Un curso de Bitcoin gratuito y de código abierto desarrollado por Area Bitcoin

---

Índice - Bitcoin 4 All -
¿Cómo sacar del exchange y tener soberanía con tu bitcoin?

Bitcoin 4 All - Texto completo

Bitcoin 4 All es un curso gratuito y de código abierto creado por Area Bitcoin. El objetivo es ayudar a más personas a comprender Bitcoin e inspirar a cualquier persona a convertirse en un multiplicador de la educación sobre Bitcoin.

Acerca de este libro electrónico

Publicado por Area Bitcoin – 2025

¿Cómo sacar del exchange y tener soberanía con tu bitcoin?

Bitcoin cambia las reglas del juego. Permite a cualquiera ser depositario de sus propios bienes y moverlos cuando y como quiera sin que nadie pueda impedírselo. Ninguna empresa ni gobierno puede impedirte que muevas tu propio dinero ni quitártelo si lo guardas con soberanía.

Soberanía es la palabra aquí. Tú eres tu propio banco. Pero para hacerlo realmente, necesitas saber cómo utilizar herramientas, billeteras, y cómo sacar tu bitcoin de las manos de estos intermediarios.

En la lección anterior aprendiste qué son las billeteras Bitcoin y por qué es importante mantener tus palabras semilla seguras para que siempre tengas acceso a tu saldo. El siguiente paso es llenar esa billetera con bitcoin y empezar a acumular para el futuro. Así que en esta lección consideraremos que ya tienes bitcoin y quieres enviarlo desde la dirección del exchange a la dirección de tu monedero.

Pero antes de hacerlo en la práctica, entendamos qué son las direcciones y cómo funciona una transacción en la red Bitcoin.

(slide 257) - Bitcoin 4 All

Cuando configuras tu billetera bitcoin, ésta genera una lista de palabras llamada "frase semilla" ("*seed phrase*"). Esas palabras representan códigos que te permiten recibir, almacenar y enviar bitcoin. A partir de la frase semilla, tu monedero generará otros códigos encriptados llamados claves pública y privada.

La clave privada es una secuencia de letras y números que te permite firmar transacciones y controlar el saldo de tu billetera. Con ella puedes mover bitcoin de una dirección a otra o importar un saldo específico. Cuando envías bitcoin de una billetera a otra, es la clave privada la que autoriza el traslado del saldo. Por eso no debes compartir tu frase semilla ni tus claves privadas con nadie. Por eso tiene este nombre: es privada, es información que debes guardarte para ti.

La gran diferencia entre una frase semilla y una clave privada es que una frase semilla (una lista de 12, 18 o 24 palabras) puede recuperar varias claves privadas de varios saldos enlazados, mientras que una clave privada sólo recupera los saldos de las direcciones que generó. Esas son las direcciones donde recibirás bitcoin.

Las direcciones se generan a partir de esas claves y son públicas. Cuando realizas una transacción, ésta aparece en la blockchain para que cualquiera pueda verificarla. No es posible averiguar la semilla o la clave privada a partir de una dirección, aunque aparezca en la blockchain de Bitcoin. Pero si no cuidas bien las semillas o claves privadas, terceros pueden tener acceso no sólo a tu bitcoin, sino a todas las claves y direcciones que generen.

(slide 258) - Bitcoin 4 All

Una billetera puede generar miles de direcciones diferentes a partir de la clave pública. Su función es generar direcciones. Una de las mejores prácticas con Bitcoin es no reutilizar nunca las direcciones. Las billeteras siempre generan nuevas direcciones después de que hayas realizado una transacción, precisamente para darte más privacidad y evitar la reutilización. Si alguna vez has utilizado una billetera de Bitcoin, te darás cuenta de que la dirección cambia con cada transacción. Al fin y al cabo, una vez realizada una transacción, las direcciones son visibles públicamente en la blockchain y sería más fácil hacer un seguimiento de los saldos por asociación.

En pocas palabras, la clave privada desbloquea el derecho del propietario de la billetera para gastar, mover e intercambiar las monedas asociadas a esa billetera. Como su nombre

indica, es privada y no debes mostrársela a otras personas. La dirección es donde envías bitcoin cuando realizas una transacción. Nadie puede adivinar tu clave privada a partir de tu dirección.

(slide 259) - Bitcoin 4 All

Podemos pensar en la dirección como si fuera la dirección de tu casa. La compartes con otras personas, es relativamente pública, pero no vas por ahí con un megáfono diciendo a todo el mundo dónde vives. A veces necesitas mostrar tu dirección para recibir una entrega, pero eso no significa que puedan acceder a tu casa. Para eso necesitas las llaves de la puerta. En el caso de las billeteras: las claves privadas.

Así que la dirección es como tu domicilio y las claves privadas son las que te dan acceso a lo que hay dentro: tu saldo de bitcoins.

Recuerda que tus bitcoins no se almacenan dentro de las billeteras. Siempre están en la blockchain. Los bitcoins siempre están en una dirección de la red blockchain y no dentro del propio dispositivo. Cuando haces una transferencia, le dices a la red que quieres mover "x cantidad" en bitcoin de una dirección a otra dirección. Las billeteras autorizan estas transacciones que llevan bitcoins de una dirección a otra mediante una firma digital realizada con la clave privada.

Pero ¿cómo funciona una transacción?

(slide 260) - Bitcoin 4 All

Abres tu billetera, tecleas la cantidad que quieres enviar, pegas la dirección del destinatario y haces clic en enviar. Cuando pulsas enviar, estás firmando la transacción con tu clave privada. Eso es lo que ocurre detrás de los códigos de la billetera.

(slide 261) - Bitcoin 4 All

Cuando firmas la transacción demostrando a la red Bitcoin que eres el verdadero propietario de la clave privada de la dirección de la billetera, esa transacción va a una sala de espera,

conocida como mempool. Es la sala de espera de las transacciones que esperan ser insertadas en un bloque por los mineros. Las transacciones se registran en la blockchain cuando un minero las selecciona para que formen parte del bloque de información. En cuanto un minero introduce una transacción en un bloque, éste es verificado por la red, que actualiza sus registros en el blockchain. A continuación, el bloque se propaga por toda la red como un bloque válido, con la transacción en su interior.

Cuando una transacción se inserta en un bloque, se dice que ha sido confirmada. A medida que se minan más bloques, se producen más confirmaciones. Generalmente, una transacción se considera irreversible después de 6 confirmaciones, cuando han pasado seis bloques. Cuando se realizan las confirmaciones, la billetera lo notifica al usuario, la transacción se considera recibida y el saldo está disponible para ser gastado. Así es como se producen las transacciones en la cadena cuando envías bitcoin.

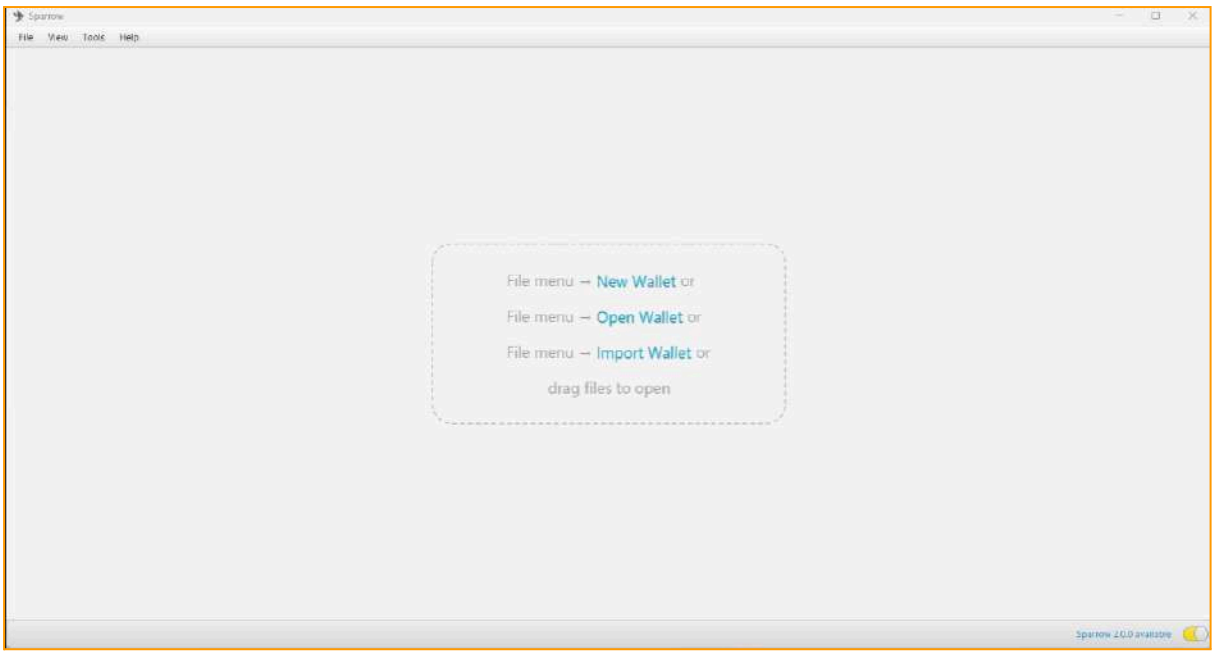
Ahora que has entendido la teoría, ¡vamos a la práctica!

