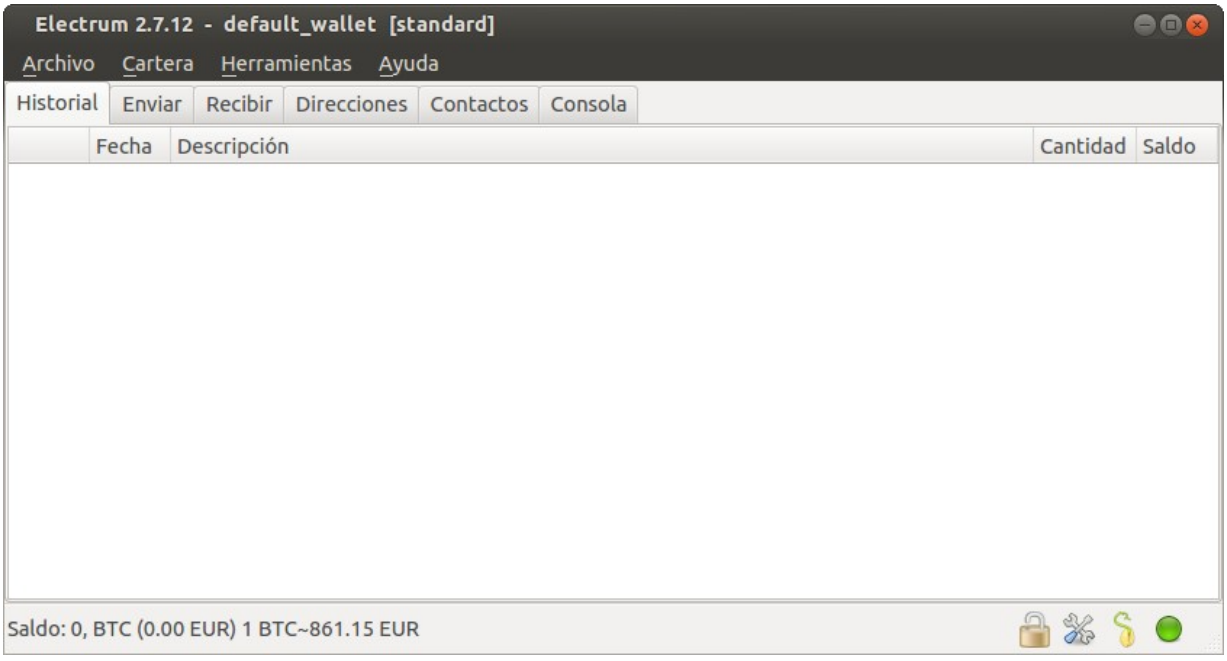
Electrum: un monedero ligero y sencillo para Bitcoin

versión: 0.1
fecha: 08-01-2017
autor: Pele

Índice



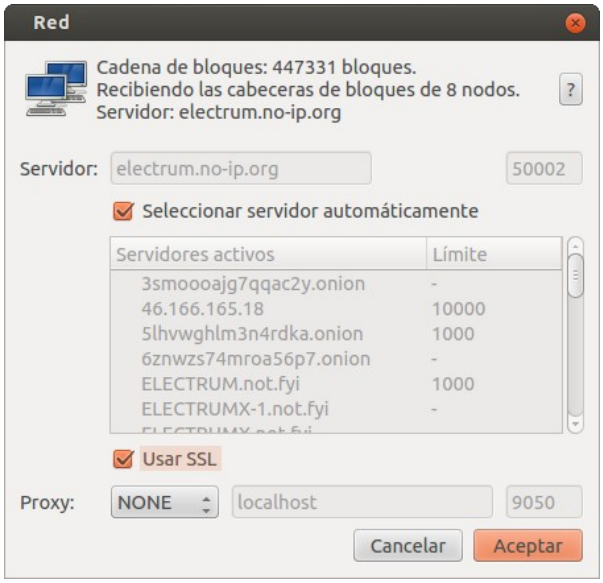
Ventana principal de Electrum

1. Introducción

Con una interfaz de usuario sencilla y clara, Electrum es una muy buena opción para iniciarse en el mundo de Bitcoin. Es un proyecto Open Source, programado en Python y disponible para Windows, OSX, Linux y Android: https://electrum.org/#download

Electrum es un cliente ligero ya que no se descarga la blockchain (la base de datos donde se almacenan todas las transacciones efectuadas en la red Bitcoin).

