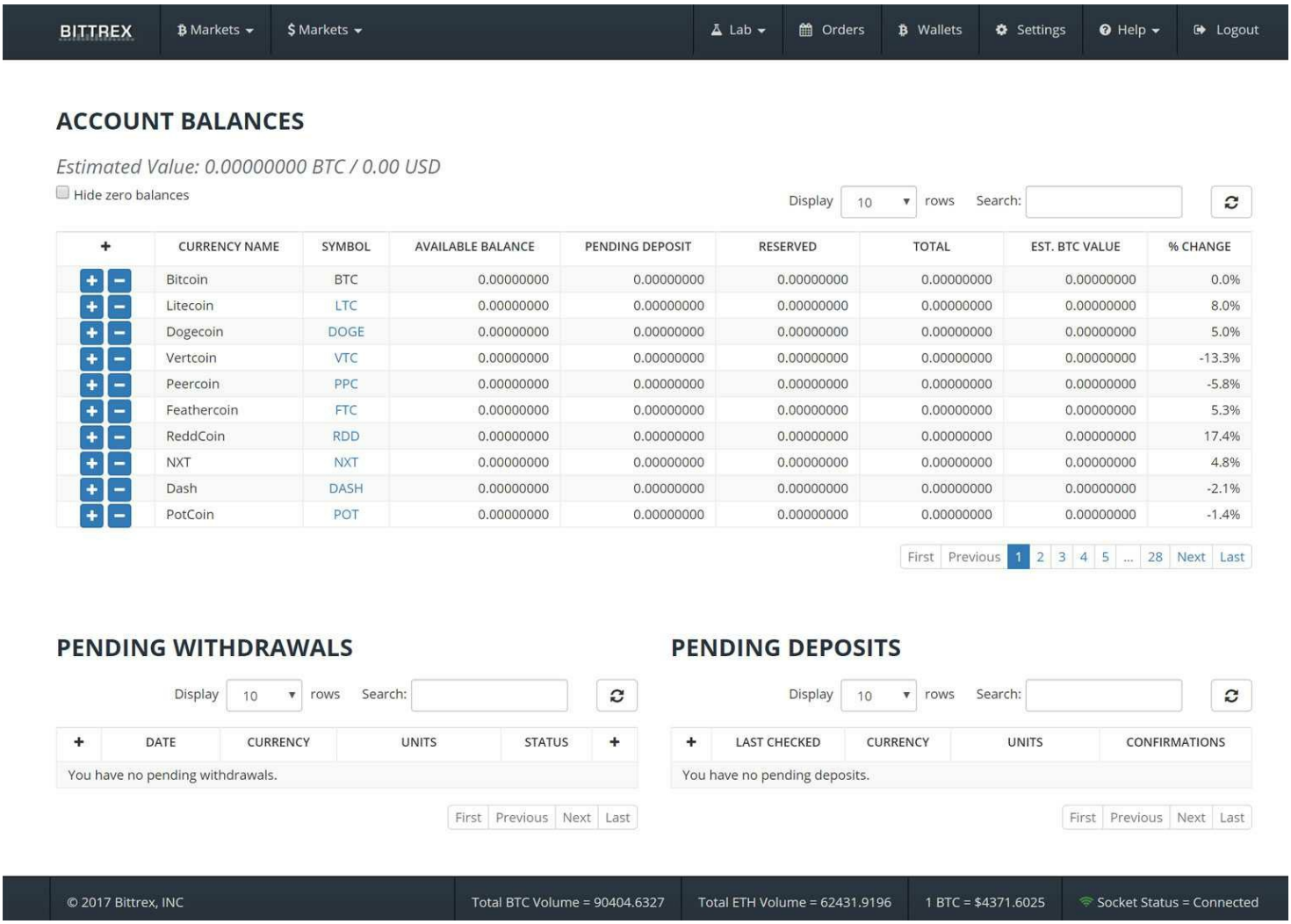
Almacenar bitcoins en nuestra cuenta de una plataforma de intercambio electrónico (exchange)

Mt. Gox fue la mayor plataforma de intercambio de bitcoins. Lanzada en Japón en 2010, a finales de 2013 gestionaba el 70% de las transacciones mundiales de bitcoins, un porcentaje increíblemente elevado. Sin embargo el 24 de Febrero de 2014, Mt. Gox suspendió el trading y la página web

desapareció. Lo que ocurrió es que a la compañía le habían robado 745.000 bitcoins de sus clientes, además de 100.000 bitcoins propios y 27 millones de dólares. Esta cantidad inmensa de bitcoins equivalía al 7% de todos los bitcoins existentes en el momento, y valían alrededor de 475 millones de dólares en aquel momento. Ahora valdrían alrededor de 8.000 millones de dólares. Como consecuencia de su situación financiera, la compañía fue a la bancarrota. Aunque 200.000 bitcoins fueron posteriormente recuperados, el destino de los otros 645.000 bitcoins no se conoce. Muchos usuarios perdieron bitcoins, y posteriormente ha dado lugar a distintos procedimientos judiciales.

Ha habido otros múltiples casos de robo de bitcoins a plataformas de intercambio electrónico.

Balance ilustrativo de criptomonedas en el servicio de intercambio Bittrex
(Fuente: Bittrex https://bittrex.com/)



La clave privada de la cartera es nuestro dinero, pero en el caso de las plataformas de intercambio electrónico, **las claves privadas sólo las tiene la plataforma**, que crea muchas carteras virtuales para su manejo interno. Nosotros sólo tenemos el nombre de usuario y la contraseña de nuestra cuenta. Aparte de un robo mayor, como el de Mt. Gox, hay muchísimos robos más pequeños, en los que un hacker consigue a través de distintas maneras nuestro nombre de usuario y contraseña de nuestra cuenta en una plataforma de intercambio, y en el momento en que la tiene puede transferir todos los fondos a una cartera suya en cuestión literalmente de minutos.

Las protecciones más básicas son seleccionar una plataforma de intercambio grande, con experiencia, que lleve años operando en este mundo, como las mencionadas en el capítulo 4. Otra protección básica implica utilizar una contraseña muy segura (más sobre esto en el capítulo de seguridad), pero aún así hay tantas formas de robar esta información que, adicionalmente, lo que tenemos que hacer es transferir los bitcoins a una cartera virtual nuestra. Esto es tan sencillo como entrar en la opción de transferir de la plataforma de intercambio, allí aparecerá una clave pública que es la que introduciremos en nuestra cartera para realizar la

operación. Voilá, en unos minutos ya tenemos nuestros bitcoins en nuestra cartera.

Almacenar bitcoins en una cartera online

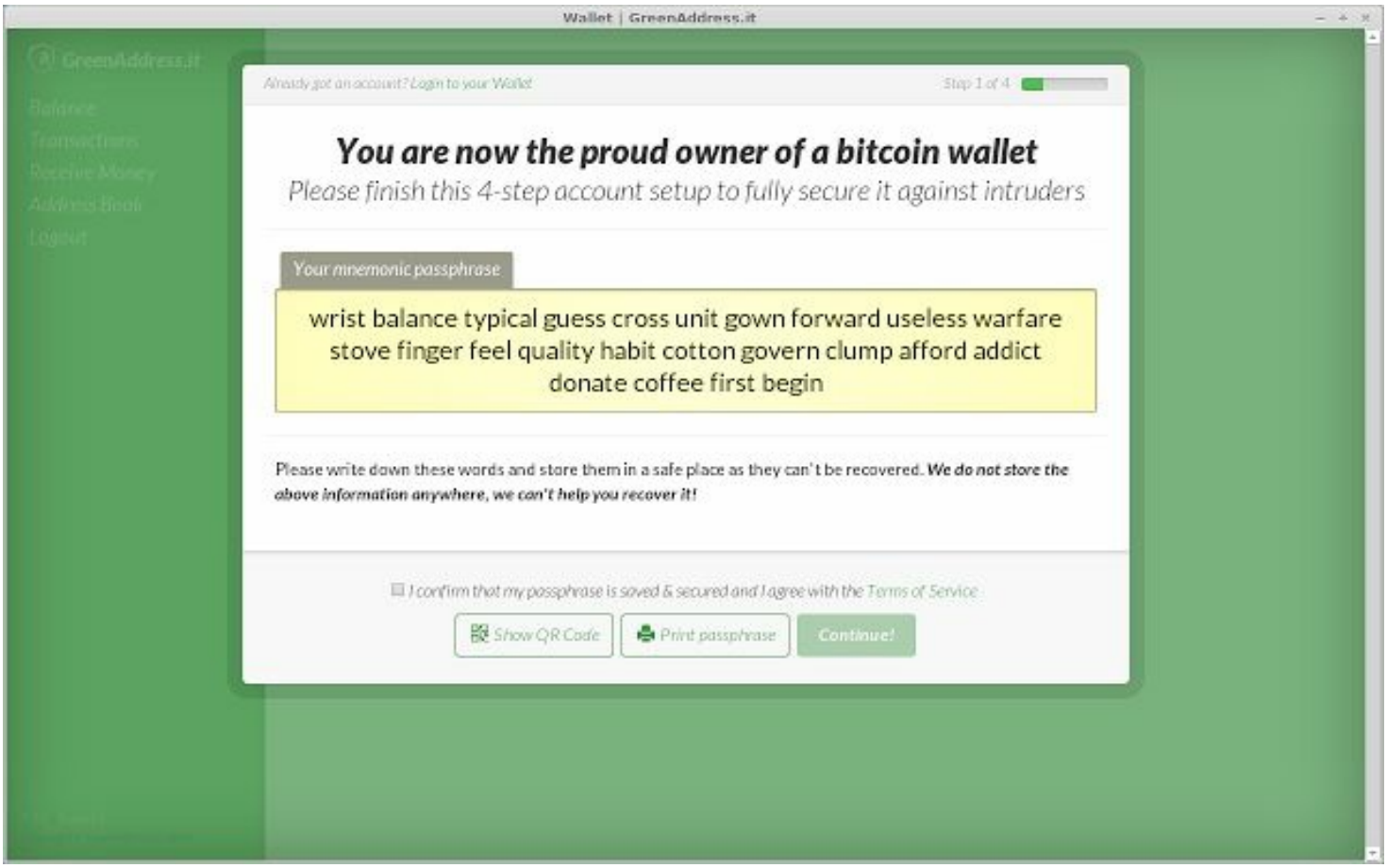
Utilizar una cartera online es una opción bastante popular. Ofrece la ventaja de que estando tus bitcoins en la nube puede acceder a ellos desde cualquier lugar, y habitualmente tanto desde ordenador como desde dispositivo móvil. Además la gestión a través de una plataforma web es sencilla, y no requiere instalación de software (salvo

apps móviles). Por otro lado estando en la nube da la sensación de que podemos confiar en sus sistemas de copia de seguridad (backup) de la información, y no haría falta hacer copias de seguridad por nuestra parte.

Sin embargo el inconveniente es que **estamos depositando nuestro dinero y nuestra confianza en un tercero.** Aunque no sea habitual, el servicio de cartera podría un día cerrar por diferentes razones. Por otro lado, un hacker podría acceder a los datos, ya sea hackeando el servicio online o bien nuestra cuenta directamente o a través de nuestro ordenador.

Algunos servicios online de este tipo son Green Address, BitGo o Coin.Space. Una funcionalidad fundamental es anotar la frase-contraseña (passphrase) de 24 (típicamente) palabras que nos permite recuperar el acceso a nuestra clave privada en caso de cualquier problema con ella.

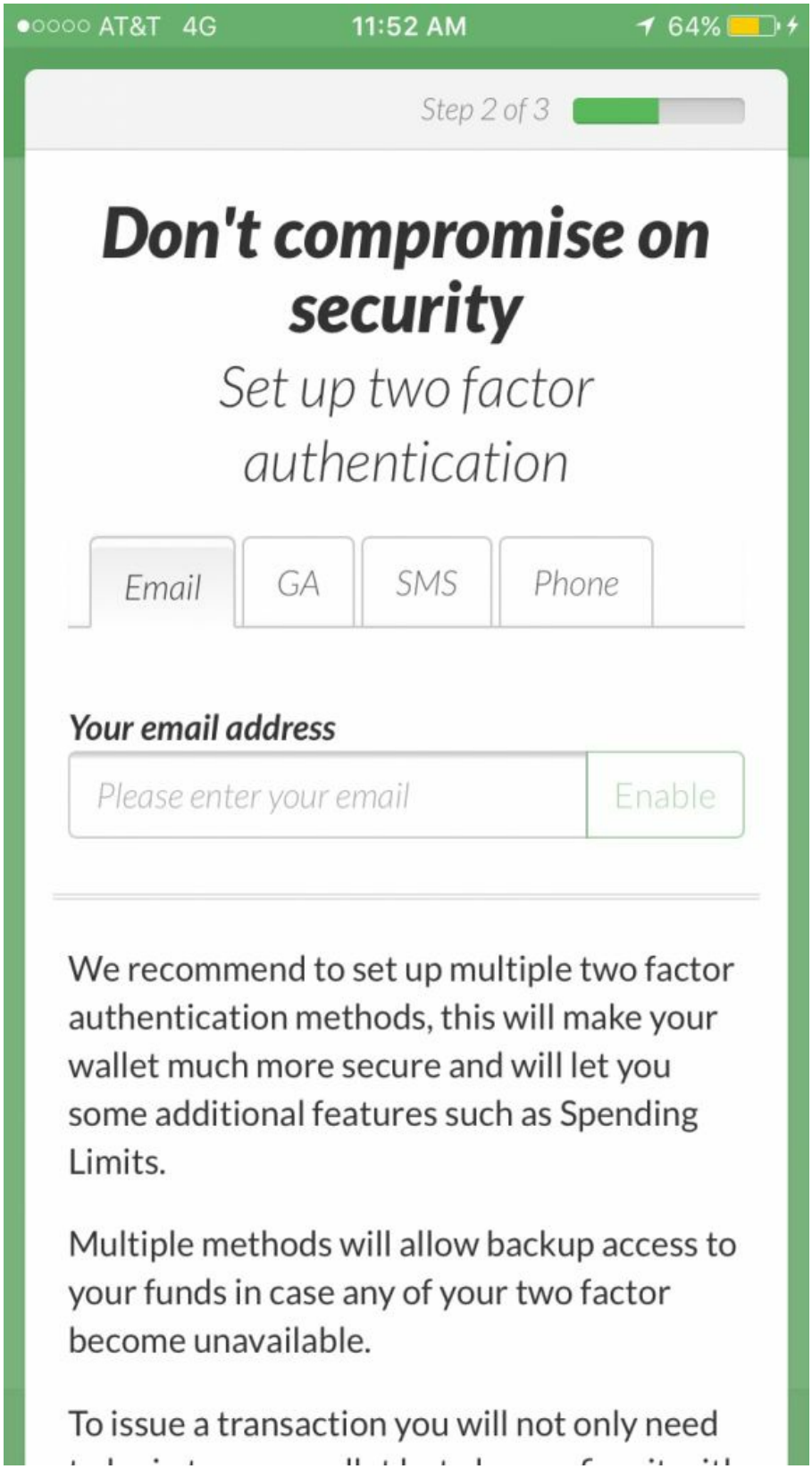
Configuración de cuenta en GreenAddress incluyendo passphrase
(Fuente: GreenAddress)



Durante la configuración también es muy importante mejorar la seguridad activando la verificación de doble factor, es decir, que si no basta con introducir el usuario y contraseña, sino que el servicio de cartera nos envía una autenticación por email, SMS, etc, cada vez que intentamos acceder.

