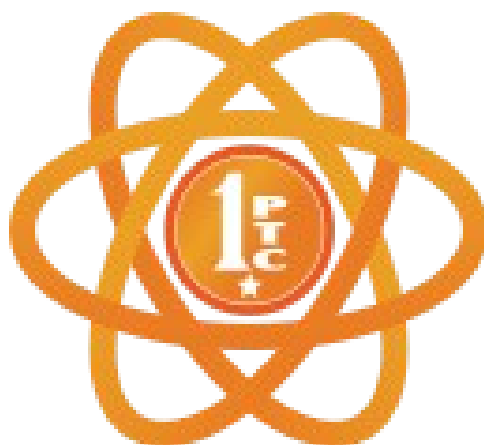


Documentación Electrum-Peseta

Versión 2.2.1



Equipo Pesetacoin

1 de Septiembre de 2017

Contenido

1. Preguntas Frecuentes
 1. ¿Cómo funciona Electrum-Peseta?
 2. ¿Confía Electrum-Peseta en los servidores?
 3. ¿Qué es una semilla (seed)?
 4. ¿Cómo de segura es la semilla?
 5. ¿Cómo puedo enviar la máxima cantidad disponible en mi cartera?
 6. ¿Cómo puedo cambiar el idioma en Electrum-Peseta?
 7. ¿Cómo puedo mandar Pesetas sin pagar comisión?
 8. ¿Que encriptación se usa para las carteras?
 9. He olvidado mi contraseña pero todavía tengo mi semilla. ¿Puedo recuperar la contraseña?
 10. ¿Porque puedo abrir mi cartera sin introducir mi contraseña?
 11. ¿Electrum-Peseta soporta almacenamiento en frio?
 12. ¿Puedo importar claves privadas desde otros clientes de Pesetacoin?
 13. ¿Puedo barrer (sweep) mis claves privadas de otros clientes de Pesetacoin?
 14. ¿Donde está localizada mi cartera?
 15. ¿Puedo hacer varios pagos al mismo tiempo con Electrum-Peseta?
 16. ¿Se puede ver el valor de las Pesetas en euros?
 17. ¿Cual es el gap limit (límite de hueco)?
 18. ¿Como puedo pre-generar nuevas direcciones?
2. Cartera estándar
 1. ¿Que es?
 2. Crear la cartera
 3. Recibir Pesetas
 4. Enviar Pesetas
3. Almacenamiento en frio
 1. ¿Que es?
 2. Crear la cartera
 3. Crear transacción no firmada
 4. Firmar la transacción
 5. Transmitir la transacción

Electrum-Peseta es una cartera ligera de Pesetacoin.

Preguntas frecuentes

1.1 ¿Cómo funciona Electrum-Peseta?

Electrum-Peseta está enfocada en la velocidad, consumir pocos recursos y simplificar Pesetacoin. El tiempo de arranque es instantáneo porque opera conjuntamente con servidores de alto rendimiento que son los que gestionan las partes más complicadas del sistema de Pesetacoin.

1.2 ¿Confía Electrum-Peseta en los servidores?

En realidad, No; el cliente Electrum-Peseta nunca envía las claves privadas a los servidores. Además, verifica la información recibida de los servidores utilizando una técnica llamada [Simple Payment Verification](#)

1.3 ¿Qué es una semilla (seed)?

La semilla es la frase aleatoria que se utiliza para generar tus claves privadas.

Ejemplo:

| |
|--|
| padre abuelo terapia malo traje amor enfermedad reloj falso verde corbata fuego odio |
|--|

Su cartera puede ser completamente recuperada desde esta semilla. Para ello, debe seleccionar la opción "Restaurar cartera" (restore wallet) al iniciar Electrum-Peseta.

1.4 ¿Cómo de segura es la semilla?

La semilla creada por Electrum-Peseta tiene 128 bits de entropía. Esto significa que provee el mismo nivel de seguridad que una clave privada de Bitcoin (de una longitud de 256 bits).

1.5 ¿Cómo puedo enviar la máxima cantidad disponible en mi cartera?

Escribe una señal de exclamación (!) en el espacio de la cantidad (amount). La comisión se ajustará automáticamente dependiendo de la cantidad.

1.6 ¿Cómo puedo cambiar el idioma en Electrum-Peseta?

Vaya a Tools → Settings. Se abrirá la ventana y en la parte de Languages → Spanish

1.7 ¿Cómo puedo mandar Pesetas sin pagar comisión?

Puedes crear transacciones con cero comisiones desde la interfaz gráfica de usuario, siguiendo los siguiente pasos:

- Activar la opción de “Ajustar comisión manualmente” (set fees manually)
- Introducir 0 en la casilla de la comisión
- Introducir la cantidad a enviar en la casilla de la cantidad

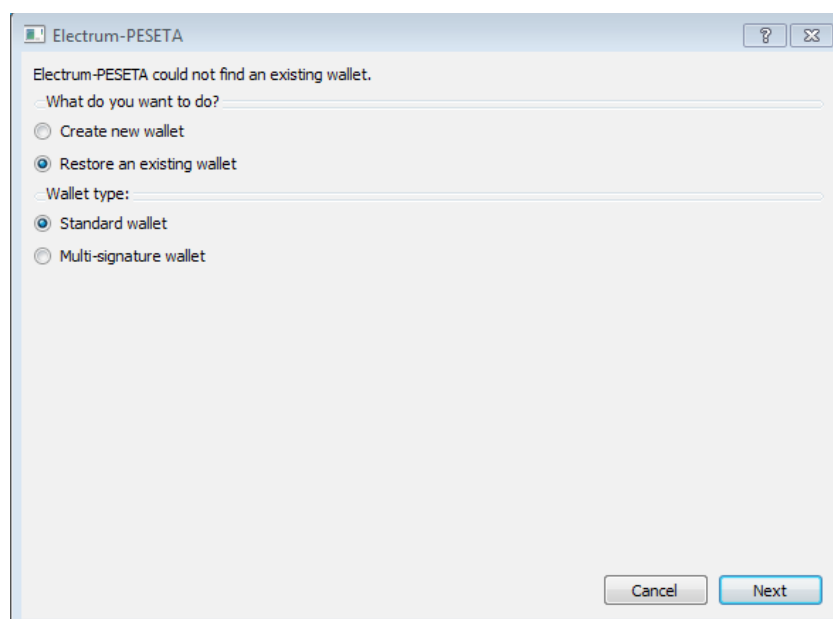
Notese que las transacciones sin comisión pueden no ser retransmitidas por el servidor de Electrum-Peseta, o por la red de Pesetacoin.