Para funcionar obtiene la información a través de unos servidores especiales que están conectados a la red de Bitcoin. Estos servidores mantienen una copia de la blockchain y notifican a nuestros Electrums cada vez que se produce un cambio que afecta a alguna de nuestras direcciones.
Podemos ver la lista de servidores entrando en el menú “Herramientas / Red”.



2. Monederos y Semillas

Un monedero es una agrupación de direcciones. En ellas es donde se almacenan nuestros bitcoins.

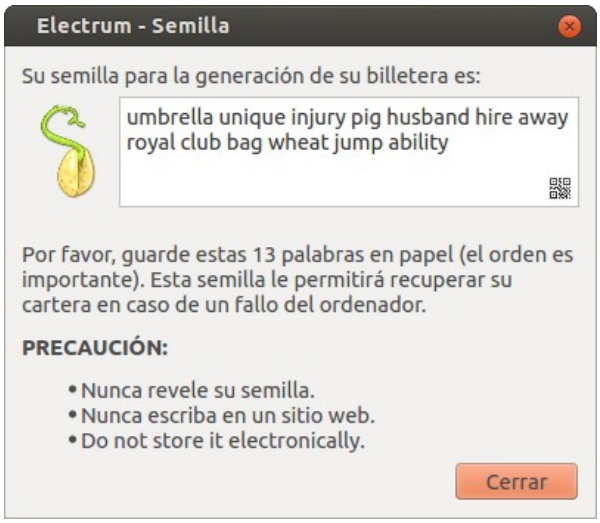
Estos monederos, en Electrum, se generan utilizando una “propuesta de mejora de bitcoin” conocida como BIP32.

BIP32 define un sistema para generar las direcciones de los monederos a partir de una semilla (o seed). Una semilla es una sucesión aleatoria de 12 o 13 palabras, fáciles de apuntar y resguardar, que permiten restaurar completamente un monedero y las direcciones que éste contiene.
Por supuesto, cada monedero tiene su propia semilla.

3. Seguridad

Cada monedero tiene una semilla y puede (y debe) tener una contraseña. Son dos cosas distintas.

SEMILLA
Una semilla, compuesta por 12 o 13 palabras aleatorias, sirve para crear un monedero por primera vez... y para volver a regenerarlo tantas veces como sea necesario.
Si alguien consigue hacerse con nuestra semilla no tendrá mayor problema en regenerar el monedero y mover los fondos que éste contenga.
Por tanto, una semilla debe almacenarse en un lugar seguro, en papel o en un pendrive USB, fuera del ordenador en el que estemos operando (el cual se podría estropear, nos lo podrían robar…) y no debe transmitirse por Internet (ni webs, ni emails, ni chats…).
Podemos ver la semilla de nuestro wallet desde el menú “Cartera / Semilla”.



CONTRASEÑA
Es importante establecerla para cada monedero. Esta contraseña se utiliza para cifrar la semilla en el disco duro y se nos pedirá cada vez que vayamos a realizar un envío de bitcoins.
Como todas las contraseñas, es interesante que esta contenga letras en mayúscula y minúscula, números y otros caracteres (como !, $, %, &, (,), ?, …) para hacerla más robusta.
Podemos establecer una contraseña para un monedero o modificar la existente, desde el menú “Cartera / Contraseña”.

4. Crear y restaurar monederos

La primera vez que ejecutemos Electrum no tendremos ningún monedero disponible. El programa lanzará un asistente que nos permitirá crear un nuevo monedero o importar uno existente a partir de una semilla.

Siempre podremos llamar al asistente para crear nuevos wallets o restaurarlos, a través del menú “Archivo / Nueva/Restaurar”.