Configuración de autenticación de doble factor en GreenAddress

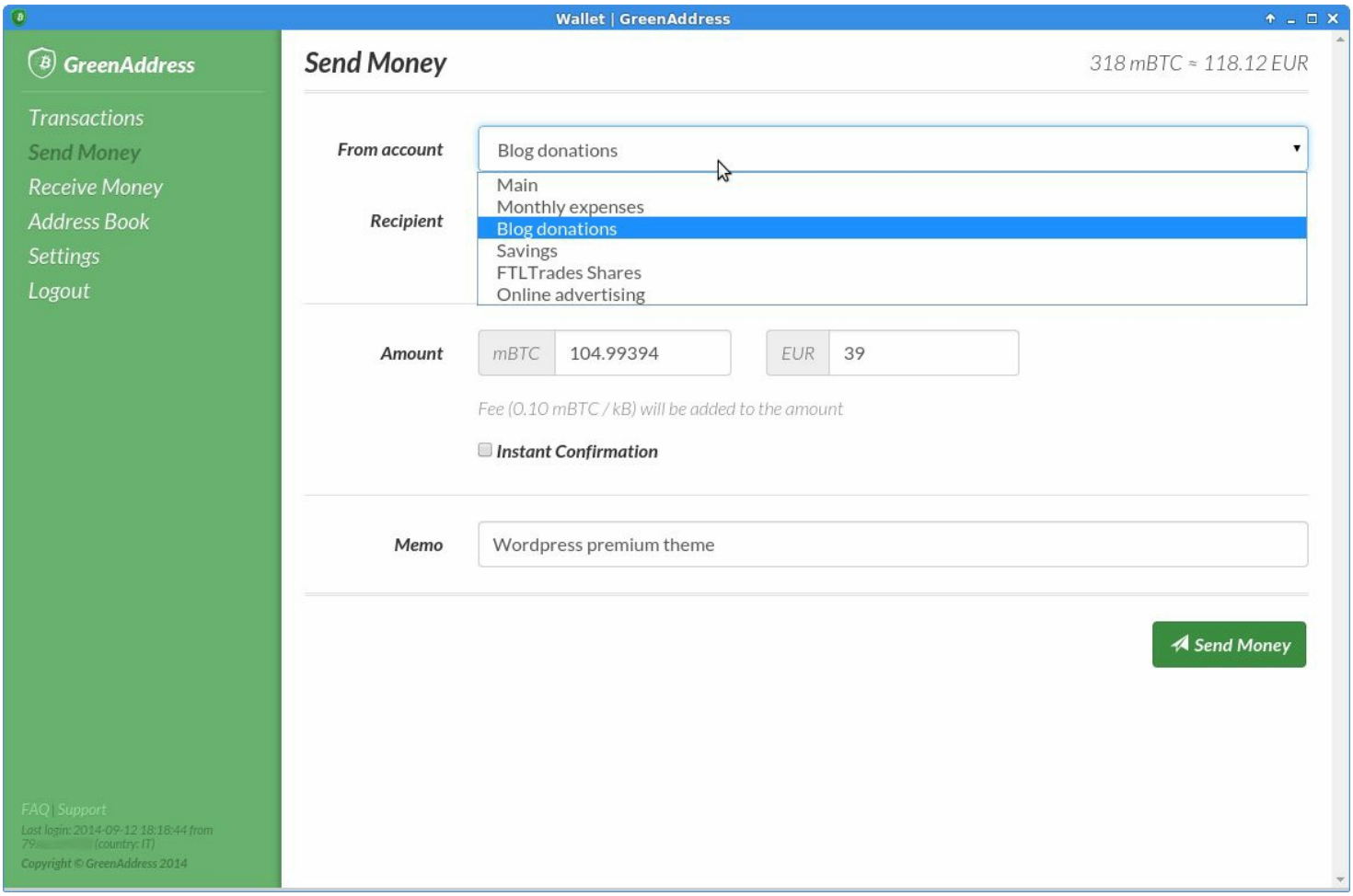
(Fuente: GreenAddress)



Posteriormente configuramos un código PIN para acceder a la aplicación. El

funcionamiento es bastante intuitivo en general y similar a otras carteras, pudiendo enviar bitcoins, recibir bitcoins, visualizar las transacciones realizadas, configurar diversas cuentas, etcétera.

Menú principal y pantalla de envío de dinero en GreenAddress
(Fuente: GreenAddress)



En mi opinión las carteras online son adecuados para iniciarse con compras pequeñas de bitcoin. Sin embargo no son el servicio idóneo para almacenar cantidades importantes, debido a los riesgos antes comentados.

Almacenar bitcoins en una cartera en nuestro ordenador

Esta opción requiere instalar un programa de cartera en nuestro ordenador. Este programa contendrá la información de acceso a nuestros bitcoins, particularmente las claves privada y pública. Las ventajas de esta aproximación es que la seguridad, a priori, es más elevada ya que **somos nosotros los que controlamos totalmente la información esencial de nuestras cuentas de bitcoins.**

Esto conlleva además una responsabilidad adicional. Debemos de

proteger este ordenador instalando un buen antivirus, y tomando otras medidas de seguridad para evitar que nuestro ordenador pueda ser hackeado, ya que en ese caso un hacker podría llegar a hacerse con la información de clave privada. Por otro lado sabemos que todo ordenador puede fallar en algún momento, y esto nos obliga a realizar una copia de seguridad de la información (sobre todo claves privadas) en un disco duro externo para evitar que se pierda la información en ese caso. En este sentido lo recomendable es al menos realizar dos **copias de seguridad externas** y que estén almacenadas en dos localizaciones diferentes.

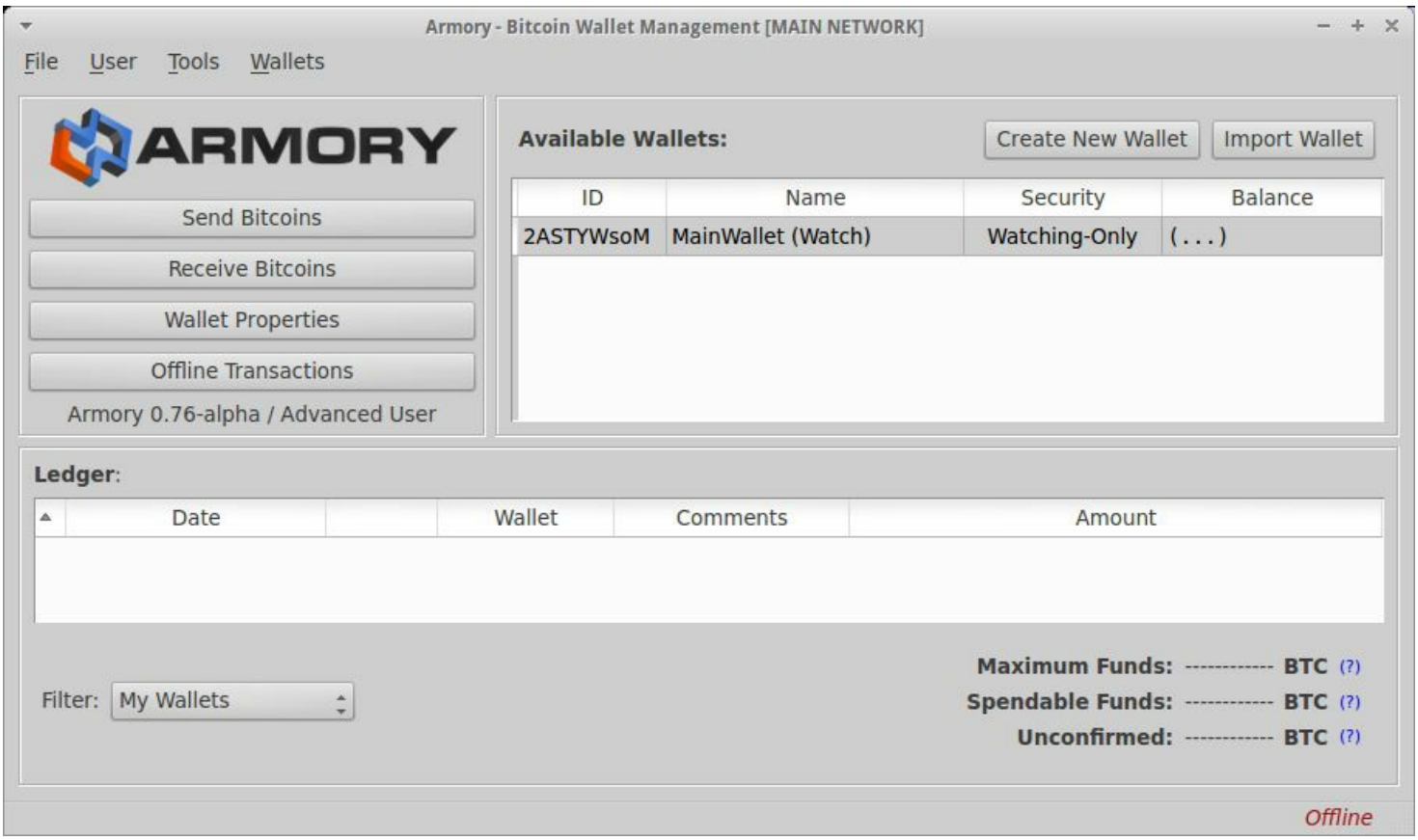
Hay muchas y buenas opciones de carteras para ordenador, algunas de ellas son Armory, Coinbase (unida al exchange del mismo nombre), Blockchain.info, Xapo, Electrum, Bitcoin Core. Cada uno ofrece ciertas ventajas respecto a sencillez de utilización, seguridad, y funcionalidades.

El funcionamiento general es el estándar en las carteras Bitcoin y con un poco de uso resulta razonablemente intuitivo:

- **Creación de una nueva cartera** (con claves pública y privada) o importación de una cartera ya

existente a partir de la passphrase.

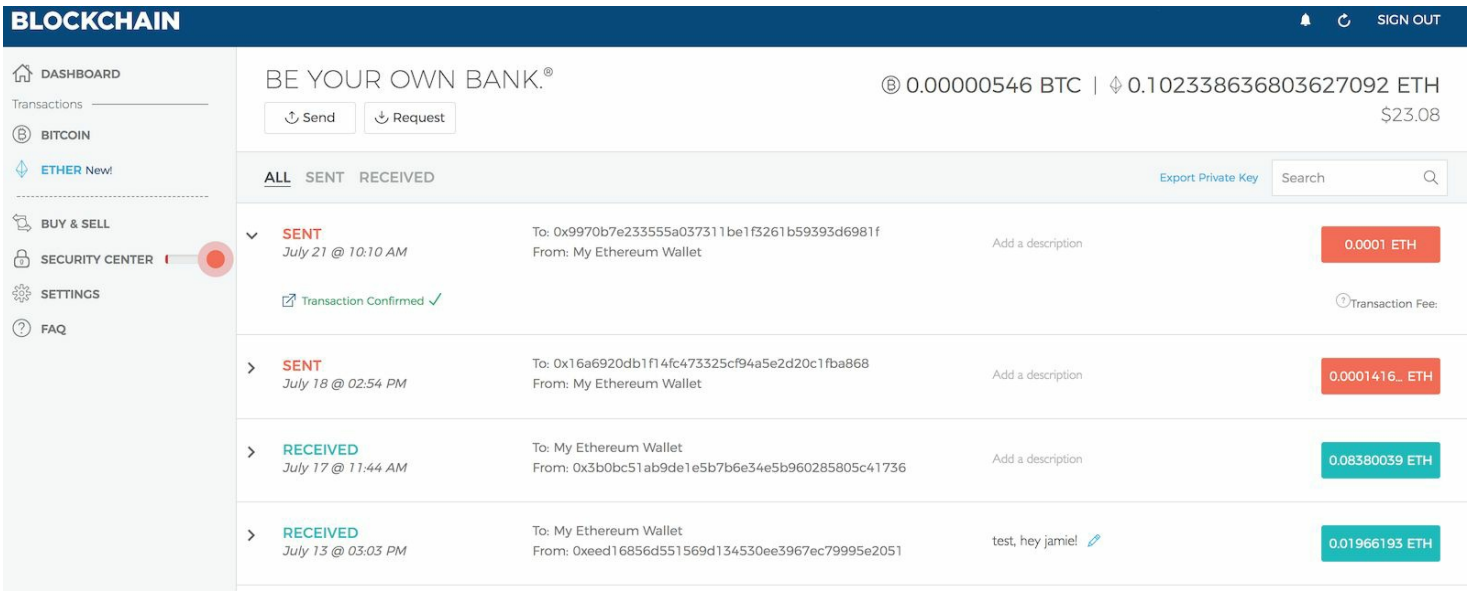
Menú principal y pantalla de gestión de carteras en Armory
(Fuente: Armory)



- **Visualización de balances y movimientos**, incluyendo balance

de las diferentes cuentas, envíos y recepciones y estado de confirmación de las operaciones.

