Equipo Fintech
6 de junio de 2017

Monederos bitcoin: cómo almacenar bitcoins de forma segura

A la hora de plantearnos comprar y utilizar bitcoins surgen muchas dudas. Una de ellas es cómo almacenar nuestros bitcoins de forma segura. Esta necesidad es cada vez más imperiosa, si tenemos en cuenta que el precio del Bitcoin no ha parado de subir a lo largo del último año.

En este momento (07/06/2017), según el Índice del precio de Bitcoin de CoinDesk, **el precio de un bitcoin es de 2.845 USD**, **habiendo duplicado su valor en los últimos 30 días**, por lo que mantener nuestros bitcoins a buen recaudo es, sencillamente, fundamental.

Para ello, **necesitaremos un "monedero bitcoin"** (*bitcoin wallet*). No obstante, elegir el más adecuado no siempre es sencillo. No solo hay distintos monederos, sino también **distintos tipos** de monederos, cada uno de ellos **con sus ventajas e inconvenientes.**

En este informe te explicamos todo lo que debes saber al respecto.

Antes de nada es fundamental entender qué es exactamente lo que debemos proteger y almacenar en los denominados monederos bitcoin.

¿Nuestros bitcoins? No exactamente.

¿Qué guardamos en un monedero bitcoin?

Pues básicamente, nuestras **claves criptográficas**. Para usar bitcoins necesitamos un par de claves criptográficas, formado por **una clave pública y otra privada**.

La **clave pública** o dirección bitcoin (*bitcoin address*) es la que daremos a los demás usuarios para que nos transfieran bitcoins. Cualquiera puede verla y no requiere protección, dado que únicamente sirve para recibir bitcoins.

La **clave privada**, en cambio, es la que necesitamos para poder hacer uso de nuestros bitcoins. Si queremos realizar un pago en bitcoins, debemos confirmar la transacción con nuestra clave privada, por lo que es fundamental guardarla en un lugar seguro.

En la siguiente imagen se puede ver un **ejemplo de clave real** (combinación de números y letras). Se trata de la clave pública de The Bitcoin Foundation:

Es importante recalcar que cada clave pública tiene asociada una clave privada única y juntas forman un par, de manera que los bitcoins transferidos a una clave pública solo se podrán gastar utilizando la clave privada del mismo par.

Podemos tener más de un par de claves. De hecho es recomendable que así sea por seguridad.

De ese modo, si una de nuestras claves privadas se ve comprometida, solo podríamos perder los bitcoins asociados a su par, mientras que los asociados a otros pares de claves permanecerían a salvo.

En conclusión, los monederos bitcoin guardan pares de claves criptográficas y lo que se debe proteger, especialmente, son las claves privadas.

Por seguridad también **conviene tener más de un monedero bitcoin**. A continuación veremos por qué.

Creación y transmisión de bitcoins

Como describimos en el informe "La tecnología Blockchain en el sistema Bitcoin", solo se crean **nuevos bitcoins** como recompensa a los mineros.

Para ello, se registra en la cadena de bloques su creación y, justo a continuación, su transferencia a la clave pública del minero al que se quiere recompensar.

Posteriormente, dicho minero solo podrá **transferirlos** a otro usuario utilizando su clave privada correspondiente y poniendo como destino la clave pública del destinatario. Y así sucesivamente.

No obstante, es importante recalcar que la moneda no se "mueve", ni se "guarda" literalmente en ningún sitio, **solo se "registra" su creación y el traspaso de su propiedad de una clave a otra en la cadena de bloques** (el libro de contabilidad de Bitcoin).

Para facilitar su uso, es habitual generar un **código QR** a partir de la clave pública (imagen anterior). De ese modo, si alguien quiere enviar bitcoins a nuestra dirección pública no necesitará teclear uno a uno todos los caracteres de la clave, sino que bastará con que ponga su móvil sobre el código QR y confirme la transacción.

¿Y si alguien pierde su clave privada?

Pues, básicamente, **perderá todos los bitcoins asociados a ella** en la cadena de bloques. De ahí la enorme importancia de ponerla a buen recaudo.

¿Qué sucede entonces con esos bitcoins?

- Si la clave privada ha sido robada o la hemos perdido y alguien la encuentra, la persona que tenga la clave en su poder podrá hacer uso de dichos bitcoins.

- Si el problema es que hemos olvidado nuestra clave privada o ha sido destruida de algún modo (incendio, inundación, etc.), nadie podrá volver a hacer uso de los bitcoins asociados a ella nunca.

Tipos de monederos bitcoin

Existen múltiples tipos de monederos bitcoin, muy diferentes entre sí y con interesantes ventajas e inconvenientes.