Cada linea representa una ventana del asistente:

NUEVO MONEDERO
- Elegimos “Standard wallet”
- Elegimos “Create a new seed”
- Apuntamos las 12 palabras que conforman nuestra semilla en un papel y lo guardamos bien
- Hacemos un “copy” de la semilla
- Hacemos un “paste” de la semilla
- Establecemos una contraseña para mayor seguridad

RESTAURAR MONEDERO
- Elegimos “Standard wallet”
- Elegimos “I already have a seed”
- Escribimos las 12 palabras que conforman nuestra semilla (guardada previamente en papel)
- Establecemos una contraseña para mayor seguridad

Después de restaurar un monedero pueden aparecer transacciones como “Pendientes”. Se soluciona reiniciando el programa.

5. Uso básico

Electrum permite operar con varios monederos a la vez de una manera muy simple. Cada vez que abramos un monedero nos aparecerá una nueva ventana del programa, debemos fijarnos en la barra de título, que siempre nos indicará el monedero con el que está trabajando.

En la imagen, nuestro monedero se llama “default_wallet”

Vamos a comentar brevemente las operaciones más comunes:

RECIBIR

Para recibir bitcoins antes debemos proporcionar nuestra dirección a la persona o servicio que nos los vaya a enviar.

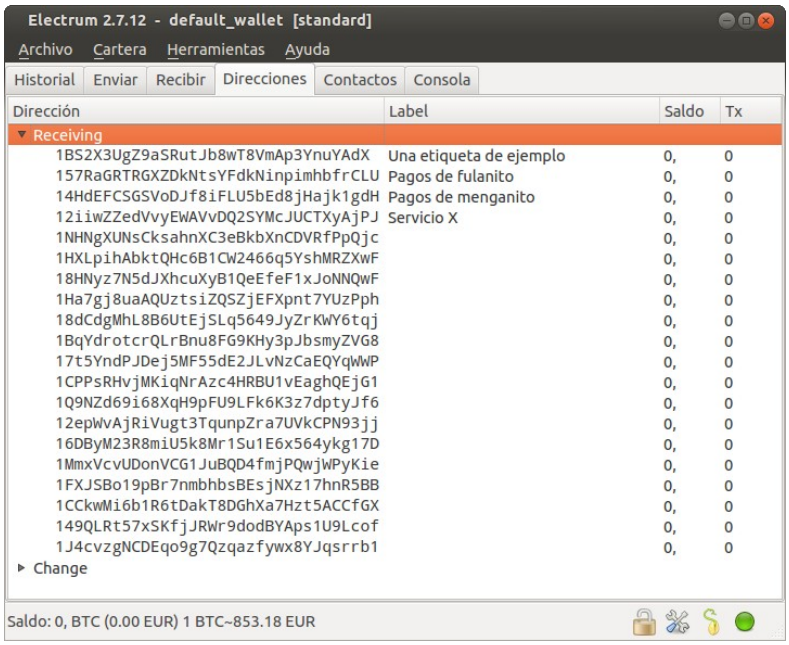
La pestaña “Recibir” es algo engorrosa. Desde ella podemos crear algo así como solicitudes de pago. Una vez creadas. Debemos compartir la URL con la persona que nos deba realizar el pago.

Recomendamos usar otro método.
Vamos a la pestaña “Direcciones”. En caso de que no aparezca, vamos al menú “Cartera / Direcciones”. En esa pestaña tenemos todas las direcciones que pertenecen a nuestro monedero. Estas direcciones están agrupadas por las que son del tipo “Receiving” y por las que son del tipo “Change”. Trabajaremos con las primeras.

Una forma ordenada de recibir nuestros bitcoins es usando una dirección para cada uno de nuestros contactos o servicios, así, será muy fácil de identificar quien nos ha realizado un pago. En la columna “label” de cada dirección, haciendo doble click, podemos establecer un nombre o referencia para cada una de ellas.

Haciendo click derecho encima de una dirección obtenemos un menú desplegable, allí seleccionamos “Copiar dirección” para que se copie en el portapapeles. Ya solo nos quedará compartir esa dirección con nuestro contacto o servicio para que nos realicen el pago.