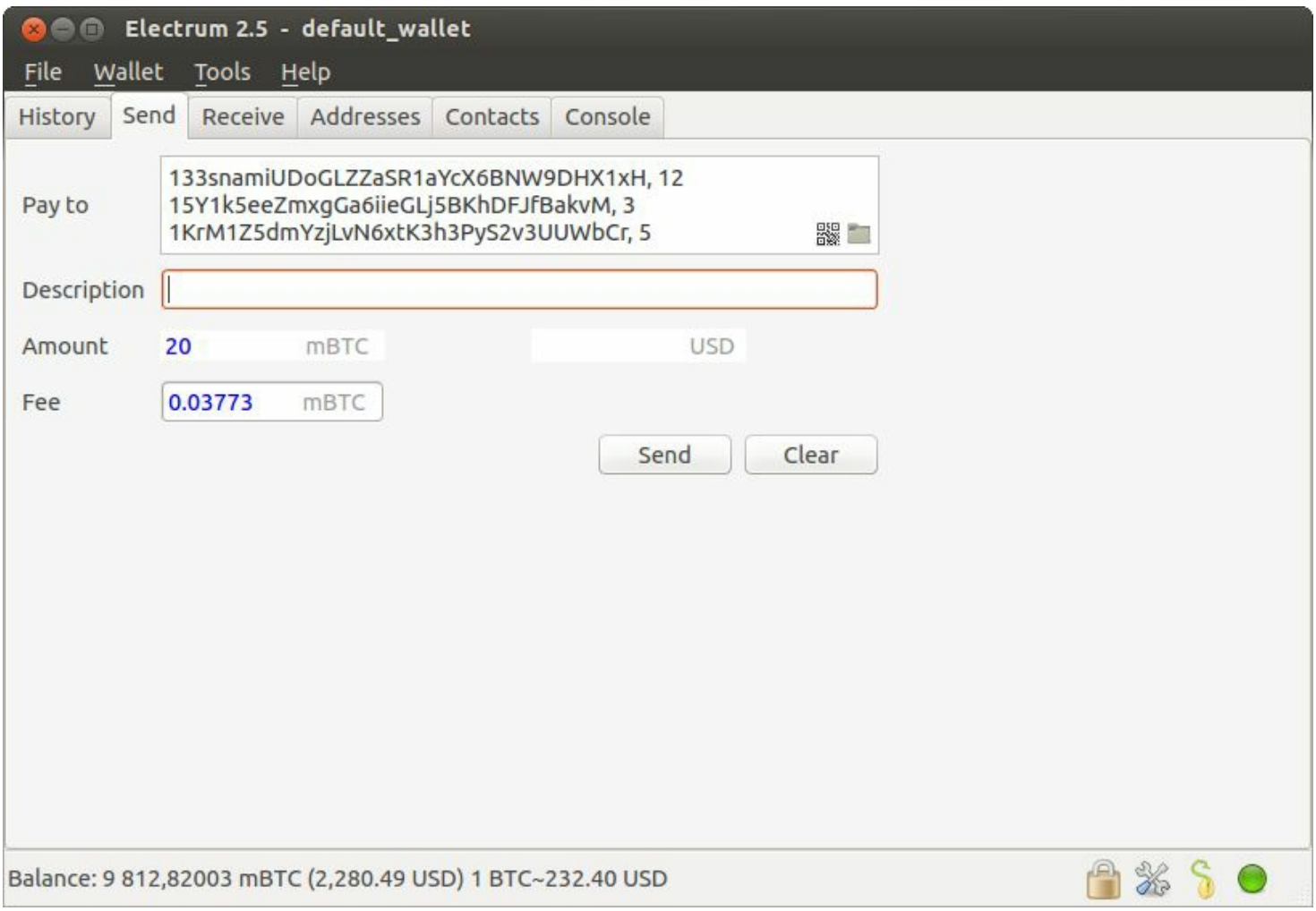
Balance y transacciones en Blockchain
(Fuente: Blockchain)



- **Envío de bitcoins**, ya sea introduciendo la clave pública completa a la que queremos enviar

o con el código QR de la dirección de destino

Ejemplo de envío de dinero en Electrum
(Fuente: Electrum)



- **Recepción de bitcoins**
- **Opciones de configuración**, incluyendo funciones de gestión de cuentas, autentificación de doble factor, multi-firma (multisig), backup, etcétera

Las carteras de ordenador son una opción razonablemente segura, en la que ya estamos teniendo el control total de nuestro dinero virtual. Ahora bien, esto requiere que seamos escrupulosos en mantener nuestro ordenador a salvo de hackers, y que realicemos copias de seguridad.

Almacenar bitcoins en una cartera móvil

Frente a la solidez de almacenar nuestros bitcoins en nuestro ordenador, almacenar los bitcoins en un dispositivo móvil ofrece **mayor agilidad para su uso**, en el sentido de que lo llevamos a todos lados, por lo que posibilita realizar compras e intercambio de bitcoins en cualquier lugar. El **inconveniente, como podrás imaginar, es que si perdemos o nos roban nuestro móvil**, y no hemos tomado otras precauciones, diríamos adios a nuestro dinero. Para evitar este problema, muchas de estas apps se sincronizan con

carteras online o de ordenador, por lo que en el fondo estamos hablando de que son carteras multiplataforma con un cliente móvil. La práctica totalidad de las carteras online que hemos comentado ofrecen aplicaciones móviles.

Algunos ejemplos de carteras móviles son Mycelium, Electrum, Green Address, o Breadwallet

Pantallas de movimientos, envío y recepción de dinero en Breadwallet
(Fuente: Breadwallet)


Carrier
10:24 PM
฿429,800 ($245.73)
sent
7/30@9p
($-5.77) ฿-10,100
($245.73) ฿429,800
sent
7/30@9p
($-57.23) ฿-100,100
($251.50) ฿439,900
received
7/30@9p
($308.73) ฿540,000
($308.73) ฿540,000
sent
7/30@9p
($-474.47) ฿-829,900
($0.00) ฿0.00
sent
7/26@1a
($-57.23) ฿-100,100
($474.47) ฿829,900
more...
about
5:29 PM
฿18,100 ($12.07)
send money:
scan QR code
address from clipboard
5:24 PM
฿0.00 ($0.00)
receive money:
QgBEWVS8vDKrBtL4mYLotwZNR

Las carteras móviles son una buena opción para tener disponible una cantidad relativamente pequeña de bitcoins para realizar compras o intercambio. Sin embargo no son tan buena opción para almacenar nuestros "ahorros" bitcoin, debido al riesgo de pérdida o robo intrínseco en todo dispositivo móvil.

Almacenar bitcoins en un dispositivo hardware

En mi opinión las **opciones más seguras de almacenamiento de bitcoins** son las carteras hardware totalmente dedicadas.

Se trata de dispositivos físicos diseñados exclusivamente para almacenar bitcoins, y que contienen múltiples medidas de seguridad en su hardware y software. Además no disponen de conexión a Internet, minimizando el riesgo de hackeo. Funcionan conectados a un ordenador, normalmente por USB, e instalando un software específico. Almacenan la información esencial (sobre todo la clave privada) y no la muestran en ningún caso, sino que tienen un sistema que valida las operaciones sin mostrar esta. Por otro lado requieren además la entrada de un PIN por parte del usuario, a través de unos botones físicos. Las dos marcas de experiencia más contrastada

en este ámbito son Trezor y Ledger, y ambas ofrecen dispositivos de mucha calidad en diferentes formatos.

Dispositivo Ledger Nano S
(Fuente: Ledger
https://www.ledgerwallet.com/)

Todo esto suena muy bien, lo único, ¿qué ocurre si se dañan? Además de ser

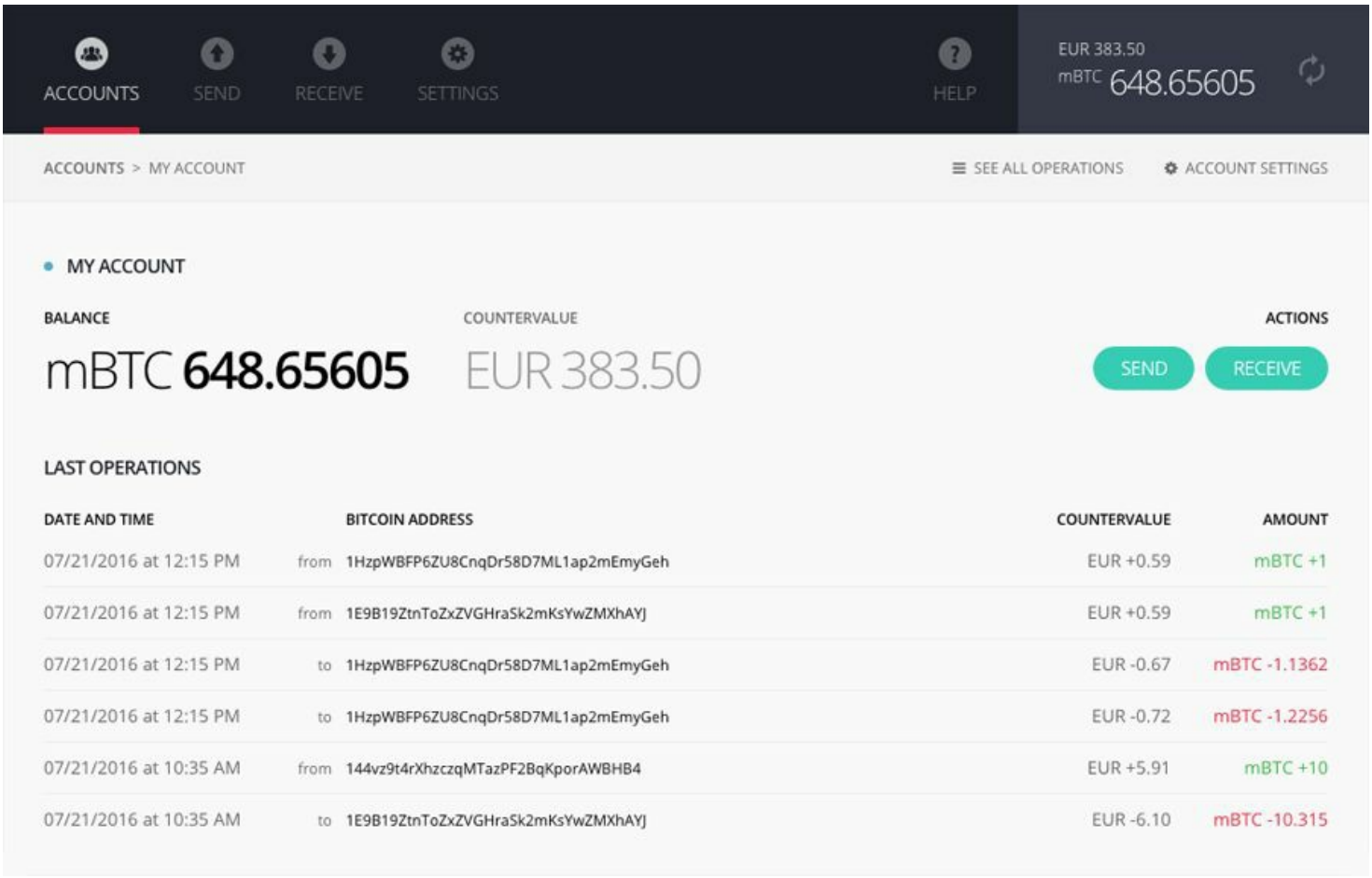
muy resistentes al daño accidental (caídas, etcétera). Estos dispositivos, de manera similar a los otras carteras, disponen de un ingenioso sistema de backup. Durante su configuración te muestran una secuencia de palabras (unas 30) que debes de recoger en una hoja con mucha atención. Esta secuencia de palabras permite que, si nos roban o se estropea el dispositivo, comprando otro dispositivo nuevo podamos reconstruir totalmente nuestras claves en el nuevo introduciendo esta secuencia de palabras.

El funcionamiento de estos dispositivos es semejante al de otras carteras. Requieren de la instalación de un

software en el ordenador con el que se manejan. Una vez conectado el dispositivo e introducido el PIN, permiten revisar el balance y movimientos de la cuenta, enviar y recibir bitcoins, y modificar opciones de configuración. Las operaciones de envíos de bitcoins siempre requerirán de presionar algún botón o introducir una clave en el dispositivo.

Información de cuenta en la aplicación de Ledger para ordenador

(Fuente: Ledger https://www.ledgerwallet.com/)



Almacenar bitcoins en una cartera de papel

Otra opción bastante popular y, desde luego, económica, es crear lo que se

llama una cartera de papel. Además es **bastante segura**, ya que no es vulnerable a hackers y no puede perderse en casos como, por ejemplo, un disco duro dañado, además las claves no están almacenadas en ningún soporte digital. Una cartera de papel puede ser tan simple como escribir en un papel la clave pública y la clave privada, en ese caso hay que ser extremadamente cuidadoso ya que cualquier error podría hacer que perdiéramos la clave privada y, por tanto, el acceso a nuestros bitcoins.

Por otro lado hay **servicios que permiten crear una cartera de papel** de una manera algo más sofisticada, por

ejemplo incluyendo códigos QR de las claves para que escanearla con una cartera de software sea más sencillo, o incluyendo un información adicional en el formato que nos ayude a utilizar estas claves. Un servicio popular es https://www.bitaddress.org , cuyo funcionamiento es tremendamente sencillo. Cuando entramos en esa dirección nos pide que ayudemos a generar aleatoriedad, ya sea moviendo el ratón o escribiendo caracteres en una caja de texto. Como medida de seguridad, una vez has entrado en la página web, debes de desconectar el ordenador de Internet y ejecutar el código totalmente offline para generar las claves.

Generación de dirección Bitcoin en BitAddress

(Fuente: Bitaddress.org)

Posteriormente nos genera las direcciones bitcoin pública y privada (incluyo un ejemplo) con los códigos QR. Imprimiendo esto, ya nos valdría como paper wallet sencillo. Toma la

precaución de desconectar la impresora de Internet antes y durante la impresión.

Claves pública y privada generadas por BitAddress

(Fuente: Bitaddress.org)

Para algo un poco más completo, con varias direcciones generadas, podemos darle a la opción Paper Wallet, y posteriormente imprimirlo.

Impresión de claves en BitAddress

(Fuente: Bitaddress.org)

Puede que te peguntes cómo de seguro es que una página web genere y te muestre tu clave privada. La respuesta es que dentro de la comunidad bitcoin, BidAdress se considera generalmente seguro. El software para generar se ejecuta en tu propio navegador, no en el servidor, y no se transmiten tus claves por Internet. Además su código es

abierto, lo que significa que está publicado y es verificable que no contiene código malicioso. Por supuesto nada es 100% seguro, como ya sabrás. Otra opción es descargar un programa generador de claves en lugares como GitHub y ejecutarlo en el ordenador desconectado de Internet.

Si quieres una cartera de papel aún más sofisticada, puedes encontrarlo en https://bitcoinpaperwallet.com/ , donde generan unas carteras de papel con protecciones por hologramas y sellos de que no han sido abiertos.

Es necesario contar con una serie de precauciones en el caso de carteras de

papel. Como ya hemos comentado perder la clave privada es equivalente a perder los bitcoins, y si alguien tiene acceso a esta información nos puede robar los bitcoins en pocos minutos. La precaución más básica tiene que ver con la propia impresión. La tinta de la impresora puede deteriorarse hasta queda ilegible cuando se moja, por eso se recomienda o bien imprimir en papel a prueba de agua, o guardar el papel en una bolsa sellada.

Por otro lado, almacenar una única copia de nuestra cartera de bitcoins tiene un riesgo considerable. Imagina que esa única copia es robada, se quema, ¡o la tienes dentro de un libro

que alguien tira al hacer limpieza! Es recomendable, de hecho, guardar tres copias (o más) en al menos dos localizaciones diferentes, mejor incluso más. Respecto a dónde guardarlas ya depende de cada uno, y del valor de lo que queramos proteger en la cartera. Hay personas que la guardan en caja fuerte, otros en algún lugar oculto en su casa.