Desde el punto de vista del **medio de almacenamiento** pueden ser:

- **Físicos:** desde una hoja de papel (*paper wallet*) en la que anotaremos el par de claves, a dispositivos de hardware específicos para su uso como monedero bitcoin.

- **Virtuales:** desde un archivo de texto con la clave almacenada en nuestro ordenador, a diversos software especializados, en forma de apps para móviles, aplicaciones web o aplicaciones de escritorio.

Otra clasificación importante desde el punto de vista de la **seguridad** es la que distingue entre:

- **Monederos "calientes"** (*hot wallets*): aquellos con conexión a Internet. En general, son más accesibles pero menos seguros.

- **Monederos "fríos"** (*cold wallets*): sin conexión a Internet. Son más seguros, pero menos accesibles a la hora de querer utilizar las claves para realizar una transacción a distancia.

Debemos pensar en los **monederos calientes** como en una cartera que llevamos con nosotros. Por su gran accesibilidad e inmediatez, son ideales para las operaciones del día a día, pero no son seguros, por lo que **no debemos acumular en ellos mucho dinero**, del mismo modo que no saldríamos a la calle con demasiado dinero en la cartera.

Lo ideal es tener a mano cierta cantidad de criptomoneda en un monedero caliente para el día a día, pero poner el **resto de nuestros bitcoins a buen recaudo en monederos fríos**.

A continuación, se analizan las ventajas e inconvenientes de cada tipo de monedero.

1. Monedero de papel

Es el más básico y rudimentario. Puede ser desde cualquier papel en el que anotamos el par de claves a algo más específico como el papel impreso con códigos QR que se puede ver en el siguiente vídeo:

Hay diversas páginas web que facilitan la creación de este tipo de monederos.

Ventajas:

- Para uso diario, podemos tenerlos siempre a mano y llevarlos encima como si se tratara de billetes en una cartera.
- Son muy cómodos y fáciles de utilizar: para recibir dinero basta con enseñar el código QR de la clave pública y para pagar, utilizar el código QR de la clave privada.
- También se pueden utilizar como monedero frío, si se pone el papel a buen recaudo, por ejemplo, en una caja fuerte.

Inconvenientes:

- Podemos perderlo o nos lo pueden robar fácilmente si lo llevamos de paseo.
- Se puede destruir fácilmente: si se moja, en caso de incendio, etc.
- Debemos calcular de manera manual cuánto dinero tenemos en él en cada momento.

2. Archivo de texto almacenado en nuestro ordenador

Es uno de los monederos más fáciles de crear y resulta muy práctico para realizar operaciones digitales, pero **no permite calcular fácilmente la cantidad de bitcoins que contiene y solo será seguro en la medida en que también lo sea nuestro ordenador.**

Esto dependerá, básicamente, de si está conectado a Internet (monedero caliente) y de nuestros conocimientos informáticos.

Si el ordenador está conectado a Internet, podremos utilizar las claves en operaciones con un simple “copia y pega”, pero siempre existirá el riesgo de que sea hackeado. En este caso, sería recomendable encriptar el archivo o el directorio que lo contiene para proteger las claves de posibles ataques externos.

En cambio, **si el ordenador no está conectado a Internet** (monedero frío), será más seguro, pero no tendremos la clave tan a mano cuando la queramos utilizar.

Además, aún sin conexión a Internet u otro tipo de red, alguien con acceso a la habitación física en la que se encuentra el ordenador, podría lograr acceder a él y hacerse con las claves, dependiendo de la seguridad de nuestro ordenador y de cómo hayamos protegido el archivo.

Por otra parte, al igual que en el caso del monedero en papel, el ordenador podría verse dañado por alguna catástrofe, como un incendio o una inundación; o verse afectado por un virus u otro tipo de malware.

3. Archivo almacenado en un pen

Es similar al caso anterior, pero algo más práctico y seguro.

Por una parte, podemos llevarlo con nosotros en caso necesario y, por otra, es más fácil de esconder (por ejemplo, se podría guardar en una caja fuerte en caso de querer utilizarlo como monedero frío).

También es fácil de utilizar, dado que en caso de querer realizar una transacción, basta con conectarlo a un ordenador con conexión a Internet durante unos minutos.

Obviamente, mientras esté conectado a Internet habrá riesgo, pero al ser un período de tiempo muy corto el riesgo se minimiza en comparación con otras opciones como un móvil o un ordenador conectados a Internet permanentemente.

En cualquier caso, siempre se pueden encriptar los datos.

En cuanto a sus inconvenientes, al igual que en los casos anteriores, tendremos que calcular manualmente la cantidad que nos queda asociada a dicha clave a medida que vamos gastando o recibiendo dinero; y si se daña la memoria del dispositivo, podríamos perder su contenido.