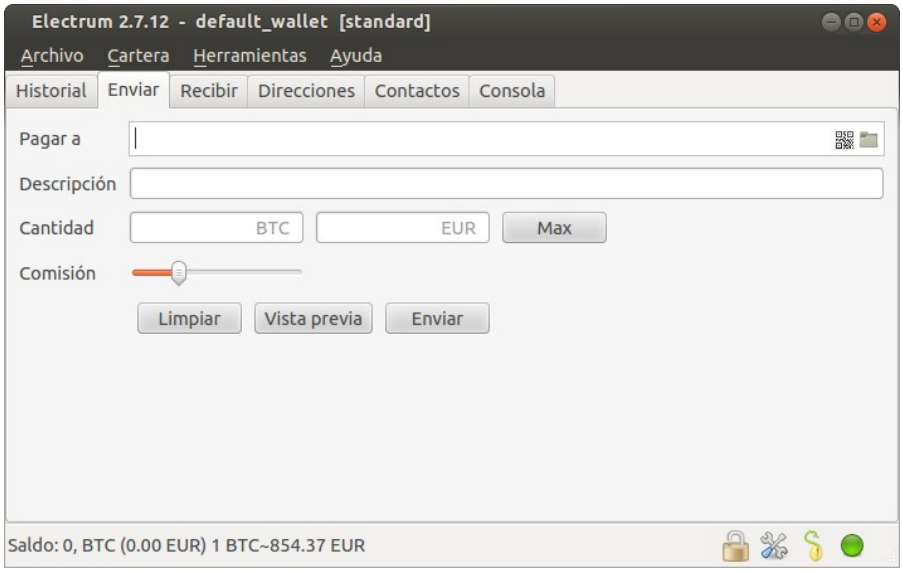
No debemos preocuparnos porque nuestros bitcoins estén repartidos entre varias direcciones, al contrario, su gestión es totalmente transparente para nosotros. Este es el mejor método que podemos usar, tanto a nivel de anonimato como, sobretodo, para tener un funcionamiento ordenado.



Pestaña de Direcciones donde podemos ver todas nuestras direcciones de “Receiving”

ENVIAR

En la pestaña “Enviar”. Solo tenemos que indicar la dirección donde queremos enviar nuestros bitcoins y la cantidad. Podemos escribir una descripción para acordarnos en el futuro del motivo del pago. Se recomienda no tocar la “Comisión” o, sino importa que pueda tardar un poco más, establecerla al mínimo (Within 25 blocks).

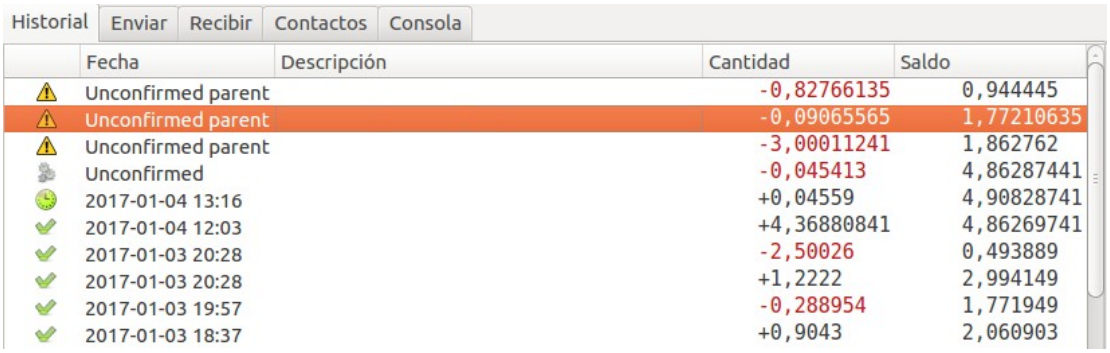


La pestaña “Enviar”

En la pestaña “Contactos” podemos establecer una lista de personas o servicios con sus direcciones. Así, para futuros pagos, bastará con hacer un “copy/paste” de sus direcciones o iniciar un pago a través de ellas.