Ahora voy a mostrarte cómo crear una billetera desde cero, retirar bitcoin del exchange a este monedero y recuperar el saldo utilizando la frase semilla.

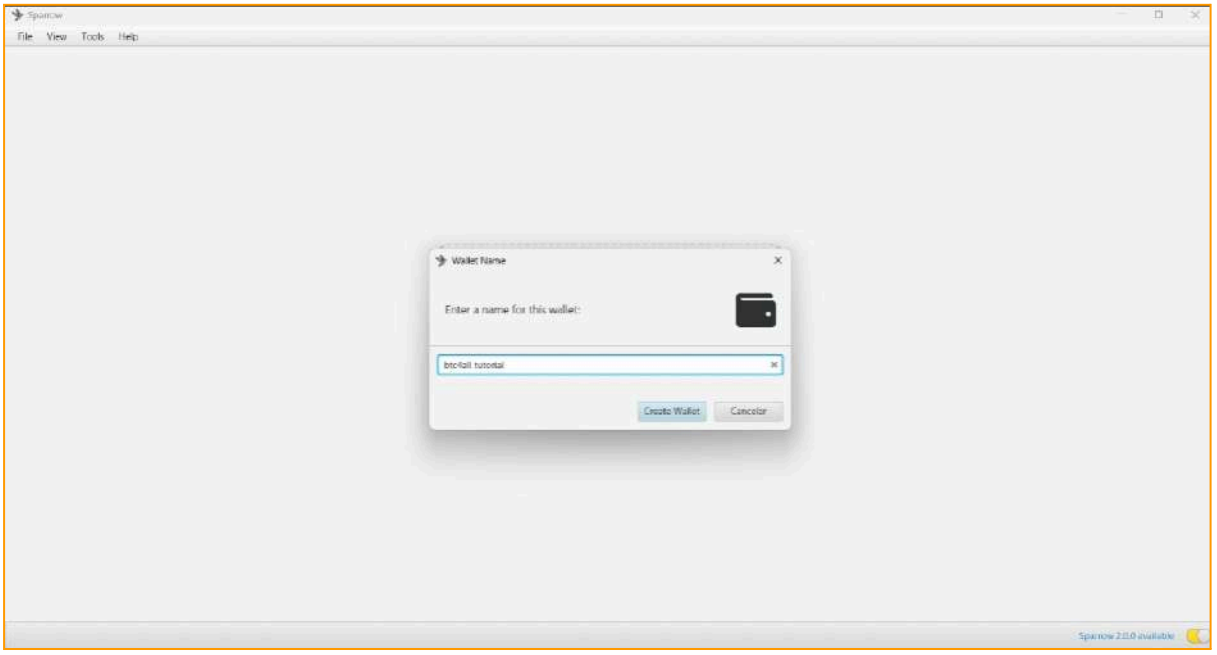
Para ese tutorial hemos elegido utilizar la Sparrow Wallet, porque es una billetera muy versátil y completa, tanto para principiantes como para usuarios avanzados. Es autocustodiable, de código abierto y funciona muy bien como billetera coordinadora entre varias marcas de billeteras hardware: Jade, Ledger, Trezor, Coldcard, Seed Signer, Krux... En resumen... prácticamente todas las billeteras hardware funcionan con Sparrow. La diferencia es que las billeteras que tienen su propio software, como Ledger y Trezor, en cualquier caso te piden que descargues el software Ledger Live o Trezor Suite para actualizar el firmware del dispositivo antes de conectarte a Sparrow.

También ofrece funciones como crear multisigs, realizar transacciones air gapped, PSBT, gestionar y consolidar UTXO, posibilidades que se centran en aumentar la seguridad y privacidad del monedero. Recuerda que Sparrow es una billetera sólo de computadora, no tiene aplicación para móviles, ni para iOS ni para Android. Te dejaré el enlace aquí en la pantalla para que lo descargues y también una lista de otras billeteras para que las pruebes y veas cuál te conviene más.

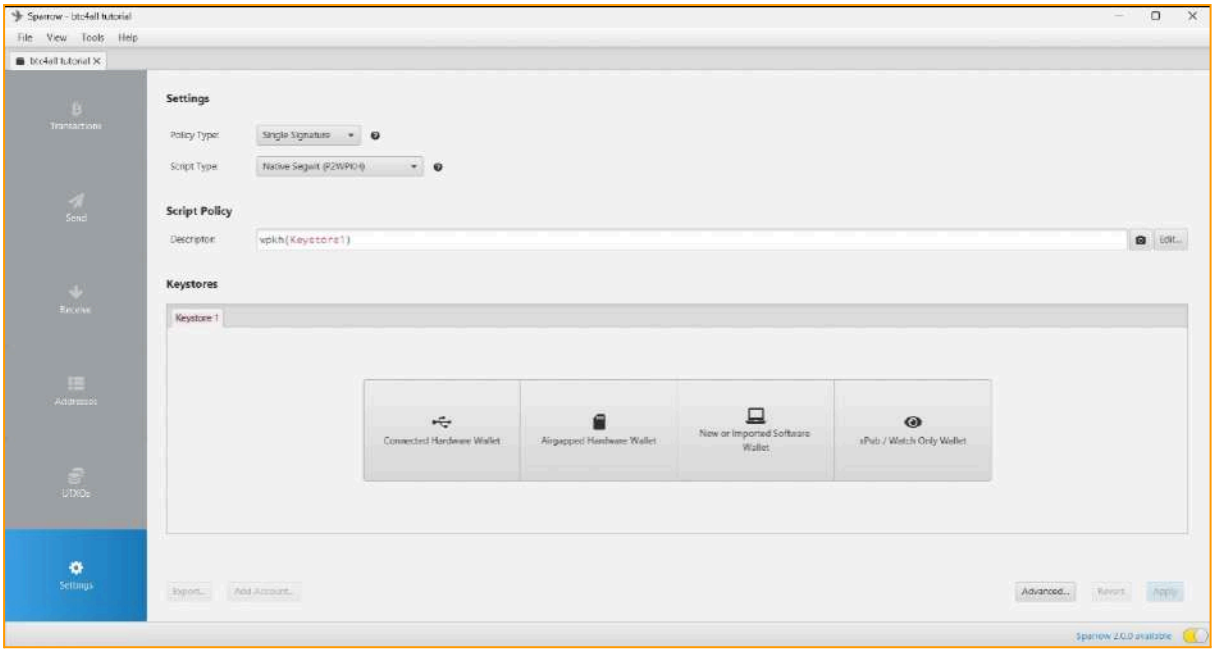
Empecemos por configurar Sparrow. El primer paso es descargar Sparrow e instalar el software.



A continuación, sólo tienes que abrir Sparrow y hacer clic en "*New wallet*" para crear una nueva billetera.



Ahora elige un nombre personalizado para este monedero – yo escribiré "btc4all tutorial" – y haz clic en "*Create wallet*".

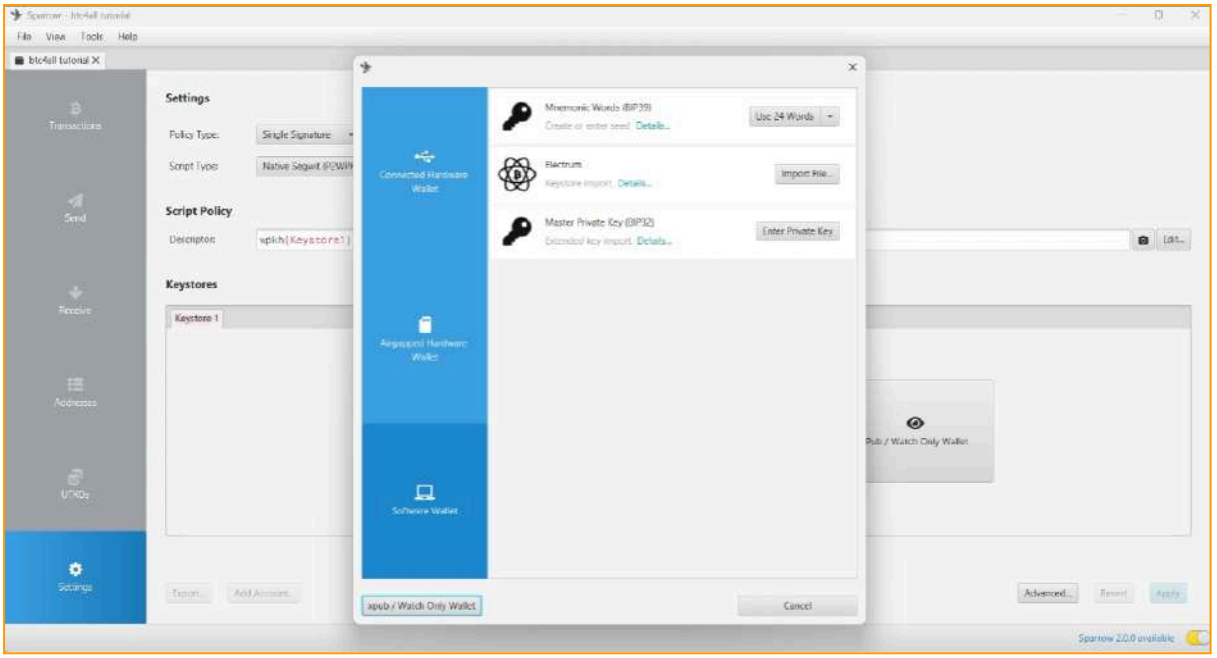


Esa es la página inicial de Sparrow. Fíjate en que la columna de la izquierda es gris y sólo las configuraciones son azules. Eso significa que la billetera no tiene ninguna información y necesitas crear una billetera, importar una o conectarte a una para poder controlar los saldos, recibir y enviar bitcoin.