1.8 ¿Que encriptación usa para las carteras?

Electrum-Peseta usa AES-256-CBC para encriptar la semilla y las claves privadas en la cartera.

1.9 He olvidado mi contraseña pero todavía tengo mi semilla. ¿Puedo recuperar la contraseña?

No, no puedes recuperar tu contraseña. Pero puedes recuperar tu dinero: recupera tu cartera desde la semilla (restore your wallet from its seed) y elige una nueva contraseña.



1.10 ¿Porque puedo abrir mi cartera sin introducir mi contraseña?

Solo la semilla y las claves privadas están encriptadas, y no la cartera entera. Las claves privadas son desencriptadas brevemente cuando necesitas firmar una transacción; para ello necesitas introducir la contraseña. Esto diseñado así para minimizar el tiempo durante el cual información sensible está desencriptada.

1.11 ¿Electrum-Peseta soporta almacenamiento en frío?

Si, mira el apartado de Almacenamiento en frío para saber más.

1.12 ¿Puedo importar claves privadas desde otros clientes de PesetaCoin?

En Electrum-Peseta, puedes importar tus claves privadas. Si las importas una vez generada la semilla, recuerda, que es necesario guardar una copia de seguridad de la cartera, ya que las nuevas direcciones introducidas no se podrán recuperar desde la semilla. Si lo haces desde el inicio (restore wallet), manejas la cartera desde la clave privada que has introducido.

1.13 ¿Puedo barrer (sweep) mis claves privadas de otros clientes de PesetaCoin?

Barrer (sweeping) las claves privadas significa enviar todas las Pesetas que controlan a una dirección de tu cartera. Las claves privadas no pasan a formar parte de tu cartera; en cambio sí que lo hacen las Pesetas que estas controlan.

Para barrer las claves privadas ve a Cartera -> Llaves privadas -> Barrer. Introduce las claves privadas en el campo apropiado y deja el campo de dirección sin cambios. Esa es la dirección a la que se va a hacer el envío y pertenece a tu cartera de Electrum-Peseta.

1.14 ¿Donde está localizada mi cartera?

La dirección por defecto donde se instala su cartera es en:

Windows:

- Mostrar todos los archivos
- Vaya a: Usuarios → "SuNombreDeUsuario" → AppData → Roaming → Local → Electrum-Peseta

On Mac:

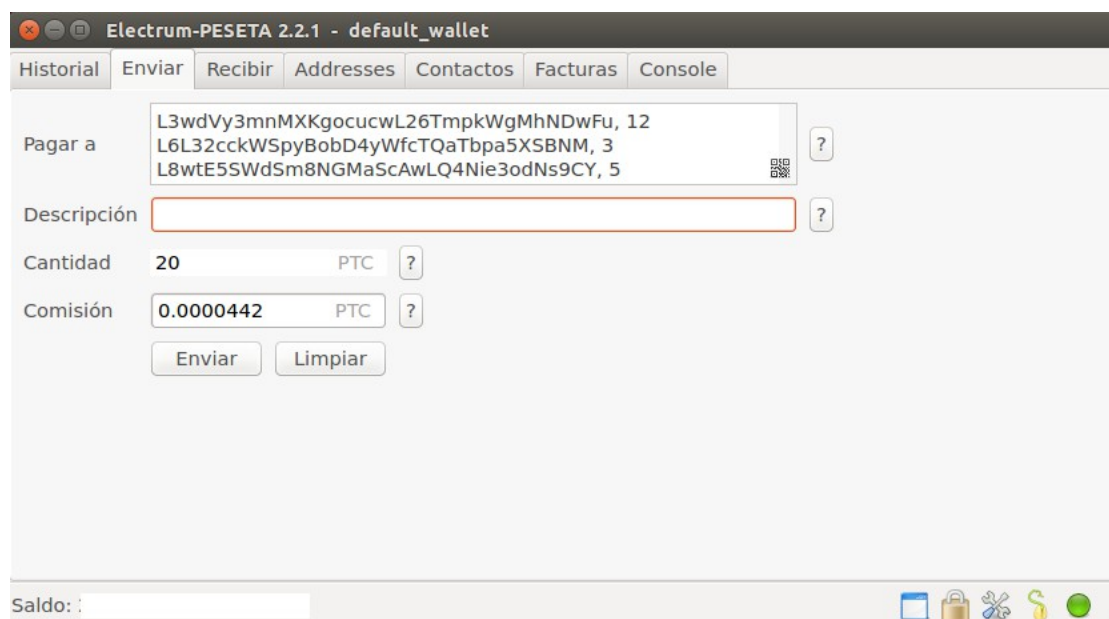
- Abra el buscador
- Vaya a carpeta (shift+cmd+G) y escriba ~/.electrum-peseta

On Linux:

- Carpeta de Inicio
- Escriba ~/.electrum

1.15 ¿Puedo hacer varios pagos al mismo tiempo con Electrum-Peseta?

Puedes crear una transacción con varias salidas (outputs). En la Interfaz Gráfica, escribe cada dirección y la cantidad a enviar en la misma línea y separado por una coma.



También se puede importar un archivo CSV desde Herramientas → Create transaction → From CSV file.

1.16 ¿Se puede ver el valor de las Pesetas en €?

No.

1.17 ¿Cual es el gap limit (límite de hueco)?

El gap limit es el número máximo consecutivo de direcciones sin utilizar que puede generar la cartera. Electrum-Peseta lo utiliza para dejar de crear direcciones y está establecido en 20 por defecto.

1.18 ¿Como puedo pregenerar nuevas direcciones?

Electrum-Peseta generará nuevas direcciones según vayas utilizandolas hasta llegar al gap limit.

Si necesitas pregenerar mas direcciones, puedes hacerlo escribiendo en Console: `wallet.create_new_address()`

Este comando generará una nueva dirección. Tengase en cuenta que esta nueva dirección se mostrará con fondo rojo en la lista de direcciones para indicar que se está superando el gap limit. Se seguirá mostrando así hasta que el gap (hueco) se complete.