HISTORIAL

Aquí tenemos el listado con todas las transferencias efectuadas, para todas las direcciones de nuestro monedero, tanto de pagos como de cobros.



Un ejemplo de la pestaña “Historial” con algunas transferencias que se encuentran en varios estados

Cada linea representa una transferencia. Con su fecha, descripción (si es que la hemos indicado), la cantidad movida y el saldo final. La cantidad se muestra en rojo si es un gasto y en negro si es un ingreso.

El icono de la izquierda tiene varios significados:

 Un tip o visto en verde significa que la transferencia se completó correctamente (tiene 6 o más confirmaciones)

 Un reloj más o menos en verde indica que la transferencia aún no tiene las 6 confirmaciones

 Tres tuercas de color gris, con fecha “Unconfirmed” (o “Pending”), significa que la transferencia no tiene, aún, ninguna confirmación

 Un símbolo de admiración, un warning, indica que la transferencia tiene algún problema (aún y así, según el problema, puede llegar a completarse). En la fecha puede indicar más detalles. Si pone “Unconfirmed parent” significa que hemos realizado una transferencia de salida con un dinero que aún no había acabado de entrar del todo (la transferencia anterior, de entrada, aún no tenia las 6 o ninguna confirmación)

Recordad que en el mundo de bitcoin para considerar una transacción como irreversible hace falta esperar un mínimo de 6 confirmaciones. Es aconsejable no gastar dinero que aun no tengamos del todo, es decir, si tenemos una transferencia de entrada de 1 BTC, es mejor no gastarse ese BTC hasta que dicha transferencia, como mínimo, tenga 6 confirmaciones. En caso de realizar una transacción de estas características es posible que esta se demore más de lo habitual en confirmarse o que, quizá, no llegue a hacerlo nunca.

6. Monederos compartidos

Electrum nos permite tener un mismo monedero en más de un ordenador a la vez. Aunque hay que tener en cuenta algunas cosas para evitar problemas.

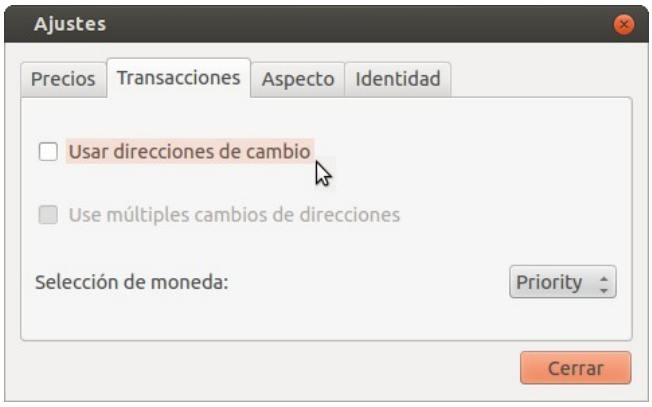
Si el monedero es usado a la vez por varias personas, desde varios ordenadores, y tiene un uso intensivo, puede ocasionar algún problema de sincronización. Y en algún caso puntual, quizá, un intento de doble gasto (?).

IMPORTAR Y EXPORTAR LABELS

Todas las anotaciones, las “labels” y descripciones que anotemos en un Electrum quedarán guardadas, solamente, en ese ordenador. Si queremos, podemos sincronizar esos datos entre varios Electrums que se encuentren en varios ordenadores. Para ello vamos al menú “Cartera / Etiquetas / Importar y Exportar”.

DIRECCIONES DE CAMBIO

Sin entrar en detalles del porqué, existe un mecanismo en Electrum que mejora el anonimato, usando las direcciones “Change” (las podemos ver en la pestaña “Direcciones”).
Este mecanismo puede dar problemas en monederos compartidos entre varios ordenadores. Afortunadamente se puede desactivar, yendo al menú “Herramientas / Ajustes”. En la pestaña “Transacciones” hay que desactivar la opción “Usar direcciones de cambio”.



7. Acciones varias

Aquí agrupamos distintas acciones que podemos realizar con el programa.