6. Seguridad y bitcoins

Una de las principales características de los bitcoins es que el dueño tiene la responsabilidad sobre la seguridad de sus propias criptomonedas. Hemos comentado bastantes aspectos de seguridad a lo largo de capítulos anteriores, y ahora es un buen momento para repasar lo más relevante y añadir otros nuevos.

Ten en cuenta que la mayoría de aspectos aquí contemplados no son exclusivos de tu actividad con bitcoins,

sino que deberían de aplicar ya a toda tu vida online. Todos conocemos casos de acceso por hackers a cuentas, robo de identidades, estafas, y términos similares. Debemos de aplicar todas las precauciones para asegurar que nuestra vida digital es segura.

Recomendaciones para el uso seguro de bitcoins

Ordenador y conexión seguros

- Sistema operativo actualizado
- Buen antivirus actualizado
- Ordenador adecuado (usos alternativos)
- Perfiles de usuarios y contraseñas
- No ordenadores compartidos
- Redes WiFi seguras (posible VPN)
- Cierra tus sesiones

Acceso seguro

- Contraseñas seguras
- Autentificación de doble factor
- Contraseña de tu coreo segura
- No repetir contraseñas
- Cambiar contraseñas expuestas
- Almacenaje seguro de contraseñas (posible gestor)

Bitcoins seguros

- Copia de seguridad de carteras
- Utilizar carteras hardware o papel
- Distribuir entre varias carteras
- Revisar bitcoins periódicamente
- Proteger clave privada
- Cuidado con servicios dudosos
- Planificar para lo peor

Utiliza un ordenador seguro

Cuando operas con bitcoins no necesitas un ordenador potente, pero es esencial que sea un ordenador seguro. Podemos utilizar las mejores contraseñas y las carteras más seguras, pero todo estará en alto riesgo si utilizamos un ordenador que un hacker controla o en el que hay instalado un programa que detecta todas las pulsaciones de las teclas y las envía a alguien con intenciones maliciosas. Por ello es fundamental partir de una serie de recomendaciones esenciales.

Actualiza siempre el sistema operativo

Continuamente se detectan nuevos

agujeros de seguridad en los sistemas operativos, y esto requiere publicación de actualizaciones de seguridad. Es esencial actualizar nuestro sistema operativo constantemente para asegurar que nuestro ordenador es inmune a estos agujeros de seguridad.

Utiliza el mejor antivirus

Hay muchas maneras diferentes de tomar control de nuestro ordenador o de instalar una aplicación que recoge información personal y se la envía a alguien. Puede ser que hayamos abierto un email dudoso, hayamos descargado un video, hayamos hecho click en el banner inadecuado. Un antivirus nos

protege de la mayoría de estas amenazas. Elige el mejor antivirus disponible en el mercado. Muchos antivirus protegen de la mayoría de virus, pero pocos protegen de la práctica totalidad de las amenazas, de manera siempre actualizada, y protegiéndonos en tiempo real al navegar por Internet, antes de que la instalación maliciosa ocurra. Estas características son esenciales para la seguridad de nuestro ordenador, y aunque implican un coste, este dinero está bien dedicado.

Usa un ordenador adecuado

Si alguien en tu casa dedica parte de su

tiempo a la descarga de películas, libros o programas por redes P2P en un ordenador, a navegar por la Internet profunda o a chatear con compañías dudosas, no es ese el ordenador que debes de dedicar a tus bitcoins. El sistema operativo más actualizado y el mejor antivirus no te protegen de un usuario que salta todas las precauciones de seguridad y acepta (o no rechaza) instalar cosas que no debe en el ordenador. Esfuérzate en mantener un ordenador seguro para us bitcoins, merece la pena.

Delimita perfiles de usuarios y contraseñas

Todo ordenador debe de tener un perfil de usuario administrador, y éste debe estar bien seguro y delimitado, con una contraseña muy segura (más sobre esto a continuación). Por otro lado si un niño quiere ver vídeos de YouTube en el ordenador, crea un perfil de usuario sin privilegios de administrador, y también con una contraseña segura, para este niño. Al no tener privilegios de administrador, se limita mucho el posible daño que un atacante podría infligir sobre el ordenador.

Nunca utilices ordenadores compartidos

Un ordenador de un cibercafé o el

ordenador de la biblioteca no son los equipos en los que debes de entrar a operar con bitcoins, nunca. La razón es doble. Por un lado, estos ordenadores no cumplen casi nunca todos los requerimientos de seguridad que hemos comentado antes. Aunque no he visto estadísticas, estoy convencido de que la mayoría de ordenadores de este tipo tienen instalado algún software malicioso, a menudo por parte de los propios usuarios. Además hay un riesgo adicional, y es que al introducir, por ejemplo, un usuario y contraseña, esta información puede quedar almacenada en el administrador de contraseñas o en el propio navegador. Incluso a veces no cerramos bien la sesión y el navegador,

y la información de acceso puede estar en la caché. Recordemos que una contraseña está expuesta en el momento en el que una sola vez deja de estar en lugar seguro, y en un ordenador compartido es muy difícil asegurar que todo lo que hacemos es seguro.

¿Y el ordenador del trabajo?

El ordenador del trabajo suele ser más seguro que la mayoría de ordenadores de uso personal, ya que las propias compañías se encargan de instalar antivirus, actualizar el sistema operativo y otras precauciones de seguridad. Dicho esto, no todas las empresas hacen esto de la misma manera. Si vas a

utilizar el ordenador del trabajo, revisa que se cumplan los requisitos que indicamos arriba.

Utiliza redes seguras WiFi

Las redes WiFi públicas son relativamente sencillas de hackear, no deberías de utilizarlas para enviar tu información más valiosa de los bitcoins, incluso a veces son creadas por los propios hackers para capturar información sensible de los que se conectan. Utiliza mejor redes WiFi privadas, protegidas con contraseñas seguras y que utilicen el último protocolo de seguridad: WPA2 (WiFi Protected Access 2).

Considera utilizar VPN (Virtual Private Networks)

Las VPN crean el equivalente a una red física local (como la de una casa u oficina) de manera virtual, sin necesidad de cableado. Ten en cuenta que las redes VPN gratuitas no suelen ofrecer garantías de calidad y seguridad suficientes para que compense utilizarlas casi nunca. Si quieres una seguridad adicional, una red VPN la ofrece. Las ventajas que ofrece este servicio incluyen:

- Mayor seguridad, ya que una vez se establece esta VPN, todo el tráfico

de información se encripta desde el ordenador hasta el servidor de VPN, y desde este servidor a Internet. Esta encriptación protege el tráfico de datos de posibles accesos a la información que un hacker pueda intentar, por ejemplo a nivel de tu router WiFi

- Mayor confidencialidad, ya que tu proveedor de Internet ni siquiera sabe a lo que estás accediendo porque para él todo el tráfico está encriptado
- Deslocalización. A efectos de Internet tu ubicación ya no está en donde tú estás, sino en donde está el servidor VPN, muchas veces en otro país. Esto puede ofrecer

ventajas como eludir bloqueos geográficos de algunos servicios de Internet

Cierra tus sesiones en todos tus servicios

Cuando has acabado de utilizar un servicio de Internet al que accedes con contraseña, cierra siempre la sesión, no cierres directamente el navegador sin cerrar antes la sesión. Las sesiones abiertas tardan cierto tiempo en cerrarse cuando cierras el navegador, y este tiempo en el que la sesión está abierta pero tú ya no estás podría ser aprovechado por alguien con intenciones

dañinas

Emplea un acceso seguro

La seguridad de aquello que protegemos depende de la fortaleza de las contraseñas que lo protegen. Si utilizas contraseñas como “password” o “123456” estás dejando aquello que proteges al alcance de casi cualquiera. Algunas recomendaciones a continuación.

Elige contraseñas seguras

Una contraseña segura no debe de ser

una palabra del diccionario, ni una secuencia de números sencilla. Debe de ser una secuencia de letras y números difícil de adivinar por lo que se llaman ataques de diccionario. Veamos un ejemplo sobre cómo elegir una contraseña segura. Supongamos que te gusta el libro de Miguel de Cervantes, Don Quijote de la Mancha. La primera frase es: "En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor.". Si enlazas las letras de esta frase, la contraseña será fácil de recordar y a la vez muy segura. Añade además un número y signo para hacerla aún más

segura, e incluye alguna mayúscula, quedaría así: “EuldlMdcnnqa7638/”. Una contraseña segura debería de tener al menos 15 caracteres, recomendable que sean 25 o más.

Contraseñas débiles	Contraseñas intermedias	C
password	paco67	PianoA
123456	cadiz1977	x1&23z
qwerty	ivan17mayo	HTk^oG*
login	kiasorento45	Renaultcc

Utiliza siempre la autentificación de doble factor

La mayoría de servicios online, y desde luego todas las webs de intercambio de

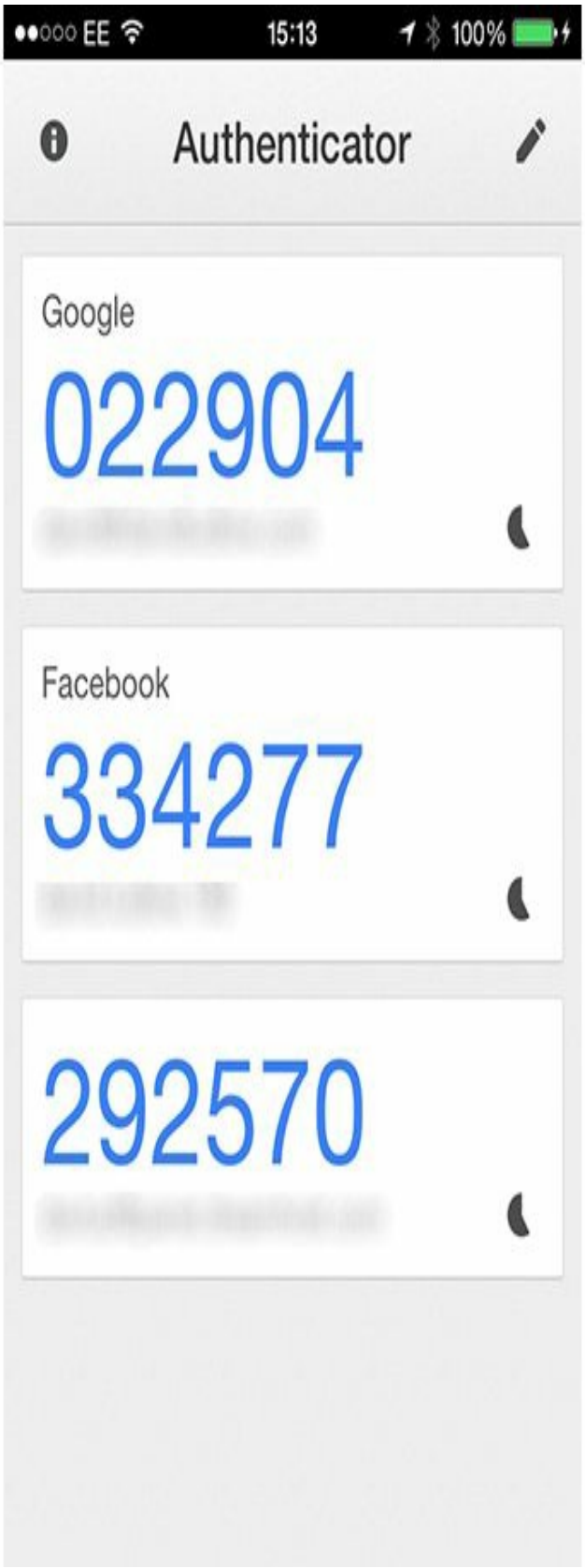
bitcoins, permiten utilizar la autentificación de doble factor. Esto significa que además de introducir el nombre de usuario y la contraseña, debes de introducir una segunda contraseña especial. Este especial puede tener distintas posibilidades. Puede ser una clave que recibes por SMS, de manera similar a cuando debes de confirmar una transacción bancaria, si bien no es lo más seguro ni aconsejable. Es mejor opción una contraseña generada con un programa de contraseñas criptográficas (tipo Google Authenticator o Authy) o por un dispositivo hardware dedicado. En estos dos últimos casos, se trata de contraseñas que cambian cada poco

tiempo (digamos que cada minuto) de manera pseudoaleatoria. La opción para activar la autenticación de doble factor viene en el apartado de seguridad del sitio web normalmente. Si usas Google Authenticator, es una App gratuita para tus dispositivos móviles y añadirlo en un servicio es tan fácil como escanearla un código de barras en la pantalla del ordenador con el móvil o introducir una secuencia de números. Lo que sí que debes de tener en cuenta es copiar una secuencia de números y letras que te aparece una sola vez al configurar authenticator. Esta secuencia es fundamental si cambias de móvil, lo pierdes o hay cualquier otra incidencia, era poder configurar el Authenticator en

otro dispositivo. Ten en cuenta que no podrás acceder a tu cuenta sin esta segunda contraseña, así que si no lo anotas y pierdes el dispositivo, no podrás entrar.

Aplicación Google Authenticator para iPhone

(Fuente: Google Authenticator)



Protege la contraseña de tu correo

electrónico

Si has elegido una contraseña segura en el sistema de intercambio, pero la contraseña de tu correo es sencilla, no estás en una situación segura. Cualquiera que pueda saber tu correo electrónico puede acceder a la opción de "olvidé mi contraseña" de la web, pedir reinstaurar la contraseña, y acceder a tu cuenta de correo con la contraseña sencilla para tomar el control de tu cuenta bitcoin y también de tu correo electrónico. La contraseña de tu correo electrónico debe de ser tan segura como la de tu web de bitcoins. Además siempre debes de activar la autenticación de doble factor también para tu correo electrónico. Otra

opción que tienes es crear una dirección de correo independiente sólo para tus bitcoins, separada de tu correo personal.

No repitas contraseñas

Supongamos que te ha gustado la contraseña de Don Quijote de la Mancha, y la utilizas en tu web de intercambio de bitcoins, pero también en la cuenta del supermercado y en una web nueva que acabas de descubrir y que te gusta. Esto pone la contraseña en riesgo, ya que cualquier hacker que pueda acceder a los usuarios y contraseñas de, digamos, esa web nueva, enseguida va a aprobar ese mismo usuario y contraseña en muchas

otras webs para ver si cuela. Muchas personas, por desgracia, repiten contraseñas, y eso es un problema de seguridad.