AVISO: Las direcciones sobre el gap limit no se generarán automaticamente desde la semilla. Para recuperarlas se necesitará bien incrementar el gap limit del cliente o generar nuevas direcciones hasta que las direcciones sean encontradas.

Si quieres generar mas de una dirección, puedes utilizar la "for" para ello. Por ejemplo, si quieres generar 50 direcciones, puedes escribir en la consola lo siguiente:

```
for x in range(0, 50): print wallet.create_new_address()
```

Cartera estándar

2.1 ¿Que es?

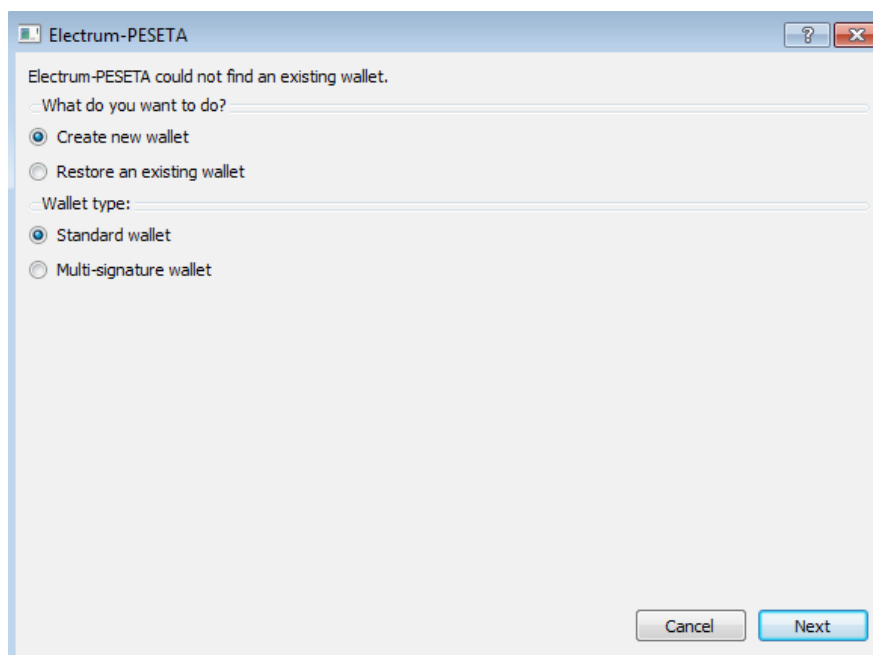
Este tutorial enseñará como crear una cartera estándar que consiste en una única cartera de firma única. A diferencia de la cartera multifirma (que analizaremos en el capítulo siguiente) en la cartera estándar todos los fondos son controlados por una única firma/persona.

2.2 Crear la cartera

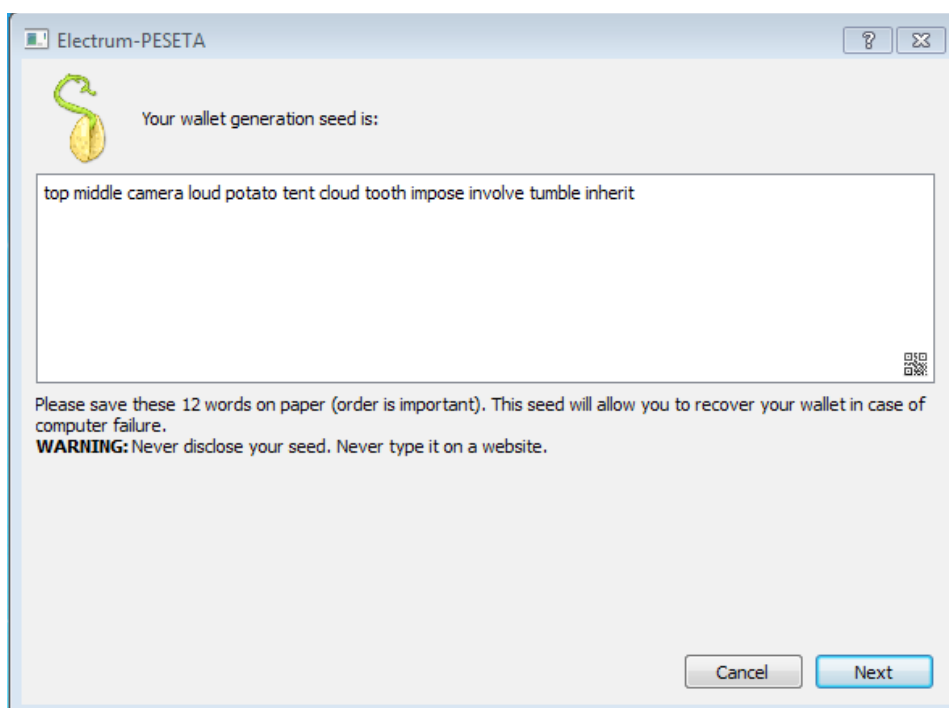
Para crear la cartera, lo que hay que hacer es instalar Electrum-Peseta y seguir los siguiente pasos:

1) Abrir la cartera y por defecto ya viene seleccionado: Create a new wallet (Crear nueva cartera) y Standard wallet (Cartera estándar). Pulsar en Next (Siguiete).

El idioma lo selecciona la aplicación automáticamente en función del idioma establecido en la computadora. Nótese que a veces puede fallar y elegir el ingles aunque su idioma sea el español.