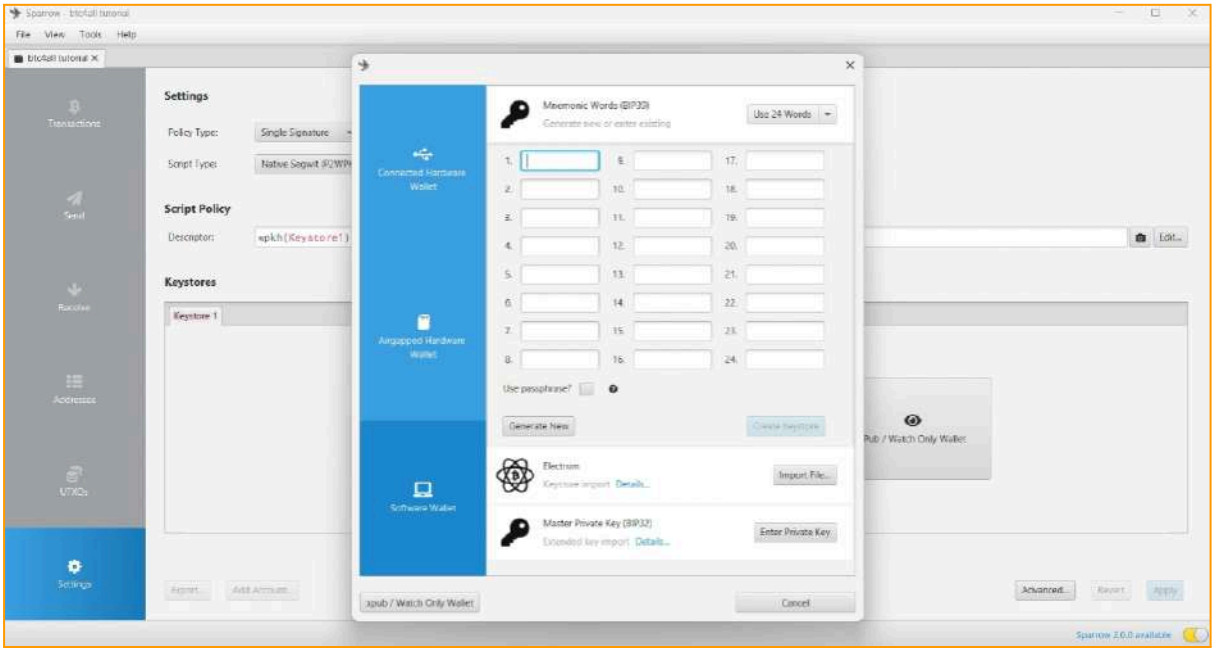
La sección "*Settings*" muestra el tipo de configuración: *single sig*, firma única. Esa configuración significa que sólo necesitas una clave para firmar transacciones desde la billetera y sólo una lista de palabras para recuperar el saldo. A continuación se indica el tipo de guión y algunos detalles técnicos más.

Mira cómo aparecen cuatro casillas en el campo "*Keystore*" con diferentes opciones. Son las formas de utilizar Sparrow. Puedes conectar tu dispositivo de billetera hardware a Sparrow y mover tus saldos a través de él. Puedes crear una billetera air gapped, donde nunca tienes que conectar el dispositivo a tu billetera para firmar las transacciones. Puedes crear desde cero o importar una billetera que ya tengas y utilizar Sparrow como billetera caliente o puedes crear una billetera "*watch only*", es decir, sólo para controlar tu saldo y no mover nada.

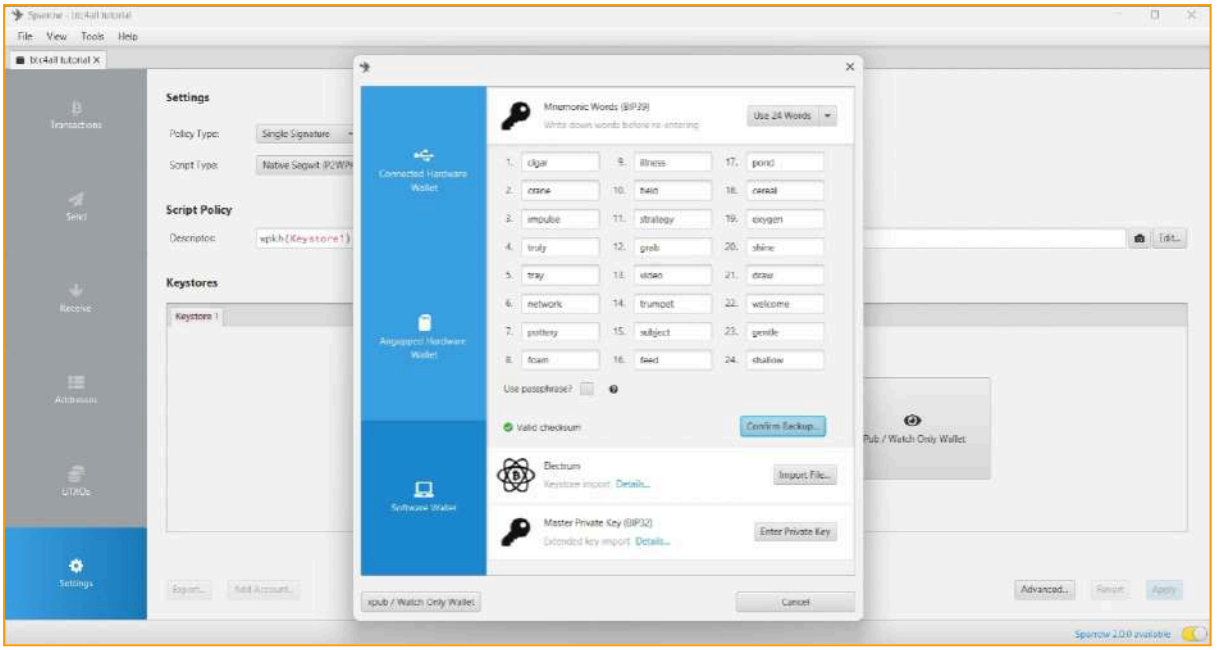
Haré clic en "*New or imported software wallet*" para crear una billetera desde cero y mostrarte cómo funciona la creación de claves.



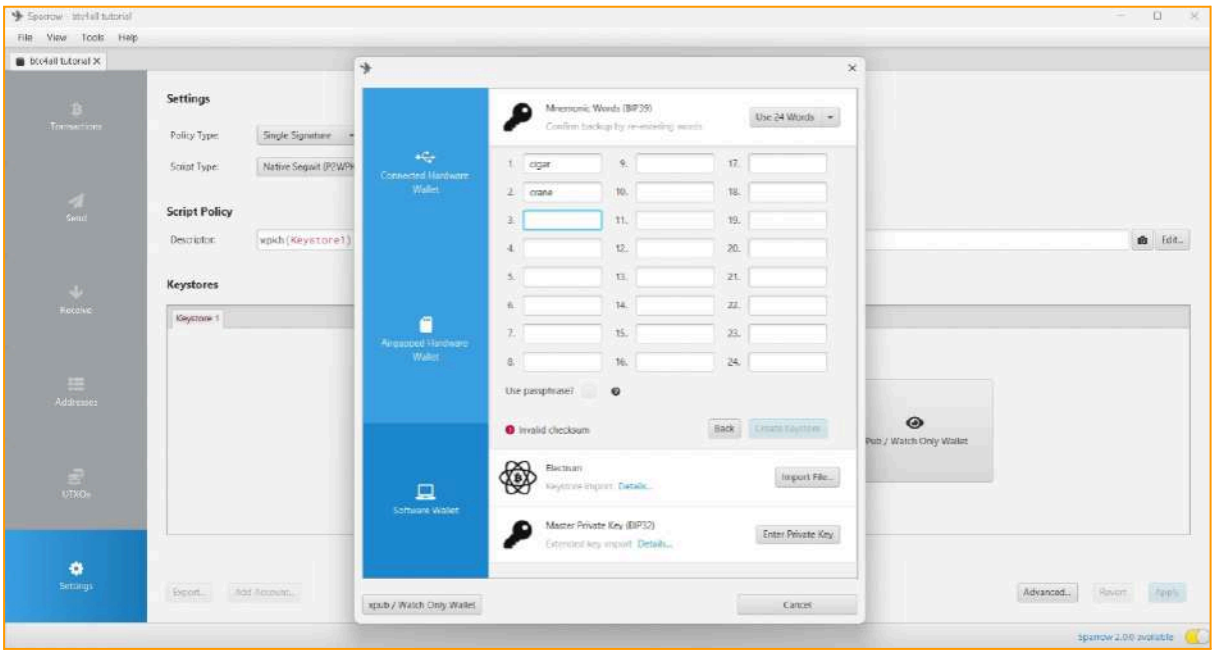
Aquí tienes algunas formas de crear palabras de recuperación de cartera. Haré clic en la primera opción, "*Mnemonic Words*", en "*Use 24 words*" para crear 24 palabras.



