Um curso de Bitcoin gratuito e de código aberto desenvolvido pela Area Bitcoin

---

Índice - Bitcoin 4 All -
Como sacar da exchange e ter soberania com o seu Bitcoin?

---

6. Enviando Bitcoin para a Carteira

6.1 Gerando um endereço na Sparrow
6.2 Sacando da Coinbase para a Sparrow
6.3 Confirmando o recebimento na carteira

---

7. Recuperando a Carteira com Sparrow

7.1 Processo de importação da carteira
7.2 Verificando o saldo reaparecendo

---

8. Recuperando a Carteira com Blue Wallet

8.1 Abrindo o app e escolhendo “import wallet”
8.2 Inserindo as palavras seed
8.3 Verificando o saldo na Blue Wallet

---

9. Bitcoin Open Source e Interoperável

9.1 Qualquer carteira compatível pode restaurar seu saldo
9.2 Bitcoin dá portabilidade e soberania real
9.3 O mesmo saldo, em diversas interfaces

---

10. Conclusão e Próximos Passos

10.1 Você está pronto para acumular e se proteger
10.2 Bitcoin é muito mais que tecnologia: é liberdade
10.3 Compartilhe o conhecimento – Opt Out!

Bitcoin 4 All - Texto Completo

Bitcoin 4 All é um curso gratuito e de código aberto criado pela Area Bitcoin. O objetivo é ajudar mais pessoas a entender o Bitcoin e inspirar qualquer pessoa a se tornar um multiplicador da educação sobre Bitcoin.

Sobre este e-book

Publicado pela Area Bitcoin – 2025

Como sacar da exchange e ter soberania com o seu Bitcoin?

Bitcoin é um divisor de águas. Ele permite que qualquer pessoa faça a própria custódia do seu próprio patrimônio e possa movimentar quando e como bem entender sem que ninguém possa impedir isso. Nenhuma empresa ou governo pode impedir que você movimente o seu próprio dinheiro ou consiga tirar de você se você guarda com soberania.

Soberania é a palavra aqui. Você é o seu próprio banco. Mas para fazer isso de fato, você precisa saber como usar ferramentas, carteiras e como sacar o seu Bitcoin das mãos desses intermediários.

Na aula anterior você aprendeu o que são carteiras de Bitcoin e porque é importante guardar bem as seeds para você sempre ter acesso ao seu saldo. O próximo passo é rechear essa carteira com Bitcoin e começar a acumular para o futuro. Então nessa aula nós vamos considerar que você já tem bitcoin e quer enviar do endereço da exchange para o endereço da sua carteira.

Mas antes de fazer isso na prática, vamos entender o que são endereços e como funciona uma transação na rede bitcoin.

(slide 256) - Bitcoin 4 All

Quando você configura a sua carteira bitcoin ela gera uma lista de palavras chamada “seed phrase”. Essas palavras representam códigos que permitem que você receba, armazene e envie bitcoin. A partir das seeds, a sua carteira vai gerar outros códigos criptografados chamados chaves públicas e privadas.

A chave privada é uma sequência de letras e números que permite assinar transações e controlar o saldo da sua carteira. Com ela você pode mover bitcoin de um endereço para outro ou importar um saldo específico. Quando você envia bitcoin de uma carteira pra outra, é a chave privada que autoriza o saldo a ser movimentado. Por isso você não deve compartilhar com ninguém a sua seed e nem as suas chaves privadas da carteira. Ela tem esse nome por isso: é privada, é uma informação que deve ficar só pra você.

A grande diferença entre seed e chave privada é que uma seed phrase (a lista de 12, 18 ou 24 palavras) pode recuperar várias chaves privadas de diversos saldos vinculados, enquanto a chave privada recupera apenas os saldos dos endereços que ela gerou. São nesses endereços que você vai receber Bitcoin.

Os endereços são gerados a partir dessas chaves e eles são públicos. Quando você faz uma transação, eles aparecem na blockchain pra qualquer pessoa verificar a sua transação. Não é possível descobrir a seed e nem a chave privada a partir de um endereço, mesmo que ele esteja aparente na blockchain bitcoin. Mas se você não cuidar bem das seeds ou chaves privadas ai sim a pessoa vai ter acesso não só aos seus Bitcoin, mas a todas as chaves e endereços gerados por ela.