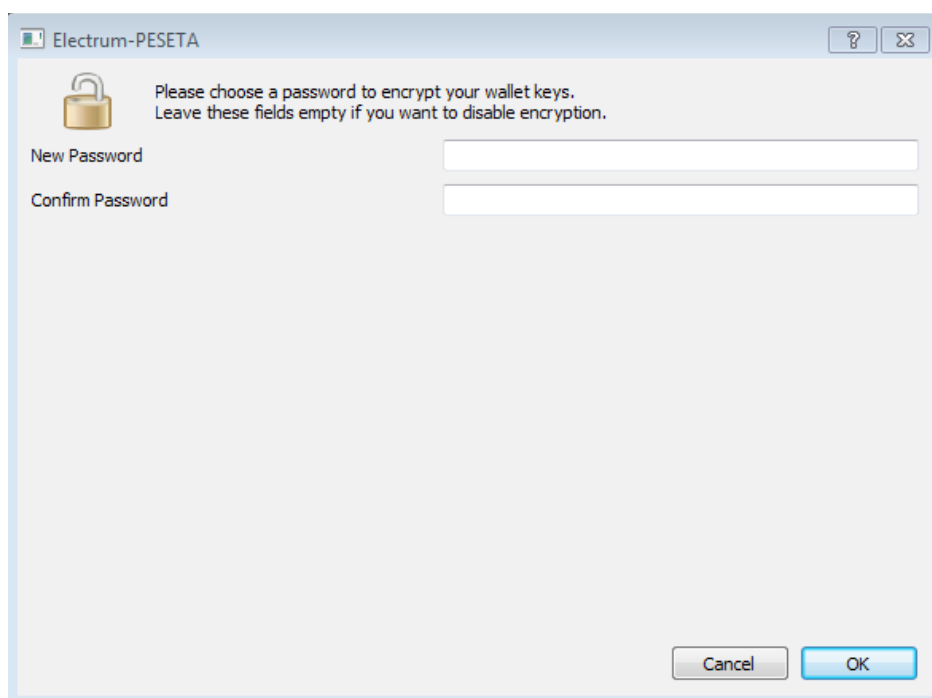
Lo siguiente que veremos será la semilla que nos ha generado. La semilla debe ser conservada con mucho cuidado ya que es lo que nos permitirá acceder a nuestros fondos aunque perdamos la contraseña o borremos la aplicación. Se recomienda no guardarla en el mismo ordenador con el que nos conectamos a internet, ya que si alguien accede a la semilla y la contraseña tendríamos un problema muy serio.

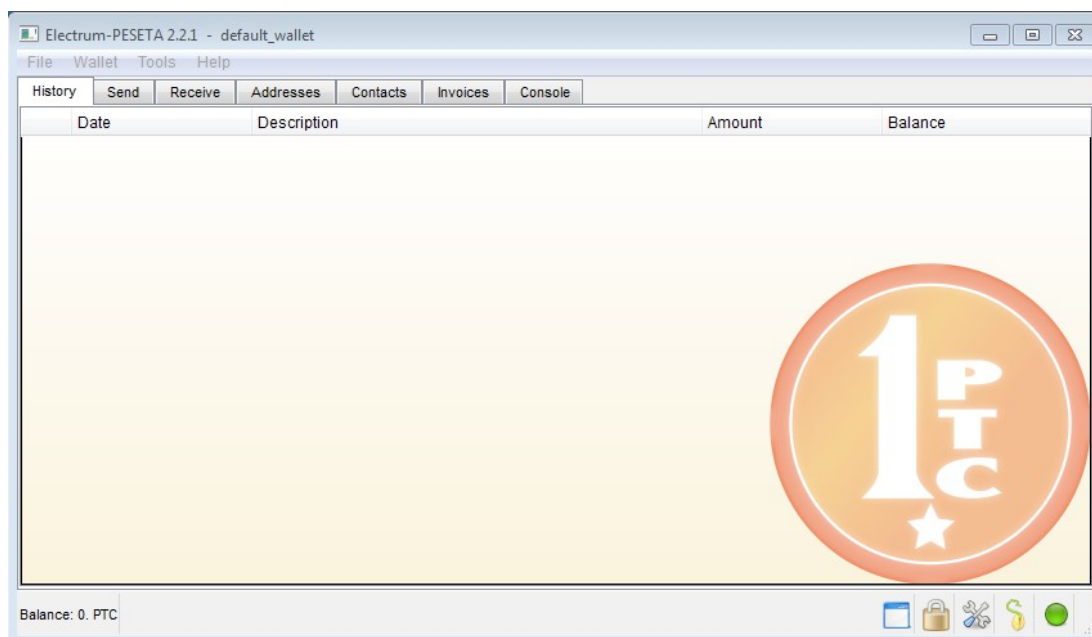


Como puede observar, en este caso, la semilla se compone de palabras inglesas. Si Electrum-Peseta detecta correctamente que su idioma establecido es el español, la semilla se compondrá de palabras en español.

Una vez presione Next (Siguiete), le pedirá que introduzca las palabras que le acaba de mostrar. Este paso es para verificar que ha anotado la semilla.

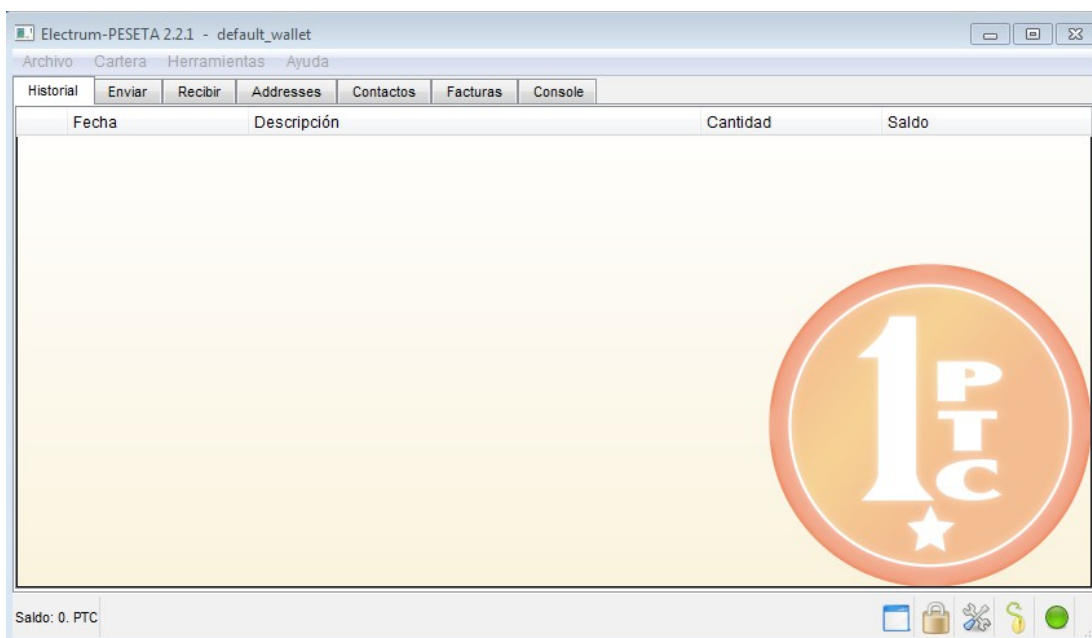
Lo siguiente es establecer la contraseña:





Y entonces ya estará disponible la cartera para ser utilizada:

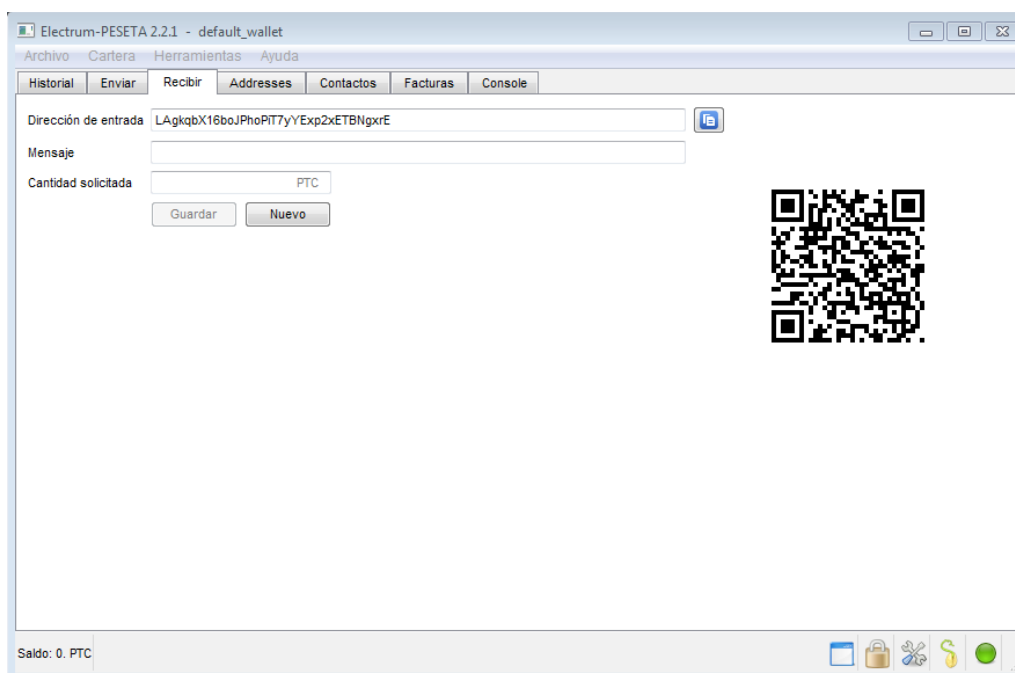
En caso de que su cartera esté en inglés, pueden cambiar el idioma siguiendo estos pasos:
Vaya a Tools → Settings. Se abrirá la ventana y en la parte de Languages → Spanish



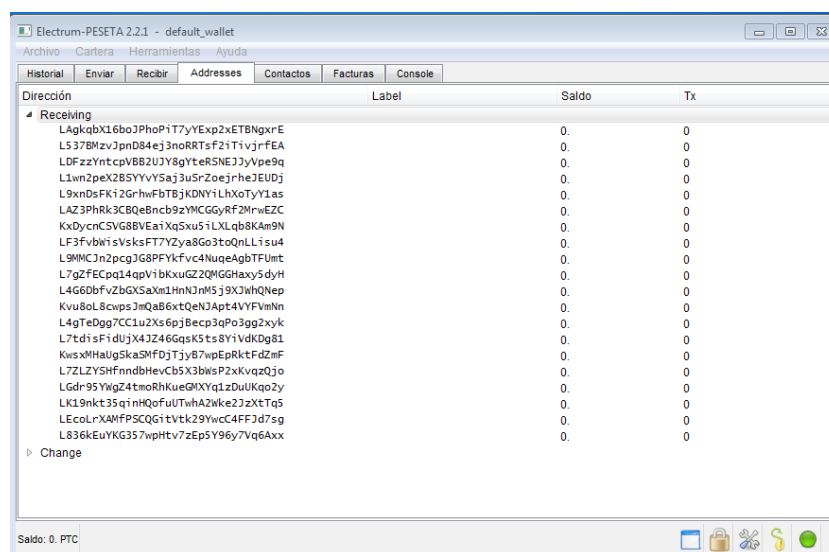
2.3 Recibir Pesetas

Este será un sencillo tutorial de como hacer las primeras transacciones con Electrum-Peseta. Una vez han visto la pantalla principal, pueden ver como hay una pestaña en la que pone “Enviar” y otra en la que pone “Recibir”. Dado que lo primero que hará será recibir, empezaremos por ahí.

Tal y como se puede observar en la imagen, en el campo “Dirección de entrada” ya existe una dirección disponible a la que se pueden enviar las Pesetas. Copie esa dirección y utilícela para hacer el envío desde donde tenga sus monedas.



Una vez halla utilizado esa dirección, Electrum-Peseta mostrará automáticamente otra dirección. No tiene que preocuparse de nada, ya que todo es correcto. Electrum-Peseta genera 20 direcciones a las que se pueden enviar sus monedas y según las va utilizando, crea otras nuevas. No significa que no pueda volver a utilizar las mismas direcciones pero por seguridad y privacidad es aconsejable no reutilizar las direcciones.



2.4 Enviar Pesetas

En este caso, lo que haremos será ir a la pestaña de “Envíos”. Este será un sencillo tutorial de como hacer las primeras transacciones con Electrum-Peseta. Como se puede ver en la foto, hay 3 campos para rellenar.

El primero es “Pagar a” y es ahí donde pegaremos la dirección a la que queremos enviar las monedas.