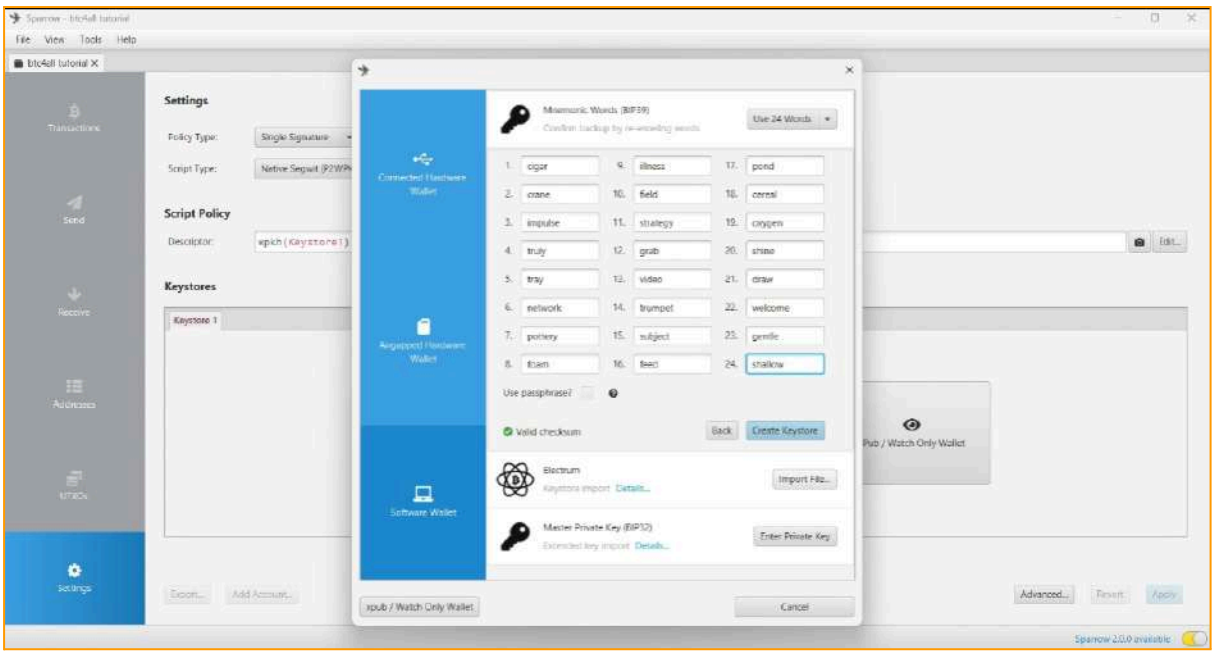
La lista de palabras vacías aparece aquí. Haré clic en "*Generate new*" y la billetera generará mis palabras.



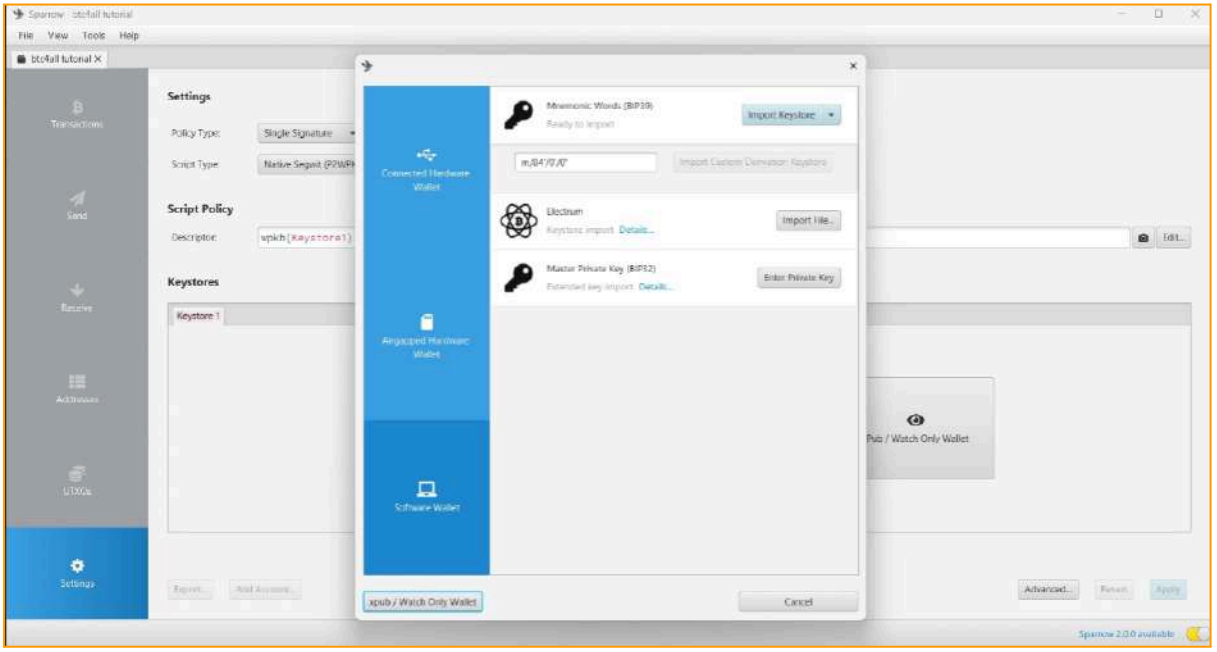
Listo. Palabras generadas. Ahora escríbelas cuidadosamente en el orden en que aparecen. Lo haré y haré clic en "*Confirm backup*" para confirmar que lo he anotado todo.



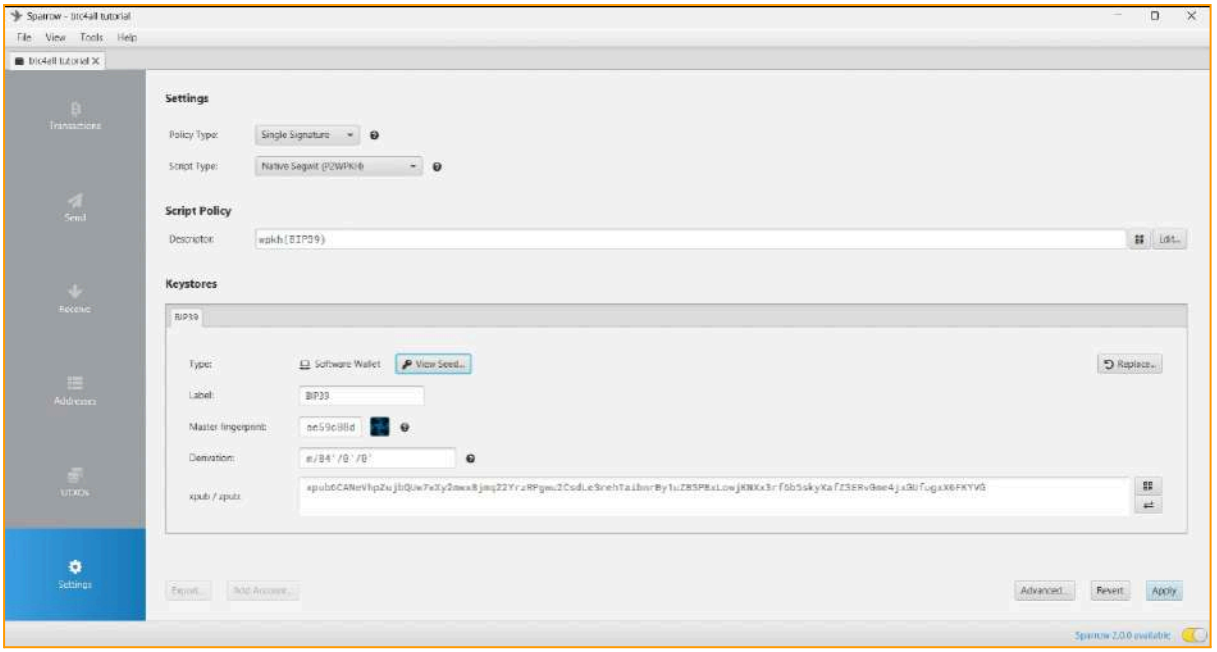
Sparrow me pide que teclee las palabras para confirmar que realmente lo he escrito todo. Ten en cuenta que hasta que no finalice el proceso, el icono "*Checksum*" aparece como no válido.