(slide 257) - Bitcoin 4 All

Uma carteira pode gerar milhares de endereços diferentes a partir da chave pública. A função dela é gerar endereços. Inclusive uma das boas práticas com bitcoin é nunca reutilizar endereços. As carteiras tão sempre gerando novos endereços depois que você faz uma transação, para justamente ter mais privacidade e evitar a reutilização. Se você já usou uma carteira de bitcoin vai perceber que a cada transação o endereço muda, isso é de propósito. Afinal, depois de feita uma transação, os endereços ficam publicamente visíveis na blockchain e seria mais fácil rastrear saldos por associação.

Em resumo a chave privada desbloqueia o direito do dono da carteira gastar, mexer, transacionar as moedas associadas àquela carteira. Como o nome diz, é privada e você

não deve mostrar pra outras pessoas. Já o endereço é pra onde você vai enviar Bitcoin quando fizer uma transação. Ninguém pode adivinhar a sua chave privada a partir do seu endereço.

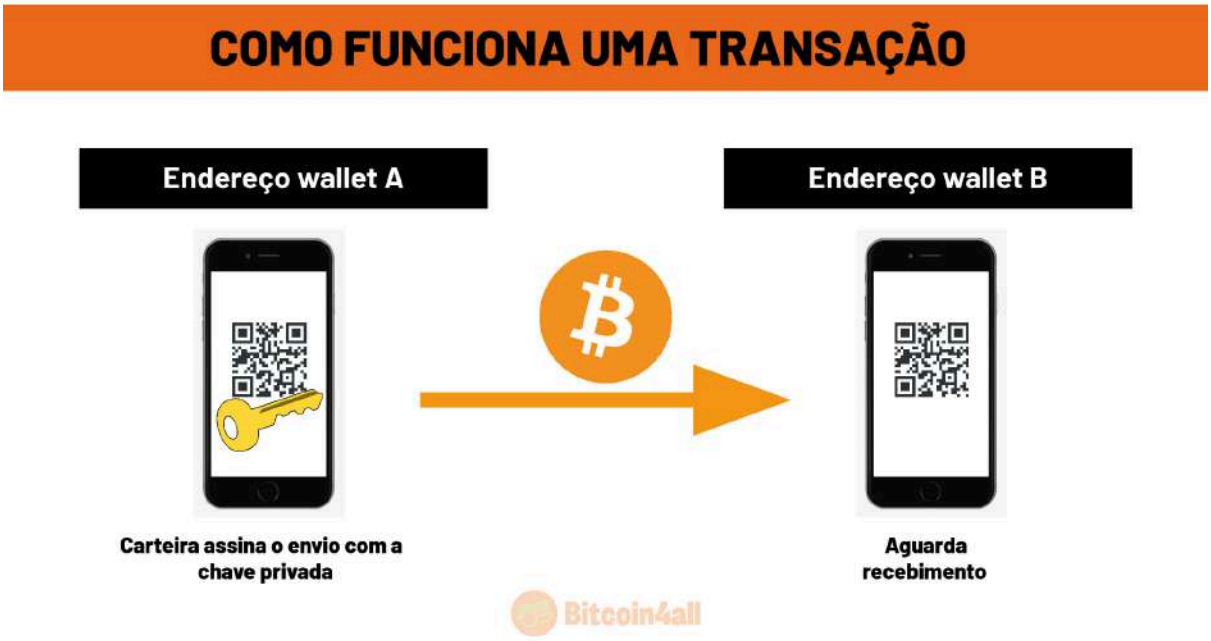
(slide 258) - Bitcoin 4 All

Eu gosto de pensar que o endereço é como se fosse o endereço da sua casa. Você até compartilha com outras pessoas, é algo relativamente público, mas também não sai com um megafone por aí contando pra todo mundo onde você mora. Você as vezes precisa mostrar o seu endereço pra receber uma entrega, mas isso não quer dizer que as pessoas vão conseguir acessar a sua casa, pra isso é preciso ter as chaves da porta. No caso das carteiras: as chaves privadas.

Então o endereço é como se fosse o endereço da sua casa e as chaves privadas é o que dá acesso ao que tem dentro dela: seu saldo em bitcoin.