El segundo campo es “Descripción” y sirve para llevar un registro de las transacciones que hacemos y poder acordarnos a que concepto esta asociada cada una. Las transacciones se pueden consultar en la pestaña “Historial”. Una vez han visto la pantalla principal

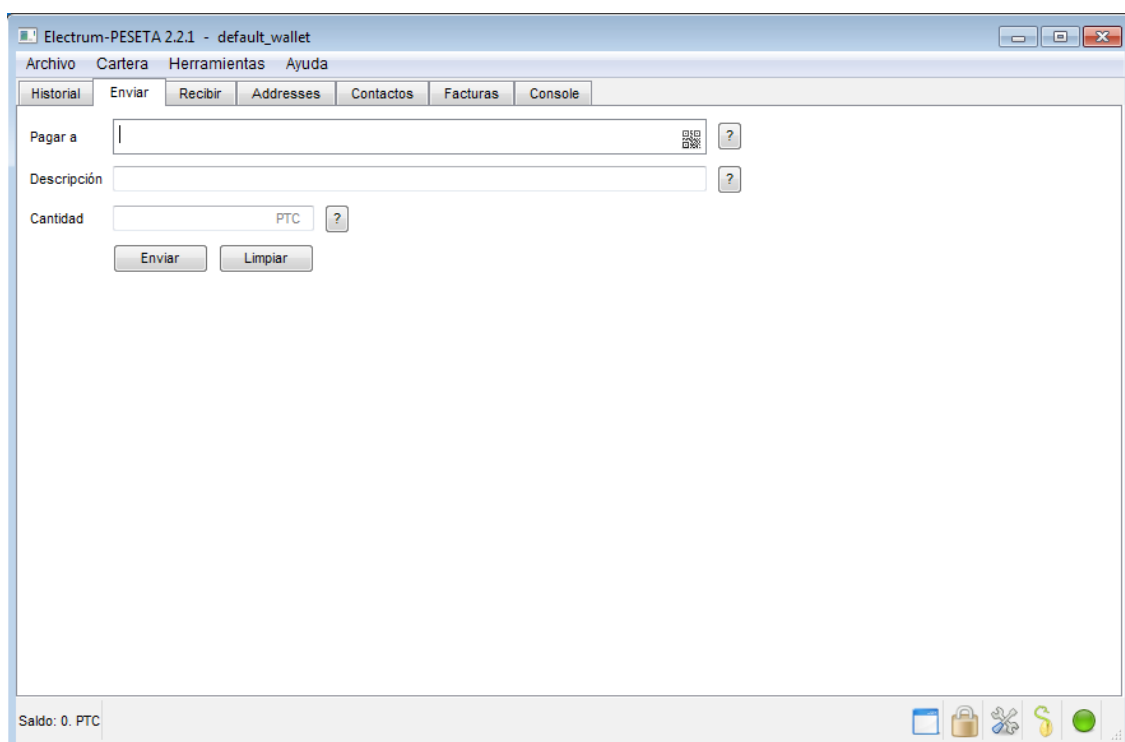
El tercer campo es “Cantidad” y como se puede imaginar es donde debe escribir la cantidad a enviar. Las cantidades se deben escribir sin separar los miles y para pasar a los decimales se utiliza el punto ya que es el sistema estadounidense y no el europeo.

Por ejemplo:

150.34453 PTC

3455.12 PTC

150000.00 PTC



Almacenamiento en frío

3.1 ¿Que es?

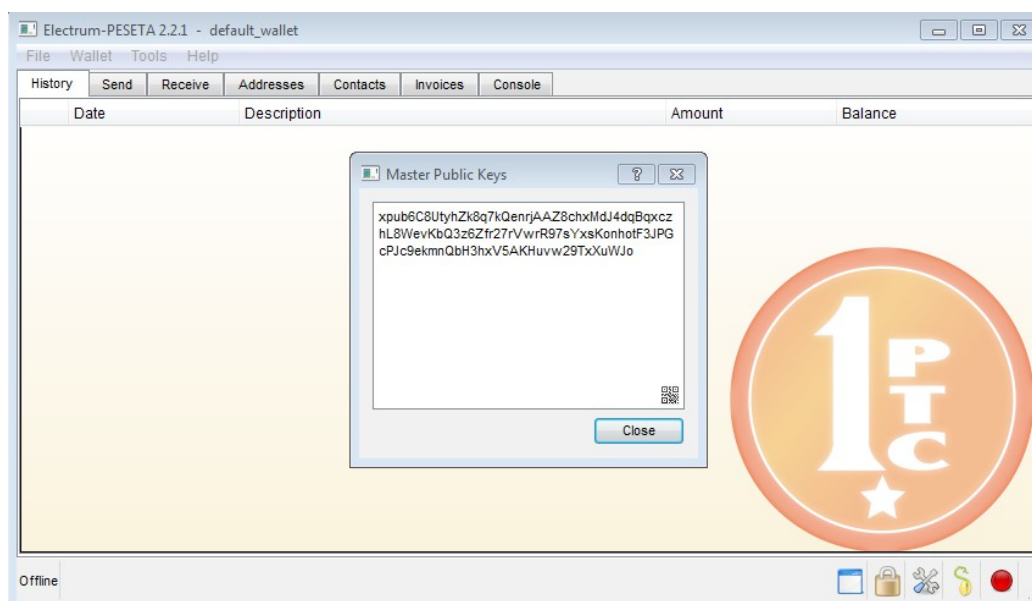
El almacenamiento en frío consiste en tener una cartera offline donde guardas las Pesetas y otra cartera online desde donde retransmites las transacciones firmadas en la cartera offline.

El almacenamiento en frío aporta un nivel de seguridad altísimo ya que los fondos nunca tendrán acceso a internet. Toda transacción necesita ser firmada por la clave privada, que en este caso está en un ordenador sin internet. La única forma que existe de hacer transacciones es iniciarla en otro ordenador y con un usb moverlas a la cartera offline y firmarlas ahí. Es decir, es 100% seguro ante robos por internet.

3.2 Crear la cartera

Para almacenar tu Pesetas en frío hay que seguir los siguiente pasos:

Instalar la cartera en un ordenador sin internet. Después de crearlo, ir a Wallet (Cartera) → Master Public Keys.



Esta es la Master Public Key que se le mostrará una ventana emergente. Transfiera esa clave a su ordenador online. En su maquina online vaya a “Archivo” → “Nuevo/Restaurar” . Introduzca un nombre para la cartera y seleccione “Restore a wallet or import keys” (Restaurar cartera o importar claves).