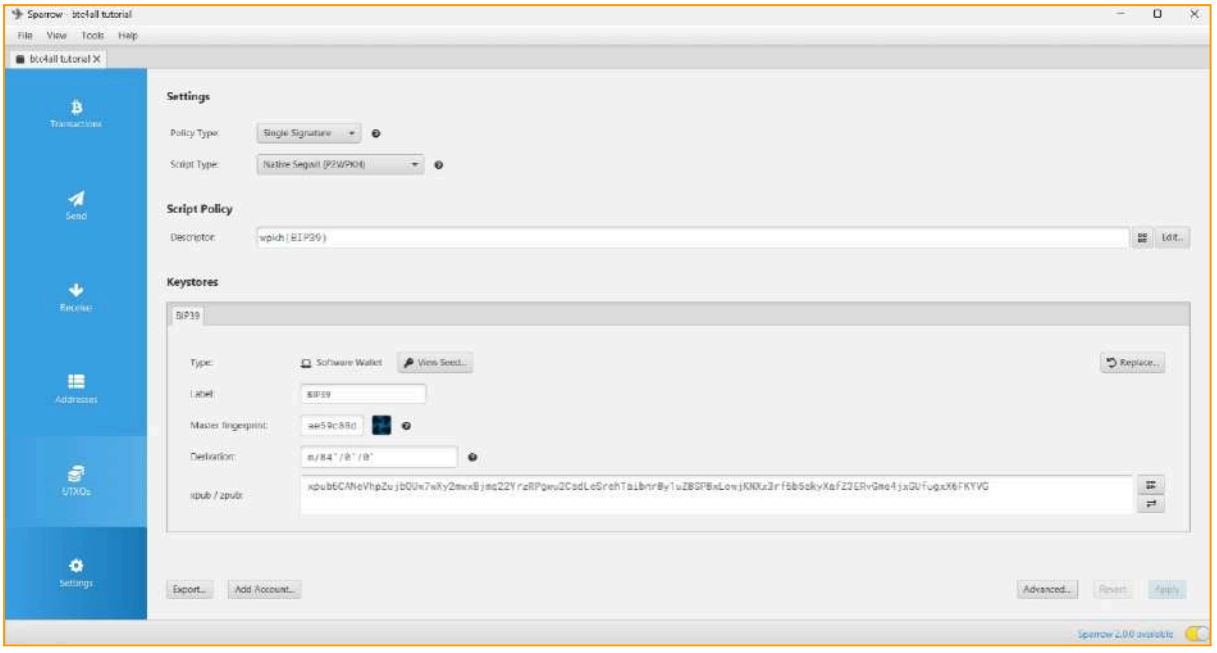
Cuando se introduce la última palabra de la frase semilla, el checksum cambia a válido, indicando que se ha introducido una secuencia de palabras válida para una billetera de Bitcoin. El siguiente paso es hacer clic en "*Create Keystore*" en el recuadro azul.



Luego haz clic en "*Import Keystore*".



Hecho. Los datos de la semilla que he generado y todas las claves se han importado. Ahora haz clic en "*Apply*" en la esquina inferior derecha de la pantalla. La billetera me preguntará si quiero crear una contraseña para proteger la billetera en caso de que alguien acceda a mi computadora. Voy a hacer clic en "*No password*", sin contraseña, pero se recomienda que tengas una contraseña para añadir otra capa de seguridad en tu billetera.

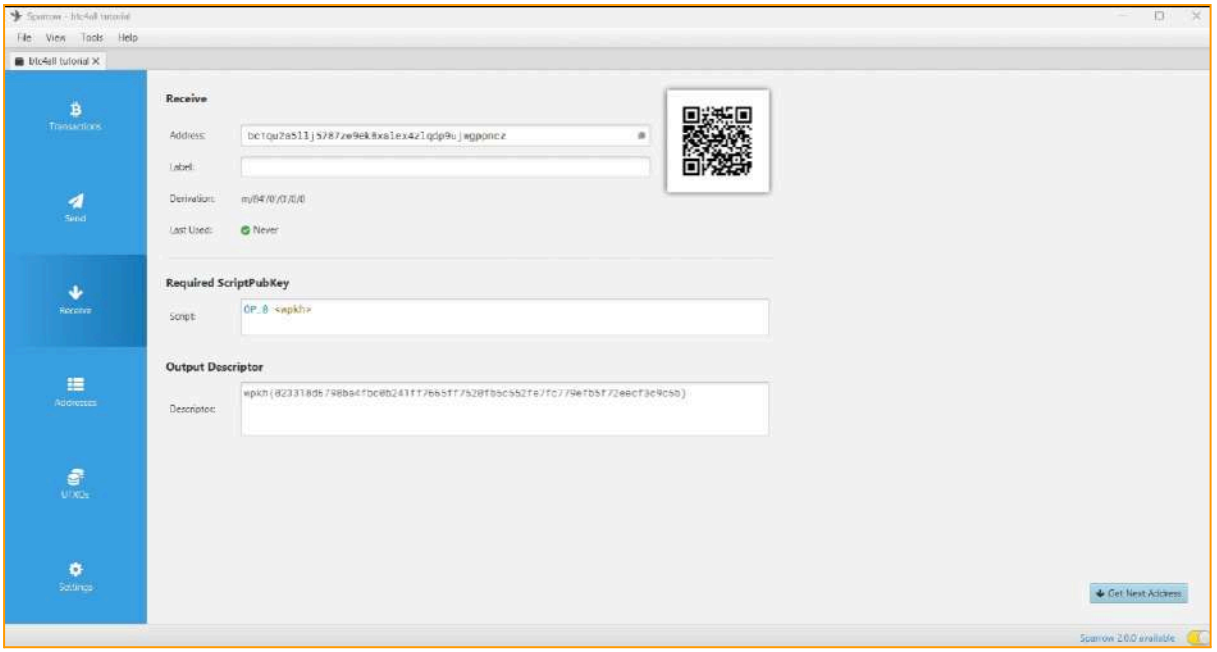


Ahora mira cómo la columna de la izquierda se ha vuelto azul de repente. Eso significa que la billetera ya está preparada para recibir bitcoin, enviar y gestionar direcciones.

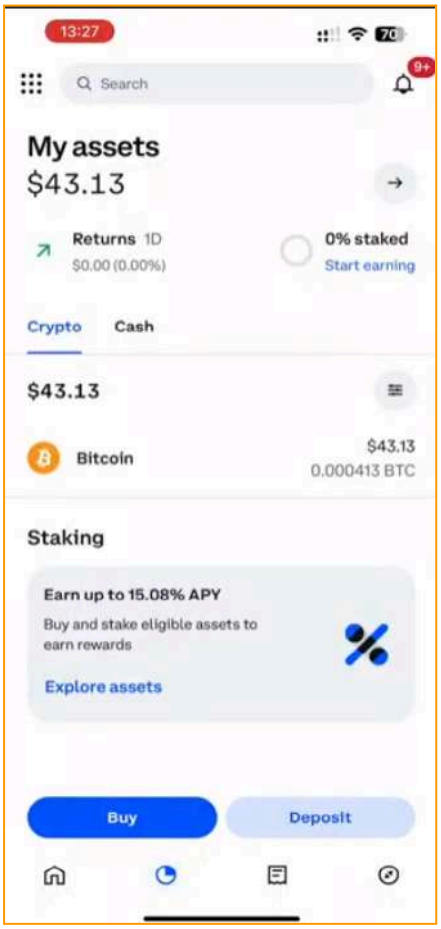
Ahora te voy a mostrar cómo enviar bitcoin a esta billetera y recuperarla para comprobar que todo va bien antes de enviar cantidades mayores. Es importante que lo hagas para que

puedas comprobar que todo funciona correctamente antes de enviar todo tu hodl a esta billetera.

Haré clic en "*Receive*", recibir.

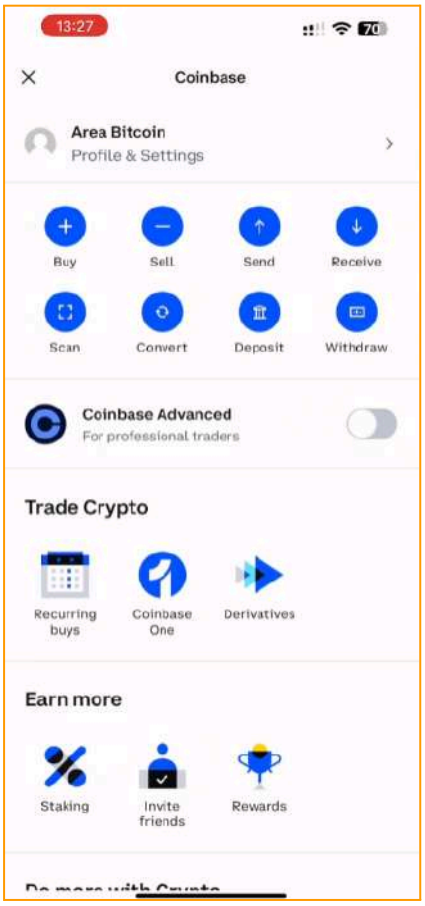


Ahora voy a copiar el código que aparece en el campo "*Address*". Esa es mi dirección en la red Bitcoin. Te mostraré cómo enviar bitcoin aquí a esta billetera recién creada. Por eso voy a sacar bitcoin del exchange. Sólo utilizaré Coinbase como ejemplo, pero el mecanismo es el mismo en otras plataformas.