Cambia tus contraseñas expuestas

Cambiar la contraseña periódicamente está bien, pero es menos necesario de lo que se suele decir si la contraseña está bien elegida. Lo que sí debes de hacer es cambiar tu contraseña en el momento en el que te das cuenta de que tu contraseña puede estar expuesta. Si en un momento dado la utilizas en un ordenador que puede ser no seguro (por ejemplo en el de un amigo o un ordenador público), o en el momento en

el que te das cuenta de que no estás cumpliendo las precauciones de seguridad, debes de entrar y cambiar todas las contraseñas que puedan haber estado expuestas.

Almacena tus contraseñas de la manera más adecuada

Si hasta ahora utilizas una contraseña sencilla para todos tus servicios de Internet, lo que estamos recomendando es que elijas contraseñas más difíciles e individuales para cada servicio, lo que hace mucho más difícil recordarlas todas. Por tanto tenemos que considerar dónde almacenarlas. Una opción sería escribirlas en un papel, que puede tener

sus ventajas como no ser hackeable, si bien también tiene desventajas como que lo puedes perder, se puede deteriorar y no está disponible en todo momento. Otra posibilidad es utilizar algún sistema de archivo electrónico. Una posibilidad es emplear una hoja de cálculo como Excel, si bien en ese caso deberías de encriptarla, protegida por una palabra clave segura para proteger el acceso a tu valiosa información. Otra opción, muy interesante es…

Considera utilizar un gestor de contraseñas

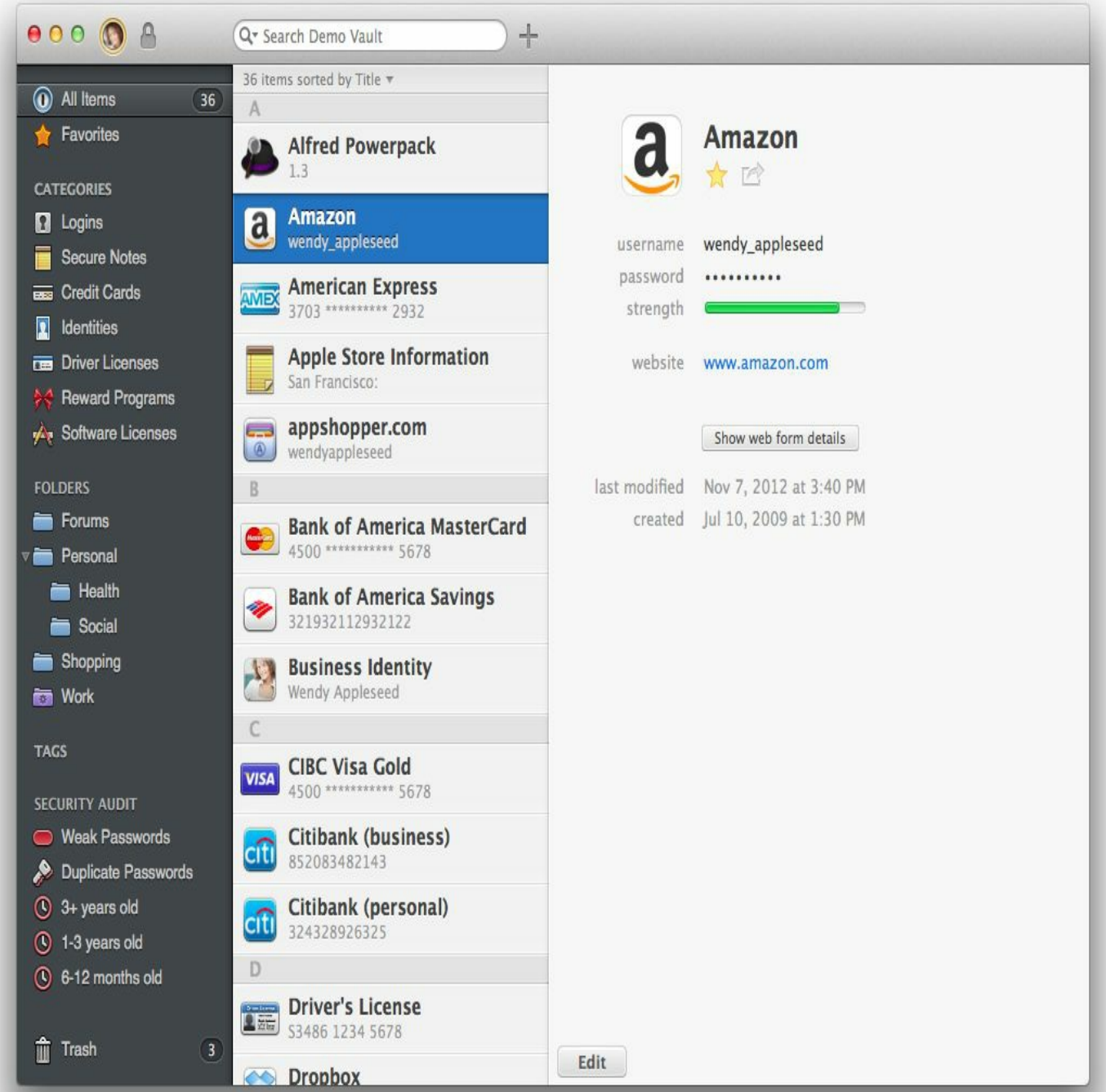
Un gestor de contraseñas es una aplicación en la que puedes almacenar

todos los usuarios y contraseñas de tus sitios web, y estar todos protegidos por una única contraseña. La elección de esta contraseña única es, lógicamente, particularmente importante, por lo que deberías de aplicar lo que hemos comentado y elegir una contraseña de, al menos, 20 caracteres. La información de tus contraseñas permanece siempre encriptada, tanto en el servidor del servicio como en tus dispositivos, por lo que ni siquiera la empresa que ofrece el servicio puede acceder a tus contraseñas. Además, habitualmente las contraseñas están en el servicio web y también se almacenan localmente en los dispositivos en lo que tienes la app o el plug-in del navegador instalado, lo que

protege de posibles interrupciones del servicio. Otras ventajas son mayor rapidez en la introducción de la información de acceso, ya que lo hacen de manera automática al detectar el sitio al que intentas acceder, la generación automática de nuevas contraseñas seguras, y la auditoría de todas tus contraseñas para ver cuáles son seguras y cuáles no. Los más utilizados son 1Password https://1password.com/ , LastPass https://www.lastpass.com/es , y DashLane https://www.dashlane.com/es

Pantalla ilustrativa de gestor de contraseñas

(Fuente: 1Password https://1password.com/)



Asegura tus bitcoins

El objetivo de los consejos anteriores en última instancia es proteger tus bitcoins, veamos ahora consejos específicos sobre estos.

Haz copias de seguridad (backup) de tus carteras

Hazlo ahora mismo si no lo has hecho antes. Si alguna vez pierdes tu cartera, podrías perder tus bitcoins para siempre si no has hecho un backup. La mayoría de las carteras de bitcoins utilizan un protocolo de backup estándar llamado BIP39, que convierte el backup en algo tan sencillo como un listado ordenado de palabras comunes en inglés, entre 12 y 24. Este listado de palabras debes de

escribirlo sin ningún error en papel y luego almacenarlo de manera segura, particularmente a salvo de despistes, robos, agua y fuego. Lo recomendable sería tener al menos dos de estos backups almacenados en ubicaciones diferentes. Cada 6 meses a 1 año deberías de revisar estos backups para verificar que continúan accesibles, legibles y que no están deteriorados.

Ejemplo de frase de recuperación de 18 palabras BIP39

sustain common uncle force bitter chief myself bamboo genre soup hundred mango toward survey member

grab choice machine

No dejes tus bitcoins en tu cuenta del servicio web de intercambio (exchange) o similar

Si no tienes las claves (privada y pública) de tus bitcoins, no tienes tus bitcoins. En un exchange lo que tienes es una cuenta con tu usuario pero que en realidad refleja un estado ficticio, puesto que tus bitcoins están muy probablemente dentro de una cartera bitcoin mezclados con los de otros usuarios. Si el servicio de exchange es hackeado o desaparece de repente (como fue el caso de Max Gov que comentamos), puedes perder totalmente

el acceso a tus bitcoins.

No dejes tus bitcoins en una cartera de bitcoins en el móvil

Una cartera móvil está muy bien por la flexibilidad que te da el llevar bitcoins encima. Sin embargo, no deberías de llevar más bitcoins en una cartera móvil que los euros que llevarías en tu cartera física. En una cartera móvil hay un mayor riesgo de pérdida, robo o que se te caiga y rompa el dispositivo.

Utiliza carteras hardware o en papel

Las carteras hardware son bastante sencillas de utilizar, y se consideran una

de las maneras más seguras de almacenar tus bitcoins, siempre usadas con un backup como hemos comentado. Tienen un cierto coste, que creo que compensa claramente si vas a utilizarlas para almacenar una cantidad de bitcoins significativa. Las carteras de papel también se consideran de las más seguras, siempre que apliquemos todas las precauciones de seguridad que hemos comentado, y tienen la ventaja de su coste prácticamente nulo, si bien hemos de tener en cuenta que hemos de extremar las precauciones con backups y protección del acceso por parte de otras personas.

Distribuye tus bitcoins entre varias

carteras

Puedes generar varias carteras y distribuir todos tus bitcoins entre ellas, reduciendo el riesgo en caso de que pierdas acceso a una cartera por alguna razón o incluso que alguien malintencionado pueda acceder a alguna de ellas. Además, como ya hemos explicado, todas las transacciones de bitcoins quedan almacenadas en la blockchain para siempre, y si has realizado transacciones importantes a una cartera concreta puede llamar más la atención que si realizas muchas transacciones pequeñas a distintas carteras.

Revisa tus bitcoins periódicamente

Al igual que revisas el estado de tus cuentas bancarias periódicamente, también deberías de revisar tus carteras bitcoins con cierta frecuencia, al menos una vez al mes.

Protege tu información más sensible

Tu clave privada = tus bitcoins. Nunca des acceso a nadie a tu clave privada, en ningún momento. Nunca expongas tu clave privada de ninguna manera, sobre todo electrónica. En un experimento realizado en Estados Unidos, un investigador incluyó su clave privada en una camiseta y salió con ella a la calle.

¿Sabes cuánto tardaron en adueñarse de sus bitcoins? ¡5 minutos! No hagas cosas como almacenar temporalmente tu clave privada en un documento de texto u hoja de cálculo no segura, o fotografiarla con el móvil. Ese documento o fotografía puede acabar en alguna nube que luego ni recuerdas, o en una papelera para archivos eliminados de las que alguien malintencionado puede rescatarla en algún momento.

Cuidado con los servicios dudosos o muy nuevos

Dentro del mundo bitcoin hay ya empresas y servicios web que tienen una trayectoria bastante consolidada, y

además hay multitud de servicios que aparecen continuamente sin que muchas veces sepamos quién está detrás. Algunos de estos podrían ser malintencionados, o simplemente su seguridad no está contrastada. No experimentes con tus bitcoins en servicios poco contrastados.

Planifica para lo peor

¿Qué ocurriría si mañana te pasara algo malo, como un accidente o una enfermedad? ¿Podría tu familia acceder a tus bitcoins? Habla con tu familia para tener un plan de contingencia si algo ocurriera, enséñales cómo localizar los bitcoins y cómo acceder a ellos, y

escribe de alguna manera las instrucciones de este plan por si algo ocurriera.

Unas palabras adicionales

Si has leído todo lo anterior, podrías quedarte con la idea de que los bitcoins no son nada seguros y que protegerlos es muy complicado. Por contra creo que los bitcoins son una moneda bastante segura (más que la de algunos países) si se utiliza adecuadamente y se toman las precauciones correctas. Y lo importante es hacer bien las cosas al principio.

Creo que la práctica totalidad de lo comentado se puede hacer en pocas horas, y una vez que tengas tus bitcoins asegurados, en las carteras adecuadas, con ordenador seguro y con contraseñas fuertes, lo único que tienes que hacer es revisar tus bitcoins y tus backups periódicamente, y pueden permanecer seguros durante muchos años.

7. Invertir en bitcoins

Lo primero a comentar en esta sección es que no es para nada una recomendación sobre si invertir o no en bitcoins, y que no soy una persona cualificada para recomendar o no una inversión. En el caso en el que hayas tomado la decisión de invertir en bitcoins, esta sección pretende darte información sobre cómo hacerlo.

Algunos datos sobre bitcoins

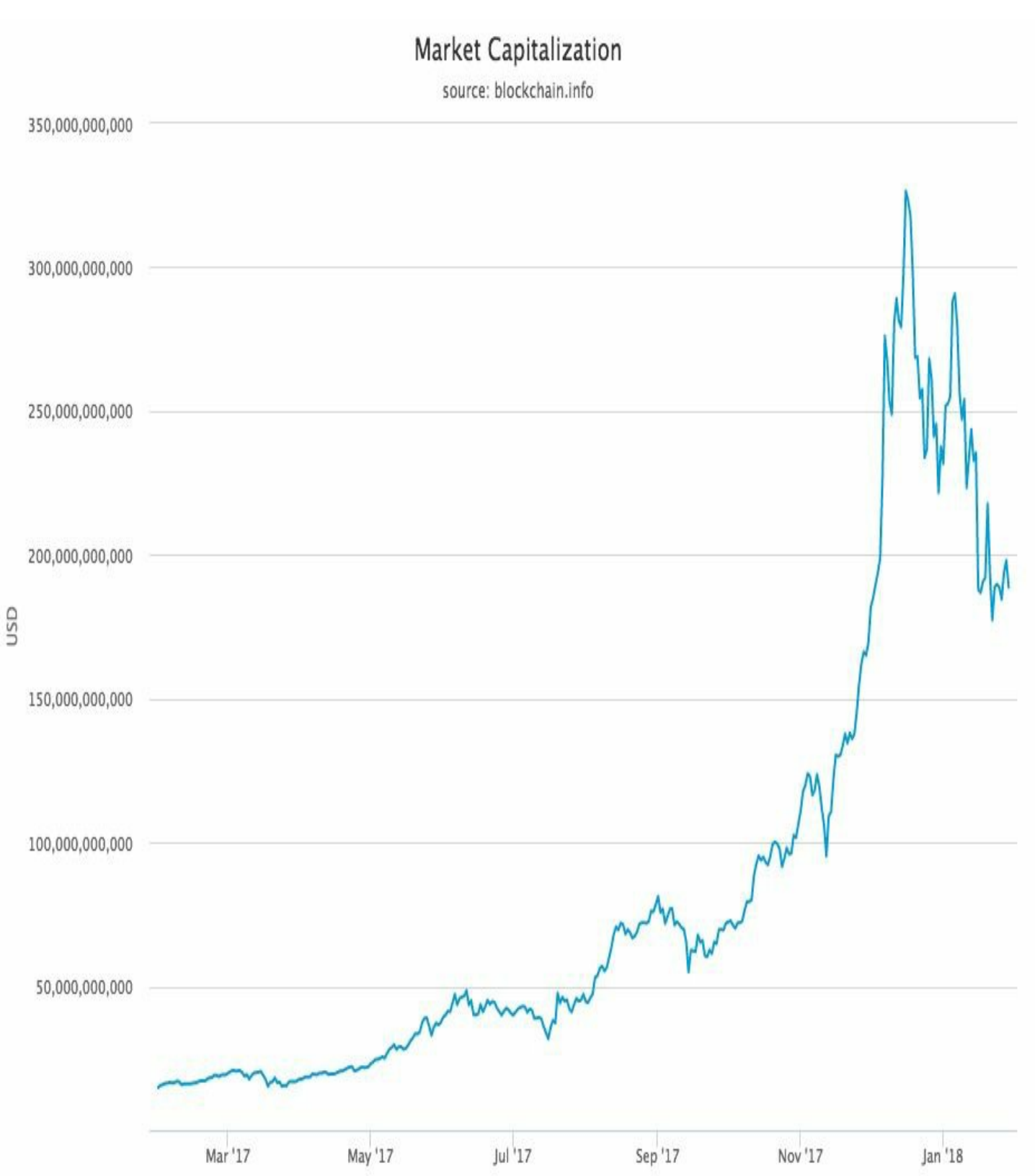
Cuando miramos la evolución del precio de bitcoin, encontramos un aumento muy rápido del precio, si bien también es verdad que la volatilidad (variación del precio en un tiempo determinado) es muy alta, y al igual que ha habido aumentos de precio rápidos, también ha habido varias caídas muy bruscas en cuestión de pocas horas. Se trata de una **inversión de muy alto riesgo**, y si inviertes hoy 1.000 euros en bitcoins, nadie sabe si dentro de 6 meses valdrán 2.000, 200 o inclusive cero. Mi opinión personal es que las personas que han decidido invertir en bitcoins no deberían de invertir nunca más de un 5% de sus ahorros debido al alto riesgo, y por

supuesto nunca invertir el dinero que necesitas para tu vida cotidiana o para tu jubilación.