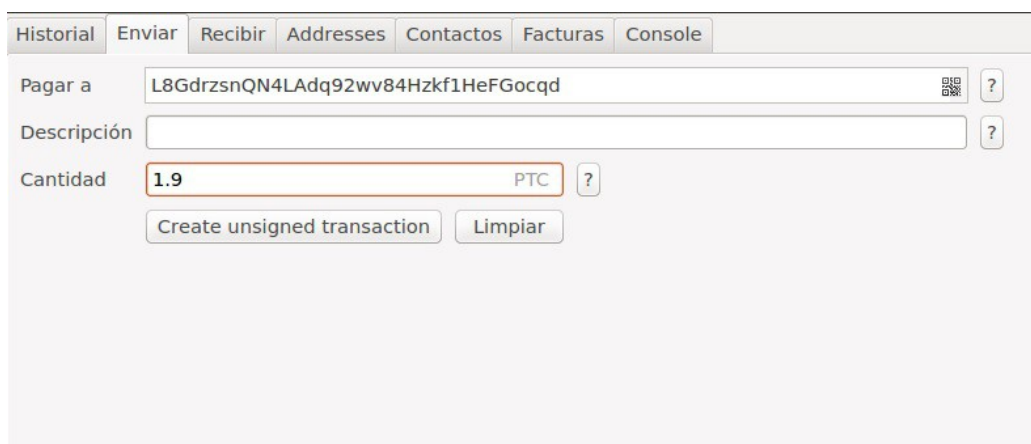
Pegue su Clave Pública Master (Master Public Key) en el campo donde le indica que introduzca su semilla, claves privadas o claves públicas. Haga click en siguiente. Ahora debería ver el historial de transacciones de tu cartera offline.



3.3 Crear transacciones no firmadas

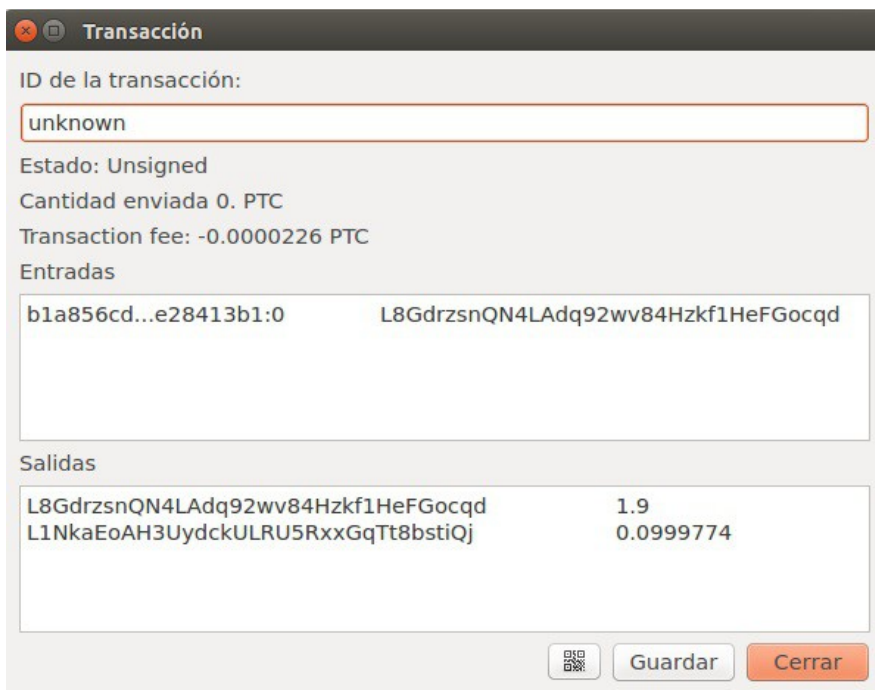
En su cartera online introduzca el destinatario y la cantidad que desea enviar.

Nota: No se puede poner descripción a la transacción ya que generará un error, pero sin poner descripción a la transacción funciona perfectamente.

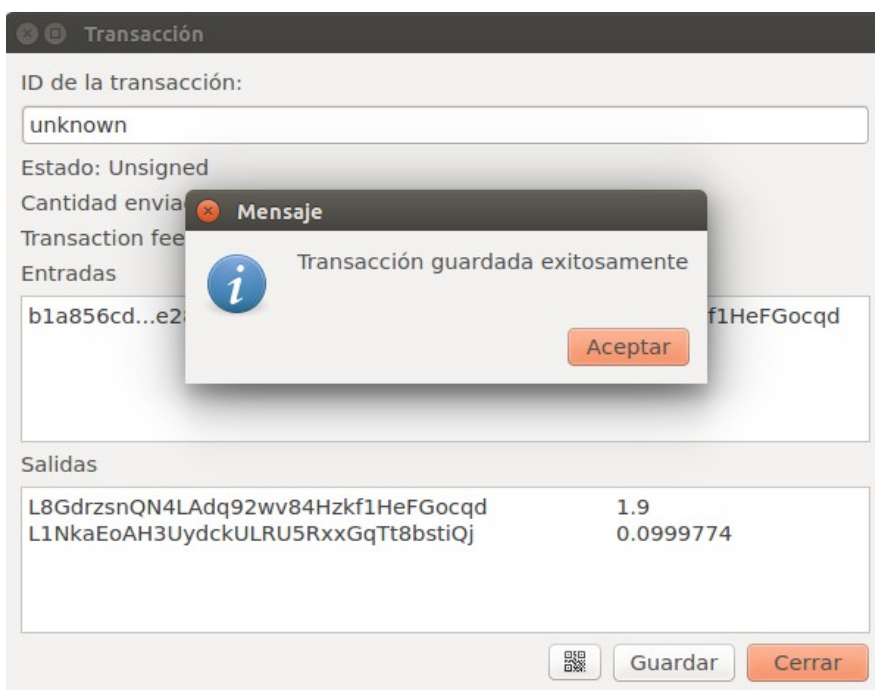


Después pulsaremos en “Create unsigned transaction” (Crear transacción sin firmar) y nos pedirá que confirmemos tanto la dirección como la comisión a pagar. Lo siguiente que veremos será una ventana donde nos muestra los detalles de la transacción y la opción de guardarla. Lo que debemos hacer es guardarla y llevarla al ordenador offline por medios seguros como un usb.

Lo que acabamos de hacer es dar el primer paso para realizar una transacción. Los siguientes pasos son firmarla y por último transmitirla a la red.