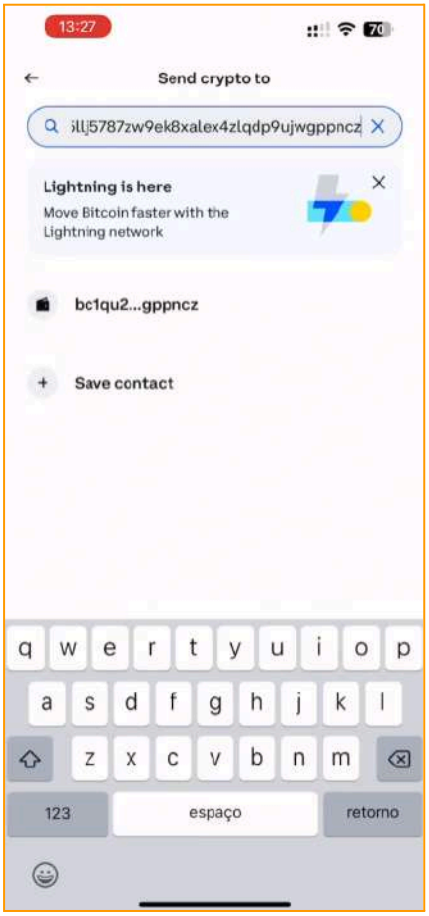


Bien, aquí tengo 43 dólares en bitcoin y voy a retirar esa cantidad del exchange.

Para ello, hago clic en la cuadrícula de la esquina izquierda de la pantalla.

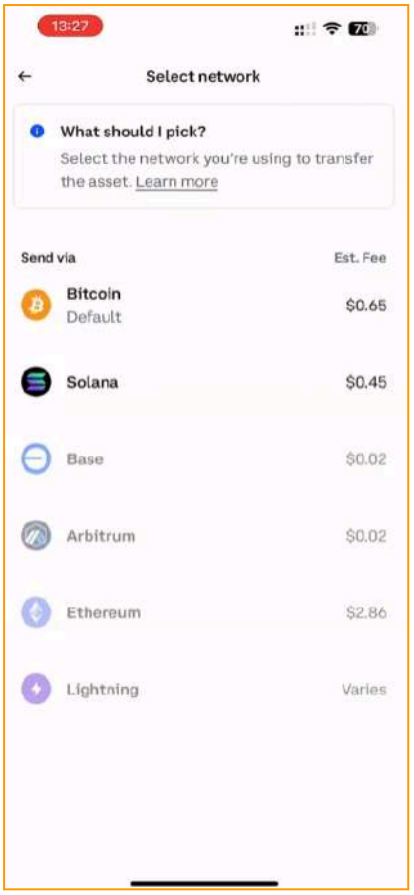


Luego sólo hay que hacer clic en "*Send*", enviar.

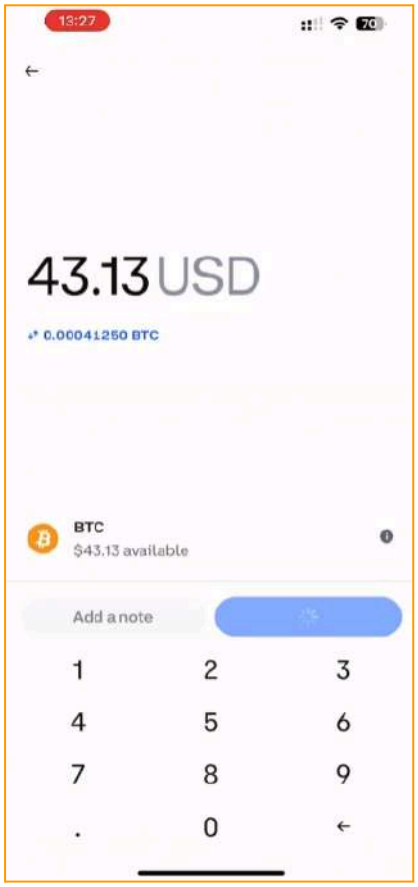


Pegaré la dirección Bitcoin de Sparrow, que ya he copiado, en este campo de la parte superior de la página.

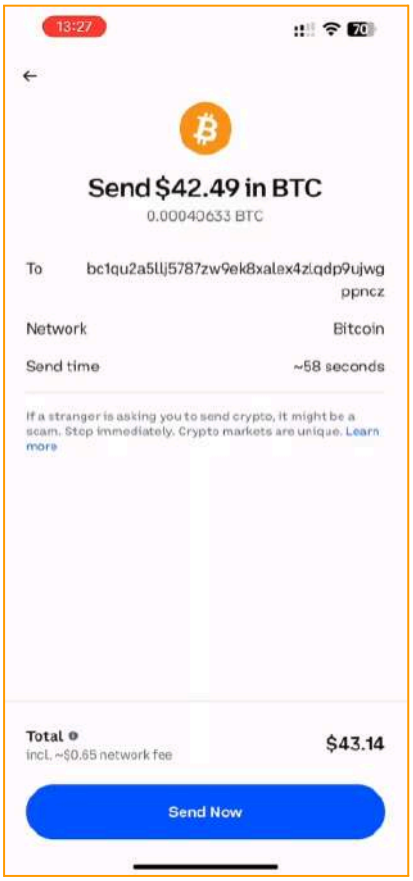
Seleccionaré Bitcoin.



A continuación, seleccionaré la red Bitcoin. Las demás redes no son Bitcoin, así que ten cuidado de no confundirlas.

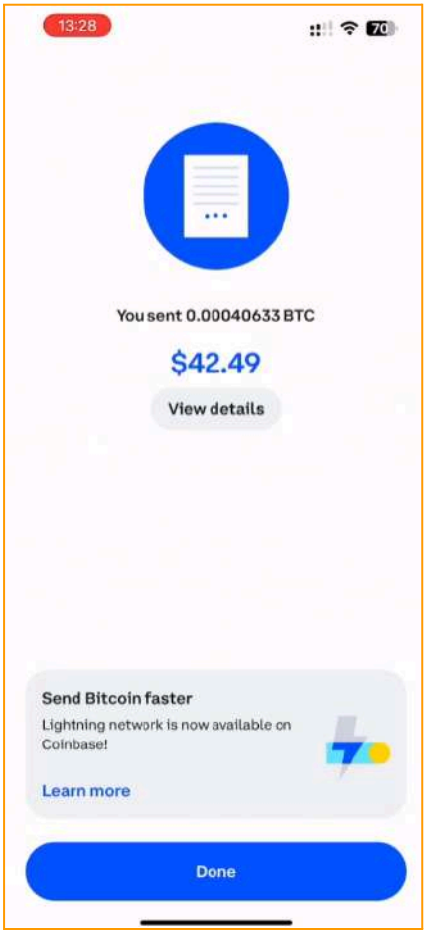


Ahora voy a introducir la cantidad que quiero retirar y a pulsar en vista previa para ver si la información es correcta.



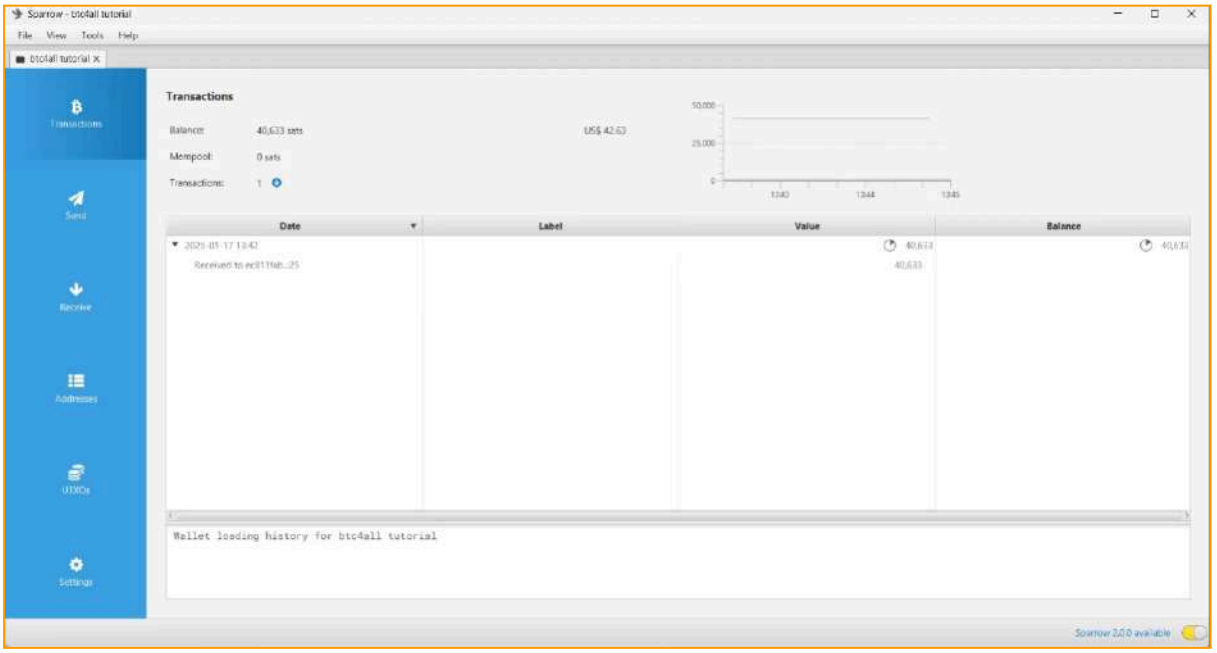
Aquí todo va bien.

Haré clic en "*Send now*", enviar ahora.