Veamos algunas cifras sobre bitcoin. A enero de 2018 hay en circulación (por tanto se han generado) alrededor de 17 millones de bitcoins, y el precio del bitcoin se sitúa alrededor de los 9.800 euros. Por lo tanto, el precio de todos los bitcoins en circulación, lo que se conoce como market cap, es de 166.000 millones de euros. Por poner la cifra en perspectiva, si bitcoin fuera una compañía que cotizara en el Ibex 35, sería la mayor por valor de mercado, por encima de compañías bien conocidas como Santander, Inditex,

BBVA, Telefónica e Iberdrola. Pero lógicamente el bitcoin no es una compañía, y una inversión en bitcoins tiene mucho mayor riesgo que en cualquiera de estas compañías consolidadas.

Evolución del market cap de bitcoin entre enero 2017 y enero 2018
(Fuente: blockchain.info https://blockchain.info/)

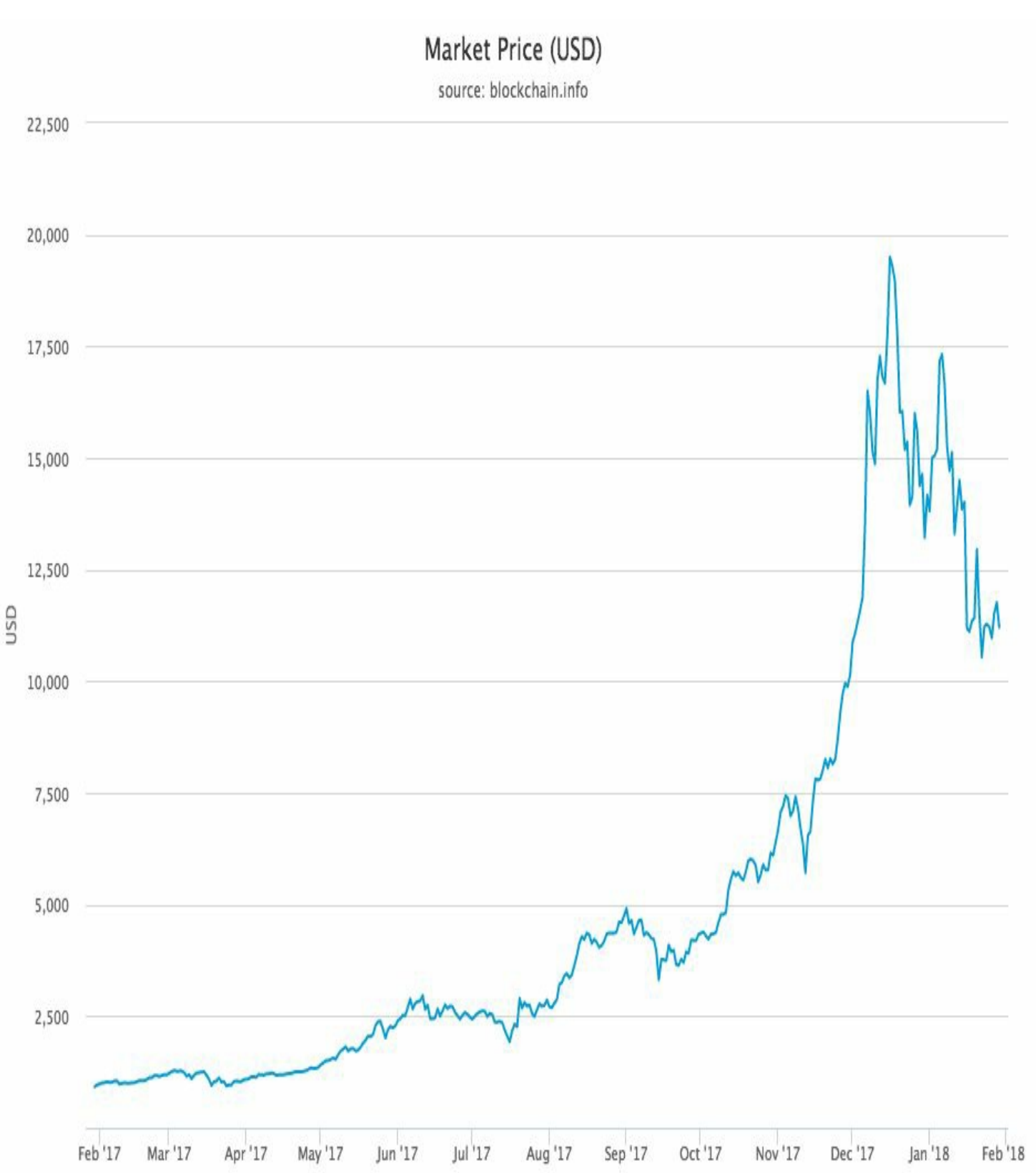


El precio del bitcoin a 1 de enero de 2017 se situaba alrededor de los 950

euros, actualmente el precio es de unos 9.000 euros, es decir que en unos 10 meses se ha multiplicado por 9, una rentabilidad muy elevada, si bien no exenta de riesgo. Por ejemplo, entre el 1 y el 14 de septiembre, el bitcoin pasó de valer 4.150 euros a 2.700 euros, una caída de un 35% en14 días. Nadie sabe si mañana un bitcoin valdrá más que hoy o menos, o si una noticia cataclísmica para esta criptomoneda lo hará valer prácticamente nada. En este sentido no deberías de toma las decisiones de inversión basadas en el criterio de una persona, deberías de aprender sobre este mundo, sacar tus conclusiones y tomar tus propias decisiones.

Evolución del precio de bitcoin entre enero 2017 y enero 2018

(Fuente: blockchain.info https://blockchain.info/)



El número de bitcoins que existirán está

limitado a unos 21 millones, y la asignación de bitcoins por esfuerzo de minería se está dividiendo por dos periódicamente. Este argumento hace pensar a algunos que al ser un recurso relativamente escaso, o al menos limitado en su número, hará que el precio siga subiendo. Si esta teoría se confirma o no es algo que habrá que ver.

Además otra precaución para invertir en bitcoins es que se tratan de una moneda que **no está respaldada ni regulada por ningún gobierno o entidad similar**, a diferencia de las monedas habituales que manejamos que están respaldadas por bancos centrales y economías de países. Un bitcoin vale lo que la gente

percibe que vale, y sabemos que las percepciones pueden variar muy rápidamente. Además, diferentes gobiernos pueden comenzar a regularla, por ejemplo, recientemente China, lo que podría afectar aspectos como la minería de bitcoins, el intercambio de bitcoins, la fiscalidad, entre otros.

Por otro lado, es importante tener en cuenta que mucho de lo que parecen inversiones a priori interesantes en el mundo bitcoin acaban siendo estafas por Internet de una u otra manera. Asegúrate de ser extremadamente cauto con dónde invertir tu dinero, y sobre todo aléjate de esquemas diferentes, que prometen retornos elevados en poco tiempo, y en

los que no veas claro cómo.

Formas de invertir en bitcoins

Hay fundamentalmente cuatro formas de invertir en bitcoins.

Comprar y mantener

La forma más común de invertir consiste en comprar bitcoins a través de un exchange o de otra de las maneras que hemos visto, almacenarlos en una cartera segura, y esperar a que vayan subiendo de valor. Si tu estrategia de inversión es invertir a largo plazo, es

menos importante el valor concreto al que compras, si bien querrás tratar de elegir un momento en el que puedas obtener una revalorización. Algunas personas invirtiendo en bitcoins por primera vez realizan una compra escalonada. Supongamos que quieres invertir 1.000 euros. Comprarías, por ejemplo 200 euros ahora, después otros 200 dentro de, por ejemplo, un mes cuando, o bien los 200 iniciales hayan tenido ya una revalorización, o bien si han bajado en valor cuando hayan llegado a un soporte de valor, y así sucesivamente. Así tus compras se asemejan al precio medio a lo largo de un periodo largo (por ejemplo 6 meses), y no dependen de una subida o bajada

concreta del precio.

Trading

Esta forma de inversión consiste en que intentas comprar los bitcoins a un precio bajo y venderlos a un precio más alto en un periodo de tiempo corto (algunos inclusive a lo largo de un día, lo que se conoce como trading diario). A priori parece una buena aproximación, el problema es que es entre muy difícil e imposible saber en un momento determinado si va a haber una subida o una bajada del precio, con lo que es realmente difícil obtener un beneficio de manera consistente. Por otro lado parte de ese posible beneficio se puede ir en

gastos de transacción e impuestos. Además, en este tipo de actividad están traders profesionales, con gran experiencia y el apoyo de herramientas analíticas y equipos informáticos sofisticados, con lo que no es fácil que sea la manera mejor de invertir en bitcoins.

Invertir en minería de bitcoins

Esta actividad consiste en adquirir equipo informático especializado, conectarlo a la red bitcoin y a un buen abastecimiento muy barato de electricidad y tenerlo funcionando resolviendo puzzles criptográficos por los que la red bitcoin te permite generar

algunos bitcoins. Esta aproximación es muy compleja de utilizar en la práctica con buenos resultados. Por un lado, el consumo de electricidad de esta actividad es enorme, y o bien la obtienes a un precio muy barato (cercano a cero) o es difícil que sea una actividad con la que puedas obtener un rendimiento elevado. Además debes de realizar una inversión importante en equipamiento muy costoso. En general se considera que, salvo que tengas la capacidad de invertir y electricidad casi gratis, es más rentable invertir a largo plazo. En el caso de que desees ir adelante con esta actividad, es aconsejable que mires la opción de los pools de mineros (mining pools) para unir fuerzas (y rendimiento

económico) con otros mineros de tamaño pequeño-mediano. Una variante de esta actividad es el de los servicios web que realizan la minería por ti, y tú les pagas una cantidad al mes, lo que se conoce como minería en la nube (cloud mining). Aunque a priori puede sonar como una idea interesante, hay que ser muy cautelosos con este tipo de servicios. Algunos de ellos son directamente estafas, que cogen tu dinero durante un periodo en el que te pueden ir engañando, y de repente se van. En otros casos de servicios legítimos, no suelen ser tan buenas inversiones, y puede ser más rentable directamente comprar bitcoins o invertir en otros activos, en lugar de pagar estos

servicios.

Invertir en compañías de bitcoins

Otra posibilidad es invertir euros en compañías del ecosistema bitcoin, ya sean compañías de minería, de carteras bitcoin, de intercambio de bitcoins, de desarrollo de aplicaciones bitcoin, etcétera. Hay que tener en cuenta que estas compañías son habitualmente pequeñas, y se trata de inversiones de muy alto riesgo, además de en muchos casos ubicarse en localizaciones cuyo marco jurídico no conocemos. Estas compañías están muy expuestas a todo lo que puede ocurrir en el mundo bitcoin (cambios regulatorios, hackers…), y

algunas son incluso directamente estafas. Hay que ser tremendamente cauteloso con estas inversiones.

8. Otras criptomonedas

Qué son las altcoins

Bitcoin es la principal moneda virtual protegida por algoritmos criptográficos (criptomoneda), así como la primera que ha tenido éxito. Por otro lado, con el tiempo han ido apareciendo muchas otras criptomonedas alternativas, que pretenden mejorar las características y resolver algunas limitaciones del protocolo bitcoin. Son éstas las

denominadas altcoins (“alt” de alternativa).

La mayoría de las altcoins tienen en común un proceso de minería aunque en ocasiones difiere del del bitcoin en algunas aspectos. También buscan una manera **más eficiente, rápida y barata de realizar transacciones**. Algunas buscan **añadir funcionalidades** como la mejora de la privacidad o los llamados contratos inteligentes, que son acuerdos contractuales que pueden ejecutarse automáticamente en la red de criptomonedas, sin intervención humana.

Hay cerca de 1.200 criptomonedas, y

otras nuevas aparecen cada semana. La inversión en criptomonedas pude ofrecer una mayor rentabilidad en menor tiempo que en el caso de bitcoin, pero conlleva un mayor riesgo, a veces mucho mayor, al ser menos usadas y tener un menor valor en agregado. Hay algunas criptomonedas que están relativamente consolidadas, y otras que siguen apareciendo cada semana, a través de un proceso llamado ICO (Initial Coin Offering) que es semejante a cuando una compañía sale a bolsa por primera vez. La nueva moneda crea un documento técnico explicando sus características y ventajas, y las personas e instituciones pueden comprar esta nueva moneda el día de la ICO. La participación en una

ICO tiene un riesgo muy elevado (mucho mayor que invertir en una moneda consolidada, como bitcoin), ya que normalmente tenemos sólo información parcial, y si bien algunas nuevas criptomonedas ganan mucho en su valor rápidamente, otras se quedan en nada y pueden llegar a desaparecer. Se trata de proyectos en muchos casos especulativos, y sin un equipo sólido y una comunidad que los apoye realmente.