También podríamos perder el pen o alguien podría robárnoslo.

4. Aplicación de escritorio

Existe una **amplia variedad de programas de escritorio para Mac, Linux y / o Windows, diseñados específicamente para ejercer de monederos bitcoin**. Su principal ventaja es que nos facilitan enormemente la gestión de nuestros bitcoins y la realización de transacciones con ellos, a través de sencillas interfaces gráficas.

En este sentido, su uso es similar al de una aplicación de banca en línea en la que podemos ver nuestro saldo y realizar transferencias indicando simplemente la cantidad a transferir y la dirección bitcoin (clave pública) de destino.

En este caso, **la seguridad de las claves estará ligada a la de nuestro ordenador** y, una vez más, dependerá, en gran medida, de si está conectado o no a Internet.

5. Aplicación móvil

Similar al anterior, pero con la facilidad que ofrece poder llevarlo encima.

Al igual que el anterior, el monedero móvil nos permite gestionar nuestros bitcoins de forma sencilla a través de la interfaz gráfica de la aplicación y es **ideal para pagar en tiendas físicas como si fuera una tarjeta de débito**.

Una vez más, **la seguridad dependerá de la del propio dispositivo,** dado que podríamos perder el móvil o alguien podría robárnoslo, podrían acceder a nuestro dispositivo ya sea físicamente o de manera remota a través de Internet y hacerse con las claves o bien podría dañarse el dispositivo por una caída, fuego o agua.

Es **ideal para llevar encima una cantidad reducida de criptomoneda** y utilizarla en las operaciones del día a día, pero no conviene acumular en ellos cantidades importantes de bitcoins.

6. Aplicación web

Hay muchos monederos web disponibles.

Son **similares a los monederos móvil o de escritorio, pero en la nube**, es decir, no requieren ningún tipo de instalación y podremos acceder a ellos a través del navegador desde cualquier dispositivo con conexión a Internet.

La primera vez tendremos que registrarnos y, posteriormente, accederemos con nuestro nombre de usuario y contraseña.

La principal diferencia con los anteriores es que, **en la mayoría de estos monederos, confiamos la custodia de nuestras claves a la empresa que gestiona la aplicación web** y su seguridad dependerá, básicamente, de la seguridad de los servidores de dicha empresa.

Al igual que el anterior, es muy práctico para realizar operaciones habitualmente, pero aunque muchas de estas empresas almacenan gran parte de los fondos en monederos fríos, **no se recomienda acumular en ellos grandes cantidades de criptomoneda**.

Es importante destacar que en caso de hackeo de sus servidores, la empresa no tendrá ningún tipo de responsabilidad al respecto y podría desentenderse por completo.

Además, el dinero almacenado en estos monederos tampoco está asegurado por ningún fondo de garantías, por lo que en caso de que el atacante se hiciera con las claves privadas almacenadas en ellos, podríamos perder todos los bitcoins asociados a ellas.

7. Dispositivo de hardware específico

Existen algunos dispositivos de hardware diseñados específicamente para ser utilizados como monederos bitcoin, por lo que resultan muy interesantes y son **más seguros que otras opciones**.

En general, se trata de dispositivos pequeños, por lo que resultan fáciles de transportar y de guardar a buen recaudo; y solo se conectan a Internet para realizar algún pago o transferencia con criptomoneda.

A diferencia de otros dispositivos de almacenamiento, disponen de una pantalla y botones que el usuario debe utilizar para confirmar diferentes acciones. De este modo, aún en el supuesto de que algún hacker pudiera acceder al ordenador en el breve momento en el que el dispositivo se encuentra conectado, no podría hacer nada con él.

Además, **permiten firmar una transacción sin desvelar en ningún momento la clave privada**.

Un ejemplo es el **Ledger Nano S**. En este caso, el acceso al dispositivo está protegido por un PIN y el firmware ha sido diseñado para que no pueda ser alterado sin conocer la clave privada.

Además, genera una clave diferente cada vez que queremos recibir bitcoins y es multidivisa, por lo que, además de bitcoin, podemos utilizarlo con otras criptomonedas como Ethereum, Litecoin o Zcash.

Se puede ver un tutorial oficial en el siguiente vídeo:

¿Cuál es entonces la mejor opción?

No existe una opción ideal, pero en general, se recomienda **combinar, al menos, el uso de un monedero caliente** con un par de claves, **con uno frío** con otro par de claves diferentes.

De este modo, podremos manejar una cantidad reducida de bitcoins para nuestro día a día en el monedero caliente (monedero móvil, web o de escritorio con conexión a Internet) y tener a buen recaudo el resto de nuestros bitcoins en un monedero frío (a poder ser, un dispositivo de hardware específico).