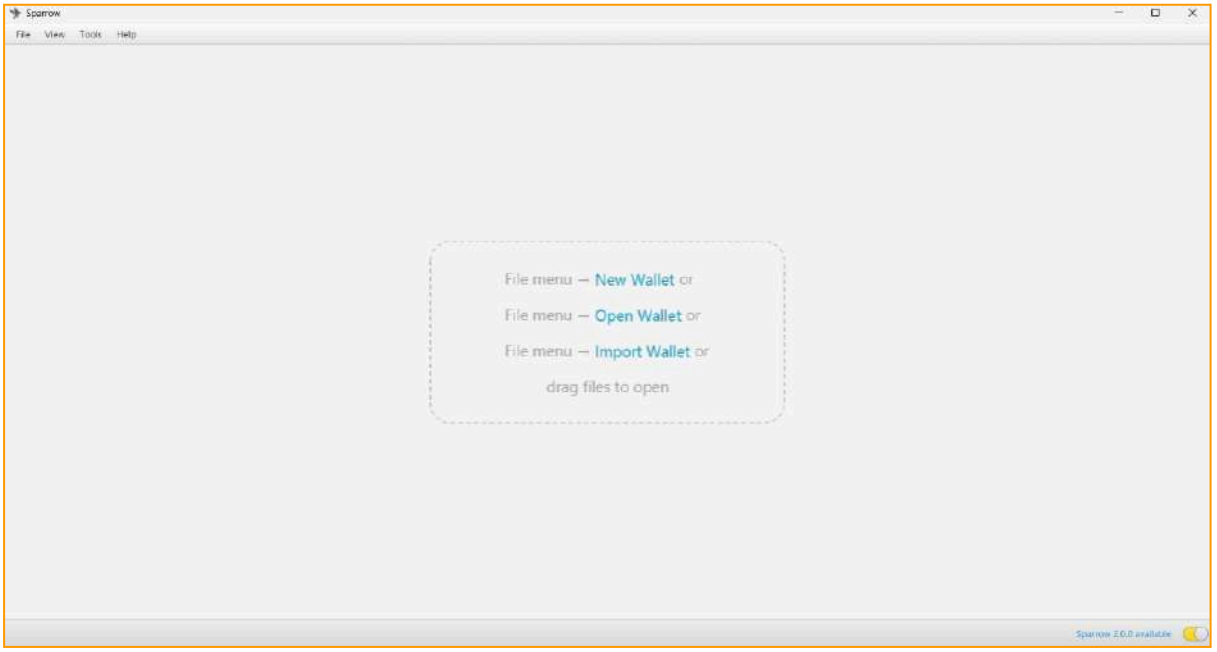
Hecho. Retirada confirmada.

Ahora acompañamos en Sparrow hasta que llegue el saldo. La red debe tardar unos minutos en procesar esta transacción.

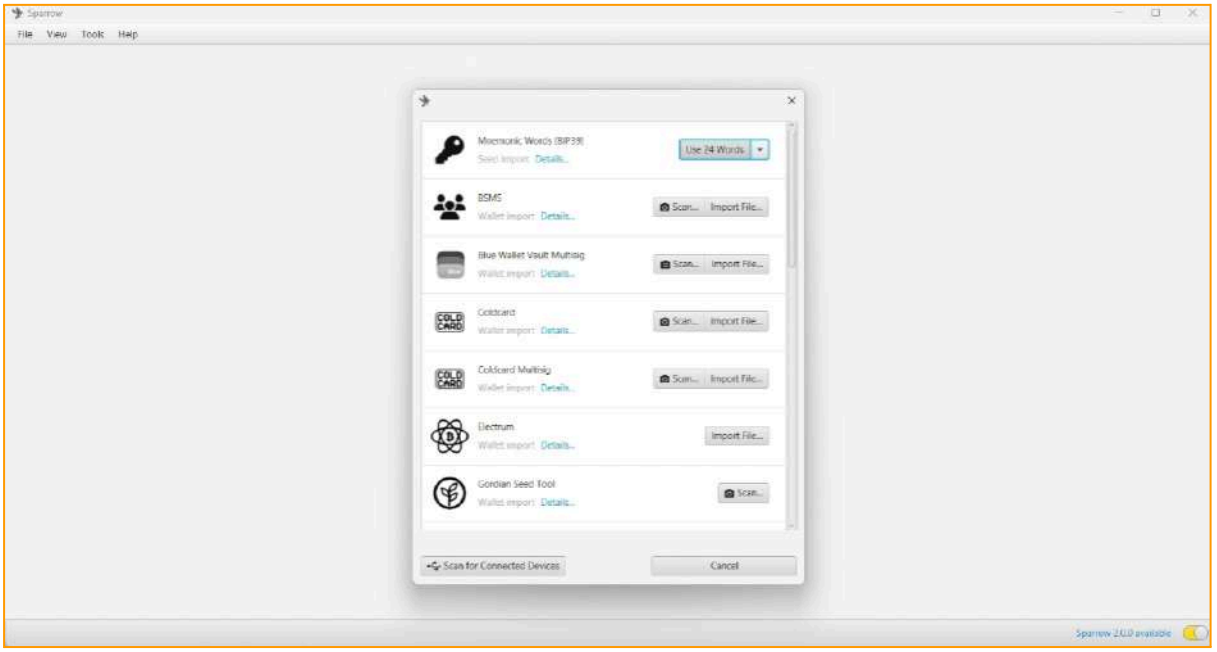


Hecho, la transacción llegó aquí a Sparrow: 40.633 satoshis están ahora bajo mi custodia.

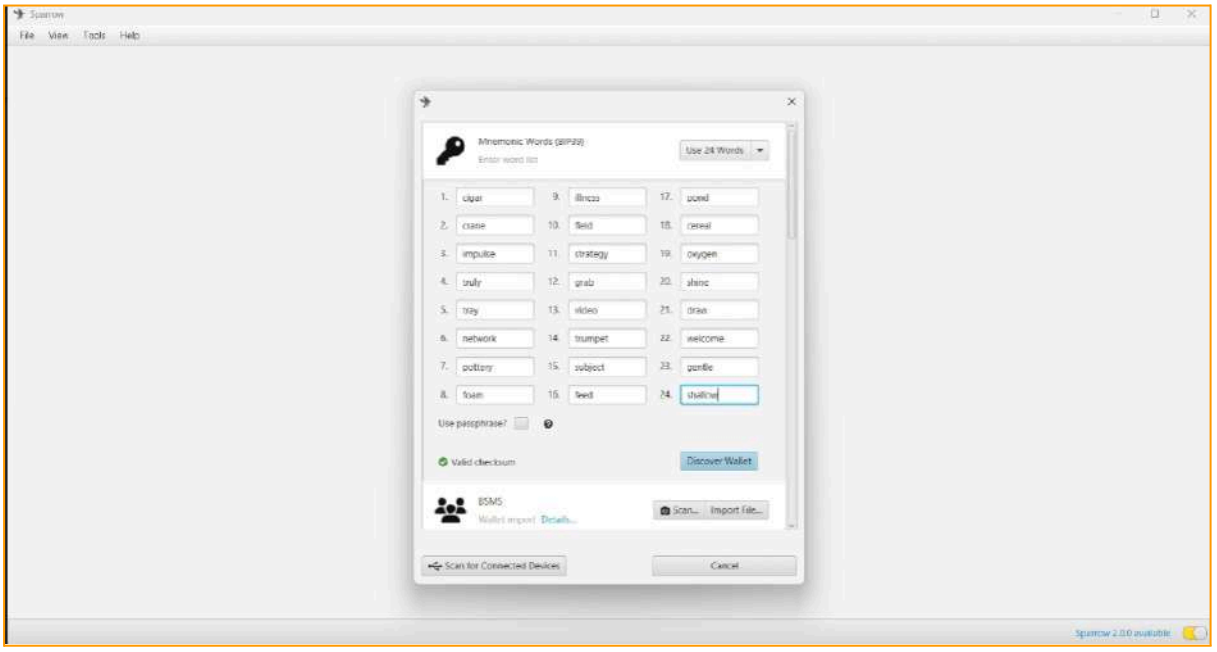
Ahora imaginemos que he perdido el acceso a este saldo en mi billetera y voy a recuperarlo desde cero. Entonces veremos si reaparece el saldo.