Cada mercado o exchange soporta operaciones sólo con algunas de las criptomonedas, las más importantes suelen estar soportadas por la mayoría de exchanges, sin embargo si quieres

operar con algunas criptomonedas de menor relevancia, has de buscar en qué exchanges operan.

Las principales altcoins

A la hora de considerar altcoins, debemos de considerar su valor total, lo que denominamos market cap, resultante de multiplicar el precio de una unidad por el número de unidades disponibles. Si juntamos los market caps de todas las criptomonedas, bitcoin sólo representa alrededor del 50%. La segunda criptomoneda con mayor market cap, representa una cuarta parte del market

cap de bitcoin, y la tercera apenas 1/20 del market cap de bitcoin. He aquí una tabla de las principales criptomonedas por capitalización bursátil:

Top 10 de criptomonedas por market cap en Enero 2018

(Fuente: coinmarketcap https://coinmarketcap.com/)

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$187.179.540.703	$11.118,60	$6.822.250.000	16.834.812 BTC
2	Ethereum	$113.720.579.439	$1.168,79	$3.414.600.000	97.297.701 ETH
3	Ripple	$49.154.548.747	$1,27	$938.872.000	38.739.142.811 XRP *
4	Bitcoin Cash	$27.537.989.495	$1.625,66	$346.520.000	16.939.575 BCH
5	Cardano	$15.401.276.222	$0,594023	$225.932.000	25.927.070.538 ADA *
6	NEO	$10.871.185.000	$167,25	$622.181.000	65.000.000 NEO *
7	Stellar	$10.019.961.227	$0,560762	$117.278.000	17.868.474.017 XLM *
8	Litecoin	$9.819.196.198	$178,58	$279.475.000	54.985.783 LTC
9	EOS	$8.429.154.497	$13,26	$566.007.000	635.606.148 EOS *
10	NEM	$8.042.210.999	$0,893579	$42.119.500	8.999.999.999 XEM *

Vamos a comentar brevemente algunas de las altcoins más destacadas:

Ethereum

Es posiblemente el proyecto más importantes y más desarrollado de criptomonedas altcoin. La moneda virtual en sí se llama Ether. La funcionalidad más característica de esta red de computadores basada en blockchain en la que se pueden construir y ejecutar aplicaciones completas. Esto permite funcionalidades como los smart contracts (contratos inteligentes), aplicaciones que permiten generar contratos que se ejecutan automáticamente en la red. Por poner un

ejemplo, imaginemos un contrato de una empresa que fabrica ropa con un transportista marítimo, en el que se contrata un seguro de que si la mercancía no llega en determinado plazo, ha de pagarse una indemnización. El contenedor de ropa podría llevar un microordenador con un localizado GPS, de manera que si en la fecha indicada el contenedor no ha llegado a destino, la red Ethereum procesa automáticamente la indemnización por parte del transportista al fabricante. Ethereum es un proyecto con una inversión importante y participación de empresas como J.P. Morgan, Microsoft e Intel.

Ripple

Fue originalmente apoyada por Google y algunas instituciones bancarias. Una de sus principales diferencias con bitcoin es que el código fuente es privado (no públicamente disponible). Está muy orientada a transacciones de diferentes unidades de valor (divisas y otras formas de valor), y es empleada por algunos bancos para el procesamiento de sus transacciones internas.

Bitcoin Cash

Moneda resultante del hard fork de bitcoin el 1 de agosto de 2017. Utiliza bloques de hasta 8 Mb (frente a 1 Mb de Bitcoin) lo que permite una mayor

capacidad de procesamiento de transacciones y en general unas comisiones más bajas.

Cardano

Una criptomoneda muy reciente que inició cotización en octubre de 2017, y que ya ha logrado situarse entre las primeras por capitalización. Ofrece mejoras sobre otras criptomonedas en protocolos, lenguaje de programación, mecanismo de consenso entre los nodos, entre otras múltiples mejoras técnicas.

NEO

Conocida en algunos foros como el

bitcoin chino, con funcionalidades avanzadas de contratos inteligentes

Litecoin

Fue creada en 2011 como una alternativa más ligera a bitcoin, centrada en aumentar mucho la velocidad de las transacciones reduciendo el tiempo entre añadido de bloques en la blockchain.

Dash

Se diferencia por transacciones anónimas e instantáneas (menos de un segundo, frente a hasta una hora en bitcoin).

Monero

Pone su énfasis en asegurar la privacidad del usuario, siendo una moneda segura, privada e ilocalizable, ya que utiliza participantes “fantasma” y transacciones aleatorias para enmascarar las transacciones reales.

9. El futuro de bitcoin

Hay diversas razones por las que bitcoin y las otras criptomonedas son y pueden llegar a ser más populares. De alguna manera son el dinero del pueblo, y además un dinero digital. Son verdaderamente abiertas a todos, descentralizadas, globales, y no dependen de ninguna autoridad ni gobierno. Son seguras (bien utilizadas, y teniendo en cuenta que nada es totalmente seguro), prácticamente infalsificables, y son anónimas. Funcionan de una manera totalmente

digital, abren nuevas vías de usos del dinero, y además pueden ser un interesante vehículo para invertir o encontrar refugio al dinero propio. Además se basan en una tecnología, la cadena de bloques (blockchain) que está muy ampliamente reconocida como revolucionaria, y sobre la que ya muchísimas compañías en distintos sectores y gobiernos están invirtiendo e investigando.

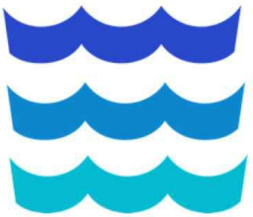
Factores fundamentales en el desarrollo de Bitcoin

Regulación

Fiscalidad

Extensión a personas y usos

Integración



Estabilización del precio

Seguridad

Comisiones

A menudo se compara bitcoin con el oro como posible reserva de valor. El valor de mercado de todas las reservas de oro es de 5 billones de dólares. Por comparativa el valor de mercado de todas las criptomonedas es de aproximadamente 170 mil millones de dólares, unas 30 veces menos. ¿Podrían las criptomonedas crecer hasta

convertirse en algo semejante?

Por mi parte veo tres posibles escenarios que podrían ocurrir: extensión hacia el uso generalizado, utilización en usos concretos o marginalización.

Extensión hacia el uso generalizado.

Se estima que actualmente poco más de 10 millones de personas en el mundo poseen algunas criptomonedas, es decir, apenas un 0,14% de la población mundial. Además las personas que las

poseen las utilizan sobe todo como vehículo de inversión y para intercambio de valor, no para el día a día. El potencial es descomunal. El uso podría ser semejante al dólar pero a una escala aún más global. Hay actualmente unos 13 billones de dólares en circulación, y unos 11 billones de euros en circulación, esto suma unas 140 veces más en valor que las criptomonedas actualmente.

¿Podrían las criptomonedas ocupar a escala global muchos de los usos de las monedas FIAT? Creo que sí, podrían. Creo que podría haber un futuro en el que cobramos la nómina en bitcoins, ahorramos en bitcoins y gastamos en

bitcoins. Además en el internet de las cosas, daríamos permiso a ciertas máquinas inteligentes para gastar el dinero y, por ejemplo, pedir la compra y pagarla por nosotros. Las monedas convencionales creo que seguirían existiendo, tal vez no para siempre. Este futuro tiene una serie de requerimientos:

Regulación (o ausencia de)

Probablemente el elemento más importante que pueda condicionar el futuro de las criptomonedas es la manera en la que sean reguladas por las diferentes autoridades. Si los gobiernos y organizaciones internacionales aprecian las ventajas y el valor

estratégico de las criptomonedas, y establecen un escenario regulatorio razonable, que permita el desarrollo, integrando las criptomonedas en la economía, esto permitirá continuar el desarrollo.

Estamos viendo ejemplos en ambas direcciones. Recientemente Japón admitió a bitcoin como moneda en ese país. La Unión Europea ha definido a bitcoin como moneda. Sin embargo China está limitando por ley el uso de bitcoin, y en el caso de Estados Unidos todavía no hay una postura clara. Creo que un cierto nivel de regulación es deseable para ofrecer mayores garantías legales del uso de las criptomonedas,

sin embargo si vamos a un escenario de regulación exagerada, e incluso limitación o prohibición del uso, el desarrollo de las criptomonedas se verá fuertemente cercenado. Sin embargo no podemos perder de vista que las criptomonedas suponen una amenaza para el status quo tanto de gobiernos como de organizaciones financieras. Si el foco está en la amenaza, es posible que la resistencia resulte en regulaciones muy desfavorables.

Fiscalidad

Muy relacionado con el anterior está el aspecto de la fiscalizad de las transacciones en bitcoins. Esto depende

mucho de su consideración legal. Si bitcoin es una moneda legal equiparable a la moneda nacional, a priori no debería de aplicarse una fiscalizad diferente a, por ejemplo el euro. Por otro lado, si bitcoin se considera moneda "extranjera", podría aplicarse una fiscalizad equivalente a la de las inversiones en moneda extranjera, tasando los incrementos de valor de esta inversión financiera. En un tercer escenario, si bitcoin se considera un activo que no es una moneda, la situación puede ser más compleja, será similar a una inversión en acciones, por ejemplo. En el segundo y tercer escenario se podría ir a una fiscalizad con poco sentido, en la que cada vez que

“vendemos” bitcoins al comprar algo con precio en moneda local, es necesario pagar un impuesto por la revalorización del bitcoin respecto a la moneda local, algo que sería tremendamente poco práctico para un uso diario.

Extensión a más personas y utilizaciones

Estamos todavía en un momento relativamente temprano de la tecnología de criptomonedas, que algunos analistas establecen como la transición entre la adopción por pioneros y los adoptadores tempranos (early adopters). Es necesario que más y más personas

conozcan y se acerquen a las criptomonedas. Esto es algo que veo ya ocurriendo en nuestro medio. Y además creo que todavía no hemos llegado al momento de explosión en la adopción de las criptomonedas. También creo que las tecnologías de este ecosistema deben de buscar la manera de simplificarse para acercarse al usuario no tecnológico. En ese respecto aún queda trabajo por hacer. En cuanto a los posibles usos, actualmente son pocos los lugares del mundo real en los que se puede utilizar esta criptomoneda. Algunas tiendas muy puntuales, y algunos usos particulares que algunas personas o instituciones ponen a disposición, desde comprar vivienda a

servicios de todo tipo.

Estabilización del precio (o mecanismos de compensación)

La gran fluctuación en el precio de bitcoin, que puede llegar en un día al 10% del valor, en ocasiones inclusive más, lo que dificulta la propia utilización de la moneda para usos convencionales. Si el precio habitualmente se establece en euros, imaginemos unas zapatillas de deporte que ahora mismo cuestan 100 euros, que serían 0,02 bitcoins si 1 bitcoin = 5.000 euros. El problema es que si mañana el bitcoin sube un 10%, esos 0,02 bitcoins esas zapatillas cuestan 110 euros, y si

baja un 10% cuestan 90 euros. Una fluctuación posible de un 20% en este ejemplo.

Esto puede asemejar a situaciones de inflación muy elevada en países en desarrollo, y supone, por ejemplo en esos casos, un incentivo para gastar hoy y no ahorrar, ya que mañana ese dinero que hoy no hemos gastado valdrá menos. En el caso de revalorización continuada del bitcoin supone de hecho lo contrario. ¿Para que voy a comprarme hoy las zapatillas con mis 0,02 bitcoins, si el mes que viene puedo comprar con esos mismos bitcoins bastante más? Otra opción es que el precio no se estabilice tanto, pero existan vehículos financieros

que nos permitan compensar esa fluctuación, por ejemplo aplicando cambios medios en periodos de tiempo, o protegiendo de las fluctuaciones excesivas del precio.

Integración (sistemas de pago, etc.)

Otra necesidad es la integración del bitcoin en la economía convencional, de manera similar a como ahora funcionamos con cuentas bancarias y tarjetas, y esto tiene más complicaciones de las que parece a priori. Ya hay empresas que han desarrollado sistemas de pago sencillos con bitcoins para comercios, así como otras que permiten pagar con tarjetas de euros pero

ocurriendo el pago en bitcoins. Sin embargo estas soluciones todavía están muy poco extendidas. Actualmente demás los tiempos de procesamiento de transacciones en la red bitcoin son de unos minutos, una hora o inclusive más a veces, dificultando el uso en aplicaciones de pago en tiempo real, si bien también se están desarrollando ya soluciones en este sentido. Más allá de comercios, no disponemos aún de un sistema sencillo y extendido semejante a las domiciliaciones de recibos para nuestros pagos, y tampoco para, por ejemplo, impuestos.

Garantizar la seguridad

La seguridad del protocolo bitcoin es, hoy por hoy, elevadísima, y la mayor garantía del funcionamiento adecuado de los bitcoins y la red. Es mucho más fácil hoy en día falsificar cualquier moneda fiat que una criptomoneda, de hecho las criptomonedas se consideran a día de hoy prácticamente infalsificables. Esto hace que la tecnología de cadena de bloques o blockchain se está extendiendo a muchas otras aplicaciones desde bancarias a registros de la propiedad.

Otra cosa es la manera en la que usamos los bitcoins. La página web de algunos servicios de intercambio (exchanges) sí ha sido hackeada, y en algunos casos

cantidades muy importantes de bitcoin han sido robados. Estos bitcoins no han sido robados en la red bitcoin, sino en el sistema informático del exchange. Otras veces carteras de bitcoin poco seguras han sido hackeadas, en general a través del ordenador del usuario, accediendo el hacker a las claves privadas y permitiendo robar los bitcoins de esa persona. Lo que quiero comentar es que mientras que la red es muy segura, lo que ocurre fuera de esa red tiene los mismos retos de seguridad que cualquier otro sistema en el que las personas y los ordenadores están presentes. Por un lado es, por tanto, deseable que la seguridad de todo el ecosistema bitcoin se continuó viendo revisada, que los

usuarios estemos más educados en estos aspectos, y que además mantener nuestra moneda segura sea cada vez más sencillo. Por otro lado sería deseable algún sistema de protección tanto legal como financiera de nuestros bitcoins para los casos de ciber-crimen.

Comisiones muy reducidas

Hemos comentado que, a día de hoy, una de las ventajas es que las comisiones por transacciones en la red bitcoins son muy reducidas, e independientes del importe. Esto es una ventaja importante cuando estás, por ejemplo, transfiriendo bitcoins a alguien en otro país u operando con cantidades elevadas de

bitcoins. Sin embargo para un uso diario con muchas transacciones pequeñas, estas comisiones ya no resultan tan reducidas. Más aún, si sobre una transacción sencilla hemos de añadir comisiones por otros servicios, por ejemplo el cambio de bitcoins por divisas locales, el pago con tarjeta, la transacción instantánea, protección frente a volatilidades muy altas en el valor, funcionalidades de cartera de bitcoin, etcétera, las comisiones pueden llegar a ser muy elevadas, en total divergencia con la filosofía del bitcoin. Es por eso que para un escenario de uso muy extenso, deben de revisarse todas estas comisiones y que sean tan mínimas que permitan el uso diario en muchas o

todas las aplicaciones.