COPIA DE SEGURIDAD

Semilla
Ya hemos comentado que podemos restaurar un monedero a partir de su semilla. Esto nos restaurará nuestras direcciones de “Receiving” y “Change”, pero no los direcciones que hayamos importado manualmente, las “Imported”.
Si tenemos direcciones importadas de manera manual hay que usar alguno de los siguientes métodos:

Guardar fichero
Con la opción del menú “Archivo / Guardar Copia” conseguiremos un fichero que contendrá una copia de nuestro monedero en su estado actual, con su semilla, encriptado con su contraseña (si está definida) y con las direcciones importadas manualmente que podamos tener.
Debemos hacer esto con cada uno de los monederos que queramos hacer una copia de seguridad (y cada vez que importemos una dirección nueva).

Guardar directorio
Con el Electrum DETENIDO.
Podemos acceder al directorio con los ficheros de usuario de Electrum (los detalles en el punto 8) y hacer una copia del directorio “wallets”. En ese directorio tenemos un fichero por cada uno de nuestros monederos. Son ficheros de texto que ocupan muy poquito espacio.

ARREGLAR PROBLEMAS CON LOS MONEDEROS
Si tenemos algún problema al realizar una transacción habitual y el programa nos arroja un error extraño (o sea, nada de que la dirección es incorrecta u otros errores lógicos) podemos optar por restaurar de nuevo el monedero.
Un ejemplo de este tipo de errores seria el de “Líneas inválidas conseguidas: ...” seguido de una dirección de BTC correcta. En inglés, este error arroja el texto “Invalid lines found”.

Antes de restaurar el monedero debemos tener en cuenta si hemos importado direcciones de manera manual. Si no tenemos, podemos restaurarlo a partir de la semilla. Si tenemos direcciones importadas, habrá que echar mano de una copia de seguridad del fichero del monedero o bien, restaurar a partir de la semilla y volver a importar las direcciones manualmente (a partir de la clave privada).

IMPORTAR PAPER WALLET
Podemos importar una dirección que tengamos almacenada en papel, en un “Paper Wallet”, a nuestro Electrum. Hablamos de direcciones y sus correspondientes claves privadas.
Para hacerlo hay que ir al menú “Cartera / Llaves privadas / Barrer (o Importar)”.

Recordad que estás direcciones importadas no son recuperables vía semilla. En caso de problemas, hay que volverlas a importar de nuevo o recuperarlas a partir de un fichero de copia de seguridad.

Ejemplo de monedero de papel o “Paper Wallet”

8. Ficheros de los monederos

Es interesante saber donde guarda Electrum los ficheros de usuario, principalmente los “wallets”. Sobretodo si tenemos que hacer alguna operación para arreglar algún monedero que nos dé problemas.

Sistema Operativo	**Directorio**
Windows	\Users\NOMBREdelUSUARIO\AppData\Roaming\Local\Electrum
OSX	/Users/NOMBREdelUSUARIO/.electrum
Linux	/home/NOMBREdelUSUARIO/.electrum

Estos directorios están ocultos. En caso de no poder verlos:

Sistema Operativo	**Ver directorios ocultos**
Windows	Mostrar archivos ocultos en Windows 10, 8.1 y 7
OSX	Ir al “Finder”. En el menú seleccionar “Ir / Ir a la carpeta”. Escribir “~/.electrum”
Linux	Ir al directorio de usuario. En el menú seleccionar “Ver / Mostrar archivos ocultos”

Una vez estemos dentro del directorio de Electrum veremos que este contiene un directorio llamado “wallets”. Ahí es donde se almacenan nuestros monederos. Cada monedero tendrá su fichero y éste se llamará con el mismo nombre que nos aparece en el propio Electrum.

9. Otras criptomonedas

Mencionar, a modo de curiosidad y para evitar confusiones, que existen unas versiones de Electrum modificadas para trabajar con otras criptomonedas. No es que Electrum funcione con más de una criptomoneda a la vez, sino que hay distintos Electrums, cada uno adaptado para funcionar con una sola criptomoneda. Por ejemplo: Electrum Litecoin y Electrum Faircoin.

10. Referencias

- Electrum Documentation

- A Beginner's Guide to the Electrum Bitcoin Wallet