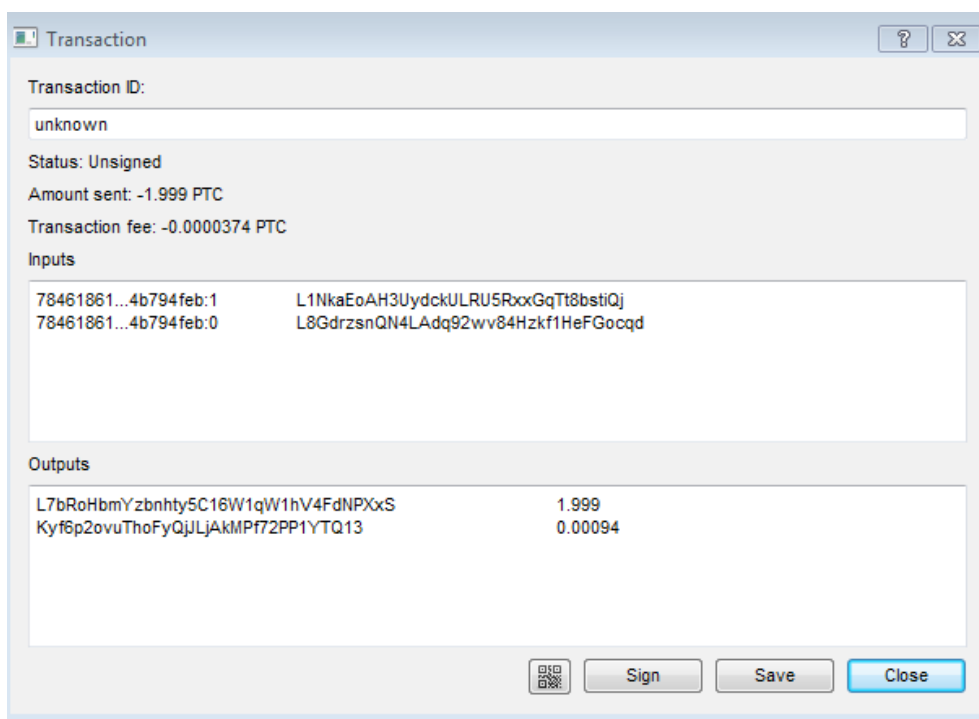
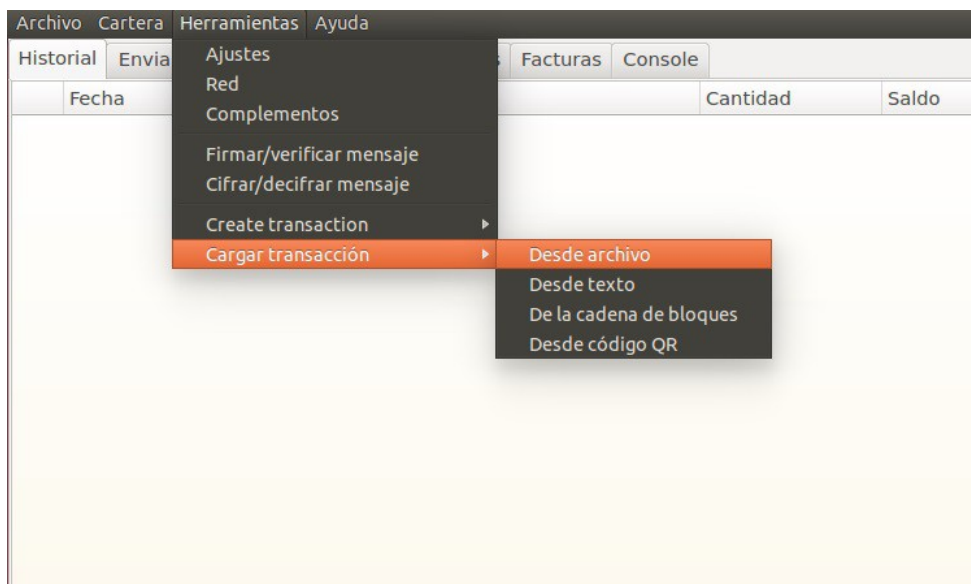


Lo siguiente es decidir donde se va a guardar teniendo en cuenta que debemos moverla a la cartera offline.

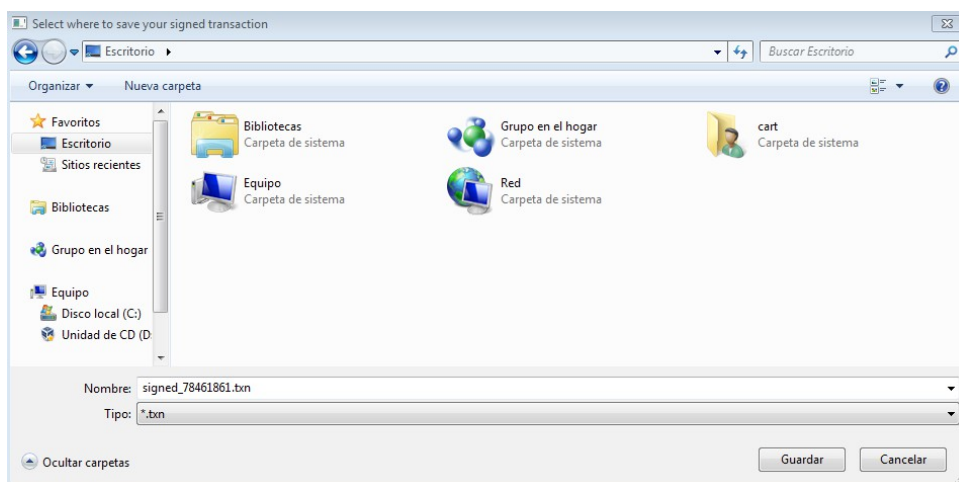


3.4 Firmar la transacción

En la cartera offline, seleccionar “Tools → Load transaction → From file” (Herramientas → Cargar transacción → Desde archivo).



Tras ver que sale esta ventana debemos pulsar en “Sign” (Firmar). Posteriormente, pulsar en “Save” (guardar) y teniendo en cuenta que debe moverse a la cartera online, guardarla en el lugar apropiado.



3.5 Transmitir la transacción

En la cartera online pulsar “Tools → Load transaction → From file” (Herramientas → Cargar transacción → Desde archivo). En la ventana que aparecerá, pulsar en “Broadcast” (transmitir). De esta forma, se habrá completado la transacción correctamente y esta será reconocida por la red de Pesetacoin.