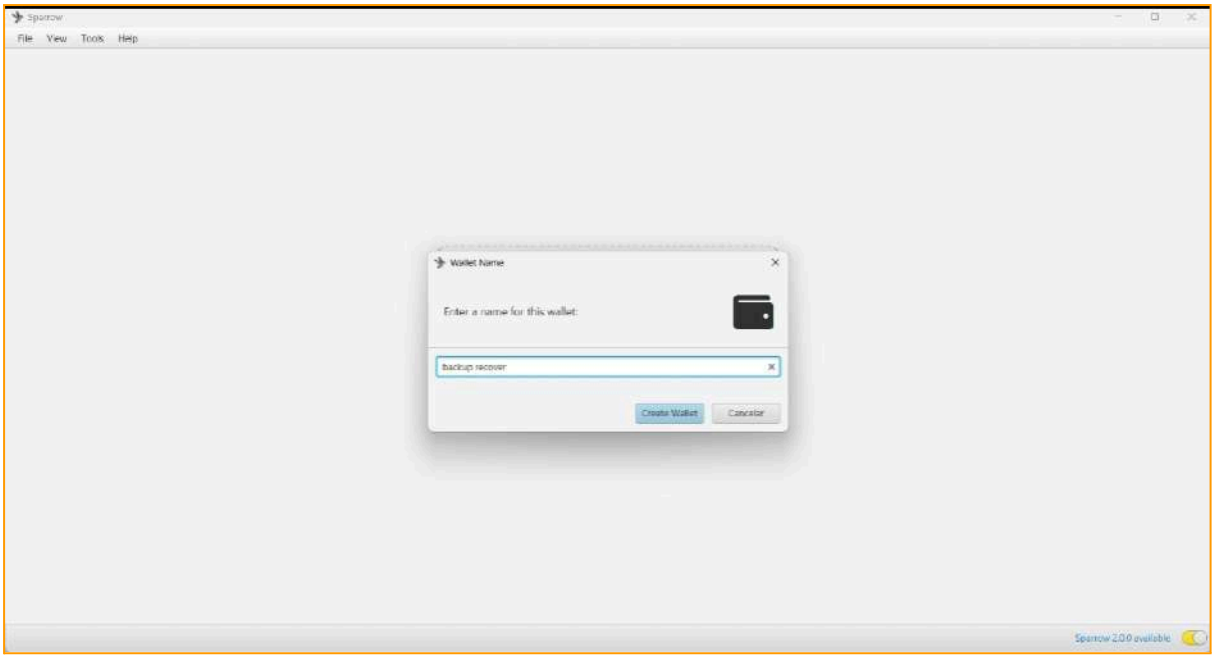
Cierro la billetera que he creado antes y hago clic en la tercera opción, "*Import wallet*", para importar la billetera.



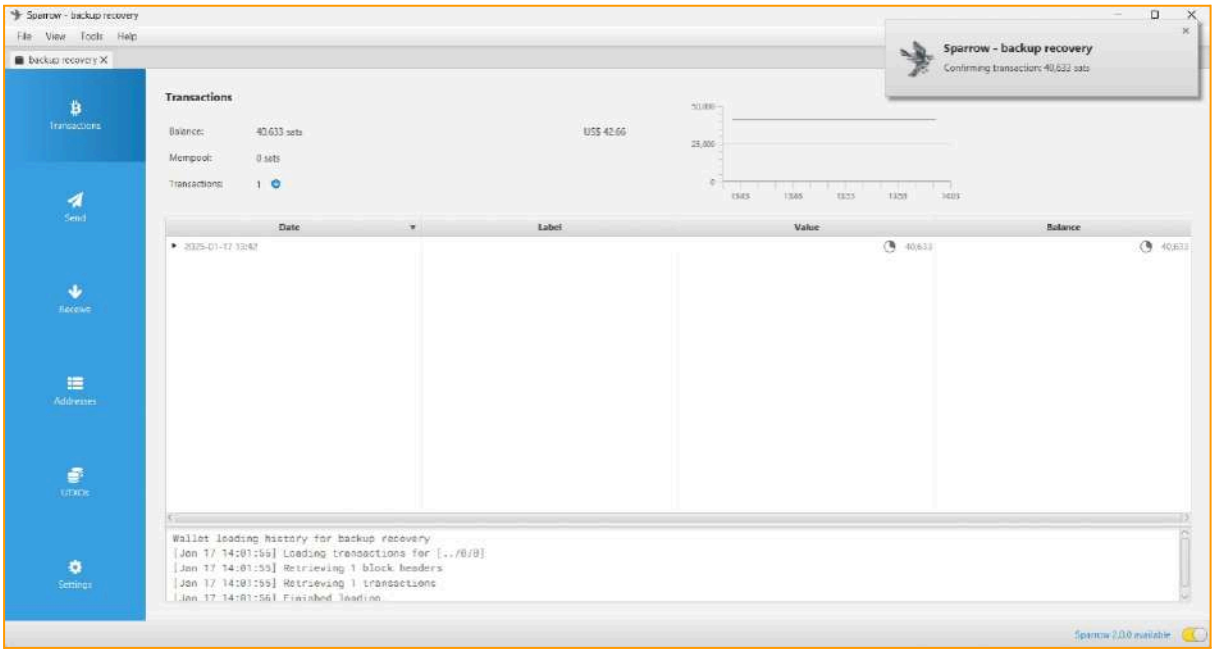
Verás varios métodos de recuperación. Me quedo con el primero, que es como generé la billetera antes, con 24 palabras.



Ahora sólo tienes que introducir las mismas palabras escritas cuando se creó la billetera anterior y hacer clic en "*Discover wallet*", descubrir billetera.

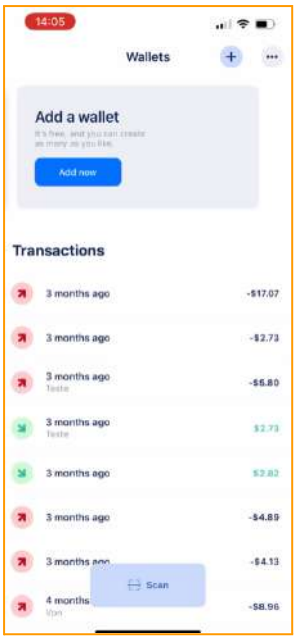


Me pedirá que cree un nombre para la billetera que quiero importar. Voy a escribir "*backup recovery*", billetera recuperada, y a hacer clic en "*Create wallet*".



Hecho. Sparrow cargó todos los datos, las claves y mi saldo de bitcoins.

Ahora voy a hacer el mismo proceso de recuperación en otra billetera Sparrow para que puedas ver cómo, independientemente de la aplicación o software que utilices, es posible recuperar tu saldo de bitcoin si tienes tu lista de palabras de copia de seguridad. Así que voy a recuperar esa misma billetera en Blue wallet, una conocida billetera para teléfonos móviles muy fácil de usar.

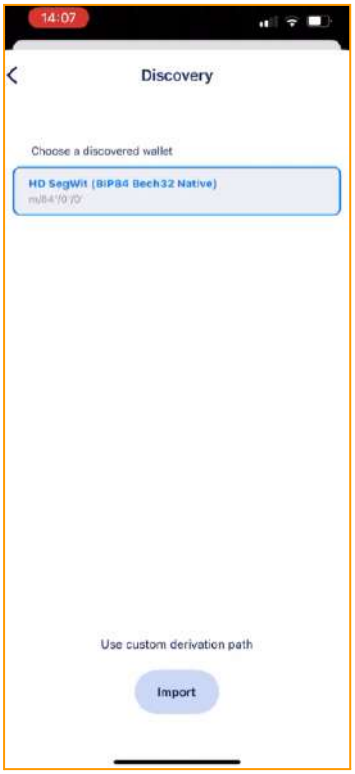


Abriré mi Blue Wallet en mi teléfono móvil y haré clic en "*Add Now*" para crear una nueva cartera.

Seleccionaré la última opción, "*Import wallet*" (importar billetera).

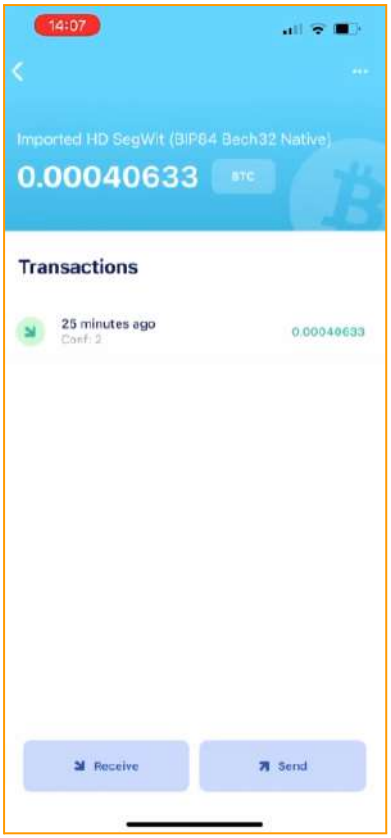
Si quieres crear una billetera desde cero, sólo tienes que seleccionar Bitcoin y hacer clic en "*Create*". Pero ahora quiero recuperar la billetera que creé en Sparrow, así que voy directamente a la opción de importar.

Voy a escribir las 24 palabras que he generado en Sparrow por orden, teniendo cuidado de escribirlas correctamente, y pulsaré "*Import*" cuando haya terminado.



Mira, Blue Wallet ha encontrado la cartera.

Haré clic en "*Import*".



Al hacer clic, se muestra el saldo que transferí desde Coinbase.

Eso es la maravilla de Bitcoin, como es open source, es decir, de código abierto, puedes recuperar tu saldo en cualquier dispositivo que siga las mismas reglas iniciales que utilizaste al generar tus claves.

Ahora que has repasado todas las lecciones de Bitcoin4All, ya puedes ensuciarte las manos y empezar a acumular y explorar el mundo de Bitcoin.

Espero que hayas disfrutado de Bitcoin4All y que esto sólo haya sido el comienzo de tu viaje de aprendizaje. Al fin y al cabo, Bitcoin no es sólo una tecnología, es un universo de conceptos que une economía, criptografía, redes descentralizadas e innovación continua. Cada día surgen nuevos desarrollos e ideas que cuestionan nuestras nociones tradicionales de dinero y soberanía.

Comparte este curso con amigos, familiares y otras personas que también sientan curiosidad y quieran aprender sobre Bitcoin.

¡Hasta la próxima y Opt Out!