Conviene tener almacenada también la clave pública de nuestro monedero frío en el monedero caliente. De ese modo, a medida que aumente la cantidad de bitcoins que tenemos acumulada en el monedero caliente, podremos ir enviando dinero al monedero frío muy fácilmente.

Dado que la clave pública solo sirve para recibir bitcoins, no hay riesgo en tener la clave pública del monedero frío en un dispositivo con conexión a Internet, porque aún en el supuesto de que un tercero se hiciera con ella, no podría utilizar nuestros bitcoins.

Paralelamente, tendremos también una copia de las claves del monedero caliente en el monedero frío. De ese modo, si le pasa algo al dispositivo que estamos utilizando como monedero caliente (por ejemplo, se estropea o rompe el móvil) no perderemos nuestros bitcoins, dado que seguiremos teniendo una copia de las claves.

No obstante, para transferir dinero a la inversa con este sistema, es decir, desde el monedero frío al caliente, necesitamos conectar ambos monederos, por lo que siempre habrá cierto riesgo, aunque mucho menor, especialmente si utilizamos un monedero de hardware diseñado específicamente para tal fin.

Monederos Multifirma

Algunos monederos ofrecen una opción de seguridad conocida como “multifirma”.

Esta opción es similar a las cuentas bancarias en las que es necesario que firme más de una persona para poder realizar cualquier operación.

En general, nos permiten especificar:

1. Un número total de firmas autorizadas (en este caso, claves autorizadas).
2. El número mínimo de firmas (o claves) necesarias para realizar una transacción.

Este sistema es ideal para cuentas de empresa, dado que si la empresa está constituída, por ejemplo, por dos socios, podrían contar cada uno de ellos con una clave privada diferente y que ambas fueran necesarias para poder transferir cualquier cantidad en bitcoins propiedad de la empresa a otra dirección.

Este sistema incrementa considerablemente la seguridad, ya que un tercero que quisiera hacerse con el dinero tendría que conseguir primero las dos claves.

También podría tratarse de una sociedad de tres con tres firmas autorizadas en la que fuesen necesarias dos firmas para realizar una transferencia, etc.

Además del uso empresarial, este sistema puede servir a un particular para mejorar la protección de sus bitcoins, dado que podría utilizar un monedero multifirma con, por ejemplo, tres claves privadas y guardar cada una de ellas en un lugar diferente.

De ese modo, aunque la seguridad de alguna de las claves se viera comprometida, los bitcoins asociados a ella seguirían estando a salvo.

Listado de monederos

1. Móviles

- Airbitz: iOS / Android
- ArcBit: iOS / Android
- AtomBit: iOS
- Bitcoin Wallet: Android
- Bitgo: iOS
- Bither: iOS / Android
- BitPay: iOS / Android / Windows Phone (beta)
- bitWallet: iOS
- Blockchain.info: iOS / Android
- breadwallet: iOS / Android
- BTC.com: iOS / Android
- Coinbase: iOS / Android
- Coinomi: Android
- CoinsBank: iOS / Android
- Coin.Space: iOS / Android
- Copay: iOS / Android / Windows Phone
- Electrum: Android
- Green Address: iOS / Android
- GreenBits: Android
- Jaxx: iOS / Android
- Luxstack: iOS
- Mobi: iOS / Android
- Mycelium: iOS / Android
- Schildbach Bitcoin Wallet: Android
- Simple Bitcoin: Android
- SpectroCoin: iOS / Android / Windows Phone
- Wirex: iOS / Android
- Xapo: iOS / Android

2. Web

- BitGo
- BitoEx
- Blockchain.info
- BTC.com
- Carbon Wallet
- Coinapult
- Coinbase
- CoinsBank
- Coin.Space
- Green Address
- Jaxx
- SpectroCoin
- Strongcoin
- Xapo

3. De escritorio

- ArcBit: Extensión para Chrome
- Armory: Windows / Linux
- Bitcoin Addrindex
- Bitcoin Core: Windows / Mac / Linux
- BitPay: Windows / Mac / Linux
- Blockchain.info: Extensión para Chrome
- Bitcoin Knots
- Bitgo: Extensión para Chrome
- Bither: Windows / Mac / Linux
- Copay: Windows / Mac / Linux
- Electrum: Windows / Mac / Linux
- Exodus: Windows / Mac / Linux
- Green Address: Extensión para Chrome
- Jaxx: Windows / Mac / Linux / Extensiones para Chrome y Firefox
- mSIGNA
- Multibit: Windows / Mac / Linux

4. De hardware

- Case
- CoolWallet
- Digital Bitbox
- KeepKey
- Ledger Blue
- Ledger Nano S
- Opendime
- Trezor

Informes relacionados:

- La tecnología Blockchain en el sistema Bitcoin