Utilización en usos concretos

En este escenario las utilidades de los bitcoins se ampliarían, pero focalizada en algunas aplicaciones, no como moneda universal para todos los usos. De los aspectos comentados en el punto anterior, para que esto ocurra sería necesario un escenario regulatorio y fiscal razonable, que diera entidad jurídica clara a bitcoin, idealmente como moneda que es, y una fiscalizad en línea. Además sería necesario al menos un mantenimiento de la seguridad y que

las comisiones de operaciones continúen siendo reducidas. Las principales aplicaciones para las que creo que se podrían desarrollar son:

Transacciones internacionales

Para mí una de las posibilidades más sólidas de uso de las criptomonedas. Millones y millones de personas han de emigrar a otro país para realizar un trabajo, ganar un dinero, y enviar una parte significativa de ese dinero de vuelta a casa para poder mantener a su familia en el país de origen. Estos envíos de dinero, muchas veces a través de grandes empresas multinacionales, origina un elevado coste, que puede ser

de hasta un 10% del valor del importe enviado, lo que resulta sumamente gravoso en esas circunstancias de necesidad. El utilizar bitcoin para estas operaciones permite realizar este envío de manera rápida, segura y con un coste muy reducido.

En otras ocasiones las personas han de realizar una transferencia de dinero a otro país por diferentes motivos, por ejemplo para pagar una vivienda vacacional, unos estudios, adquirir un bien o servicio, infinidad de posibilidades. Las transferencias bancarias internacionales sabemos que ofrecen esta posibilidad si bien con unas comisiones elevadas y unos tiempos de

ejecución que pueden llegar a una semana, además de la información que hay que intercambiar (nombre completo, número de cuenta, SWIFT…). Esto mismo puede realizarse en minutos de manera sencilla y menos comisiones con bitcoin.

A un nivel más institucional, creo que cada vez las transferencias de dinero entre empresas ubicadas en diferentes países se realizará por esta vía, ofreciendo las ventajas comentadas de mayor rapidez, y menores comisiones. Si las empresas deciden mantener una parte de sus activos en bitcoins, la necesidad de muchos cambios de divisa llegaría a desaparecer, de tal manera

que bitcoin podría ser el eje de valor de muchas de las operaciones de las multinacionales.

Activo para inversión a medio-largo plazo

Actualmente se trata de uno de los usos más habituales (sino el más habitual) de bitcoin. Personas y organizaciones invierten en bitcoins como inversión a medio o largo plazo. Esta circunstancia ya está ocurriendo, y podría expandirse más. Cada vez son más los bancos de inversión que plantean a sus clientes destinar una parte de sus inversiones a bitcoins y otras monedas virtuales. Cada vez son más las personas que están

comprando bitcoins, y el potencial aquí es enorme, habida cuenta de que se estima que únicamente alrededor de un 0,15% de las personas tiene una cartera para criptomonedas. Por otro lado están comenzando a surgir iniciativas de fondos de inversión y vehículos financieros semejantes que invierten en bitcoin y otras monedas, lo que a priori tiene algunos inconvenientes pero también ventajas como un contexto más regulado que facilita la inversión por parte de grandes actores financieros como grandes planes de pensiones e inversores institucionales.

Vehículo para inversión a corto plazo

Bitcoin posee una volatilidad muy elevada, pudiendo su valor fluctuar en un día concreto desde un 5 a un 30% y más. Muchísimo más elevada que la mayoría de activos financieros. Esto genera oportunidades interesantes para inversores que buscan comprar en momentos relativamente bajos y vender en momentos altos en plazos muy cortos de tiempo, a menudo dentro de un mismo día. La posibilidad de obtener muy buenos retornos existe, lo que creo es que no es nada fácil saber en qué momento comprar y vender. Por otro lado la llegada a este mercado de inversores más sofisticados, hace muy complicado obtener un beneficio de ella. Por otro lado, considero que al irse

produciendo la maduración de esta moneda, la volatilidad se irá poco a poco reduciendo.

Moneda refugio

El hecho de poder poseer una cantidad elevada de dinero únicamente con un código que podemos escribir en cualquier pequeño trozo de papel, es una gran ventaja cuando la comparamos con almacenar cantidades de billetes en algún lugar físico. Nos referimos a sistemas políticos y financieros en situaciones difíciles, en los que puede haber limitación a los depósitos y retiradas bancarias, restricciones al cambio de divisas, o incluso riesgos de

confiscaciones. Imaginemos otras situaciones en las que las personas perciben un riesgo de tener que abandonar su lugar de residencia, y la ventaja que aporta el que simplemente llevando ese código escrito en cualquier lugar, podemos movernos entre países y seguir llevando nuestro dinero, sin tener que recurrir a otras formas más arriesgadas como esconder billetes o joyas. También posee la ventaja de poder realizar transacciones sin intermediación por parte de ninguna entidad financiera. Un particular y otro pueden realizar transacciones simplemente intercambiando la clave pública y verificando en webs de transacciones de bitcoin que se ha

realizado unos minutos después.

Donaciones

Como vehículo para donación a ONGs y otras causas, bitcoin ofrece la ventaja de transferencias internacionales sencillas, rápidas y con comisiones bajas. Para muchas causas otra gran ventaja es la anonimicidad (relativa), comparada con tener que introducir nuestra información completa para una transferencia bancaria o un pago con tarjeta.

Backbone de criptomonedas

Hay más de 1.000 criptomonedas en existencia y bitcoin es con diferencia la

dominante. Más del 55% del valor de todas las criptomonedas en existencia corresponde a bitcoin. Esta posición de claro liderazgo hace que, por ejemplo, cuando se lanza una nueva criptomoneda, las aportaciones de dinero para la Inicial Con Offering (ICO) se realizan mayoritariamente en bitcoins, más que en moneda fiat u otras criptomonedas. Adicionalmente, en varios servicios de intercambio de criptomonedas (exchanges) no puedes, por ejemplo, utilizar euros directamente para comprar criptomonedas, sino que has de utilizar bitcoins. Además en pocos casos puedes hacer compra-venta de distintas criptomonedas directamente, sino que has de pasar por una

conversión a bitcoin.

Marginalización de bitcoin

Un tercer escenario es la reducción progresiva del uso de bitcoin hasta la casi desaparición. Estamos en un punto de desarrollo de las criptomonedas en el que cada vez un mayor número de personas (si bien todavía minoritario) conoce las criptomonedas, invierte en ellas y comienza a entender las ventajas que aportan. Adicionalmente los gobiernos, bancos y muchas empresas tecnológicas cada vez conocen más y mejor bitcoin y están estableciendo

marcos regulatorios y operativos que integran las criptomonedas. Más allá incluso, estas mismas organizaciones ya están invirtiendo tiempo y recursos para desarrollar soluciones basadas en cadena de bloques (blockchain) para diversas aplicaciones internas, ya que consideran que esta tecnología puede ser revolucionaria para muchas aplicaciones. Por tanto creo que para llegar a este escenario deberían de ocurrir tres tipos de acontecimientos:

Prohibición legal efectiva en la mayoría de países clave

Consistiría en la prohibición de la utilización o el intercambio de bitcoin

en Estados Unidos, Europa, Japón. Esta prohibición claramente alejaría a los inversores institucionales de la criptomoneda, y además haría que muchas personas que poseen bitcoins los vendieran para regularizar su situación legal. En este contexto el precio del bitcoin caería fuertemente, así como el número de usos y usuarios. Probablemente esto también llevaría a una fuerte reducción en el número de equipos conectados a la red Bitcoin. Creo que incluso en este contexto tan restrictivo, bitcoin no desaparecería, y que en algunos países se seguiría utilizando, así como para ciertos usos. En el momento actual la probabilidad de este acontecimiento creo que es muy

baja, ya que la tendencia apunta en la dirección contraria salvo en algún país como China.

- En Japón, bitcoin ha sido legalmente categorizado como medio de pago desde el 1 de Abril de 2017.
- En Europa el Banco Central Europeo ha clasificado a bitcoin como una moneda virtual descentralizada, y la Unión Europa ha declarado oficialmente que el IVA no es aplicable cuando hacemos conversión entre euros y bitcoin lo que, de alguna manera, lo define como moneda y no como un activo no financiero. Hay algunas

señales de que la Unión Europea se moverá legislativamente para regularizar la utilización de bitcoin mientas extiende algunas medidas anti-lavado de dinero y para evitar el uso con fines criminales.

- El caso de Estados Unidos es menos claro, ya que el Tesoro clasifica bitcoin como una moneda virtual descentralizada pero la hacienda estadounidense (IRS) lo clasifica como una propiedad. También hay alguna señal de que el gobierno americano va a adoptar medidas legislativas, posiblemente en favor de la regularización como moneda, a la vez aumentando las garantías para inversores y de anti-

lavado de dinero y uso criminal.

- En el extremo prohibicionista, en septiembre de 2017 el gobierno chino prohibió la actividad de los servicios de intercambio (exhanges) en su territorio y limitó el intercambio de bitcoins, además de las Initial Con Offering (ICOs)

Crisis de seguridad

Este acontecimiento se desencadenaría por el hackeo del protocolo o de la red de bitcoin, lo que convertiría a bitcoin en poco seguro. Si esto ocurriera a gran escala, sería el acontecimiento brusco que creo que podría amenazar más a la

criptomoneda. Seguramente una modificación del protocolo podría solventar esta circunstancia, pero la pérdida de confianza llevaría a muchas personas e instituciones a dejar de participar en la criptomoneda, y a perder confianza en sus posibilidades. Creo que la probabilidad de que esto ocurra es muy baja, el protocolo de bitcoin se basa en los algoritmos más seguros conocidos, investigados y atacados durante décadas sin éxito. Además a día de hoy no se conoce ningún ataque a nivel de protocolo o red con éxito, y seguro que ha habido innumerables intentos. En todo caso no podemos excluir que pueda ocurrir como posibilidad.

Abandono de los usuarios

Este último acontecimiento vendría en el caso en que, sin existir una crisis de seguridad ni una prohibición legal, los usuarios van dejando de lado bitcoin, bien porque no perciben un gran desarrollo de las aplicaciones de la criptomoneda, bien porque ya no les resulta una inversión atractiva, bien porque surgen otras alternativas más ventajosas. De acuerdo con las tendencias actuales, este escenario no me parece probable en absoluto. Siendo todavía conocido por una minoría de la población, las ventajas de bitcoin están haciendo que su uso se esté extendiendo

de manera progresiva, y que muchas más personas se acerquen a bitcoin como una criptomoneda alternativa a su moneda habitual. A nivel institucional hay un interés creciente por bitcoin. Y, si bien es cierto que bitcoin podría ser reemplazada por otras criptomonedas alternativas, hoy por hoy es la referencia, el estándar, el patrón oro de las criptomonedas, y aunque veo un lugar para otras criptomonedas, no veo que la dominancia de bitcoin se vaya a ver reducida.

Epílogo

Bitcoin tiene **los elementos para convertirse en una moneda de referencia a nivel internacional.** Es independiente de cualquier gobierno o autoridad financiera, es segura, relativamente anónima, está distribuida por todo el mundo, la posesión implica simplemente conocer un código, y ubicua, pudiendo almacenarse o llevarse en el móvil o incluso en el reloj. Veo un futuro en el que bitcoin reemplaza las monedas que utilizamos a diario para muchos usos, quizás incluso para la mayoría de los usos.

También veo a personas y organizaciones no creyendo en esta posibilidad, diciendo que es una burbuja, que no va a ir a ningún lado, y que si bien la tecnología de cadena de bloques (blockchain) es muy interesante (creo que ya nadie niega que blockchain, como tecnología, va a revolucionar muchas aplicaciones del mundo financiero y legal), lo que acabará habiendo son criptomonedas tal vez de un país en particular o aplicaciones de la cadena de bloques privadas. Y cuando escucho este tipo de declaraciones, también percibo cierto miedo, de **algo disruptivo que cambie el mundo de las finanzas para siempre**, y tal vez las compañías de este sector no

sepan o no puedan adaptarse. Y esto ha ocurrido y está ocurriendo ya muchas veces en otros sectores. En el sector editorial (¿dónde están las librerías?), en el sector audiovisual (¿qué es un cd?), en la prensa, en la televisión, en la distribución comercial, y en un largo etcétera. Algunas empresas han sabido adaptarse al cambio y han prosperado, otras no se han adaptado y han desaparecido.

Cuando pienso en esto, pienso en los paralelismos con Internet. Una red independiente de cualquier gobierno o autoridad, relativamente segura, relativamente anónima, distribuida por todo el mundo, y ubicua hasta el punto

de que prácticamente cualquier objeto, desde luego relojes, pueden conectarse a ellas. Las similitudes son tantas que recientemente ha aparecido un libro sobre bitcoin y otras monedas alternativas titulado “El Internet del dinero”.

Vayamos aún un paso más allá. Una parte del futuro vendrá de lo que se viene llamando el Internet de las Cosas (Internet of Things en inglés, abreviado IoT). Los objetos cotidianos se irán conectando entre sí y a sistemas que les dotarán de nuevas capacidades y de ciertas formas de inteligencia artificial. Por ahora son luces y persianas conectadas, y ya electrodomésticos a los

que podemos dar instrucciones a distancia, o frigoríficos que pueden llegar a detectar lo que tienen dentro, y pedir directamente la compra de manera automática cuando empieza a escasear algún alimento. Un paso más allá serán los coches autónomos y conectados. Y más allá las casas inteligentes, wearables, y muchas otras aplicaciones que aún no somos capaces de anticipar.

Muchas de estas aplicaciones requerirán de pagos entre esos mismos objetos que interactúan entre ellos, muchas veces en forma de micro pagos. Por ejemplo, la electricidad podría ser pagada según es consumida de tal manera que los electrodomésticos ajustaran sus

actividades en función de las tarifas. Los coches eléctricos podrían recargarse mientras esperan el semáforo en rojo a través de instalaciones de carga bajo el pavimento. El frigorífico podría hacer la compra, que sería entregada inmediatamente por un dron, y un autómata colocaría esa compra en la nevera. Bitcoin podría ser, no sólo la moneda preferente para muchas aplicaciones que requieren intercambio de valor entre personas, sino que estaría perfectamente adaptada para este intercambio de valor entre máquinas. Y éste es, probablemente un futuro mejor a nuestro presente, y hacia el que nos dirigimos.