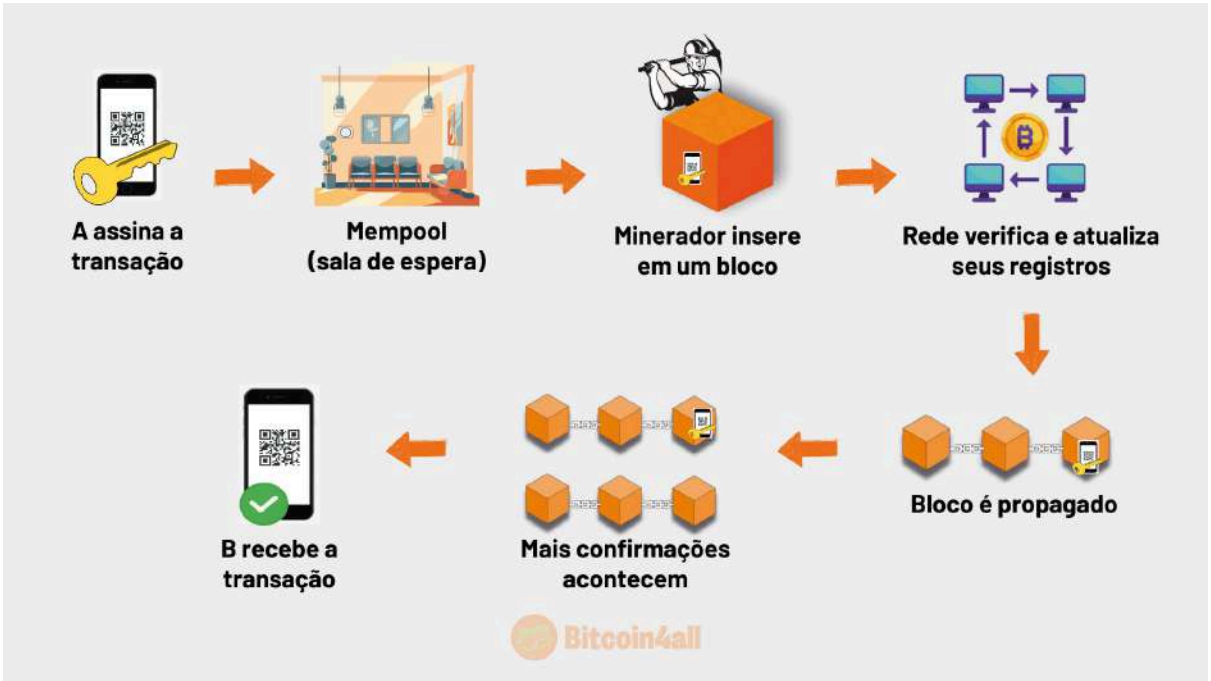
Lembrando que os seus bitcoin não ficam guardados dentro das carteiras. Eles estão sempre na blockchain. Os bitcoin estão sempre em um endereço na rede blockchain e não dentro do dispositivo em si. Quando você faz uma transferência, você diz pra rede que quer mover “x valor” em bitcoin de um endereço para outro endereço. As carteiras fazem a função de autorizar essas transações que levam os bitcoins de um endereço a outro através de uma assinatura digital feita com a chave privada.

Mas então como funciona uma transação?



(slide 259) - Bitcoin 4 All

Você abre a sua carteira, digita o valor que quer enviar, cola o endereço do recebedor e clica em enviar. Quando você clica em enviar, você está assinando a transação com a sua chave privada. É isso o que acontece por trás dos códigos da carteira.



(slide 260) - Bitcoin 4 All

Quando você assina a transação provando pra rede bitcoin que é o verdadeiro dono da chave privada do endereço da carteira, essa transação vai para uma sala de espera,

conhecida como mempool. Essa é a sala de espera das transações que ficam aguardando até serem inseridas em um bloco pelos mineradores. As transações são registradas em blockchain quando um minerador seleciona as transações para fazerem parte do bloco de informação. Assim que um minerador inserir a transação em um bloco, esse bloco é verificado pela rede e ela atualiza os seus registros da blockchain. Aí então esse bloco é propagado por toda a rede como um bloco válido, com a transação dentro dele.

Quando uma transação é inserida em um bloco se fala que ela teve uma confirmação. Conforme mais blocos são minerados, mais confirmações acontecem. Geralmente uma transação é considerada irreversível depois de 6 confirmações, quando seis blocos se passam. Quando as confirmações acontecem, a carteira notifica o usuário, a transação é considerada recebida e o saldo fica disponível para ser gasto. É assim que as transações on chain acontecem quando você faz um envio de bitcoin.

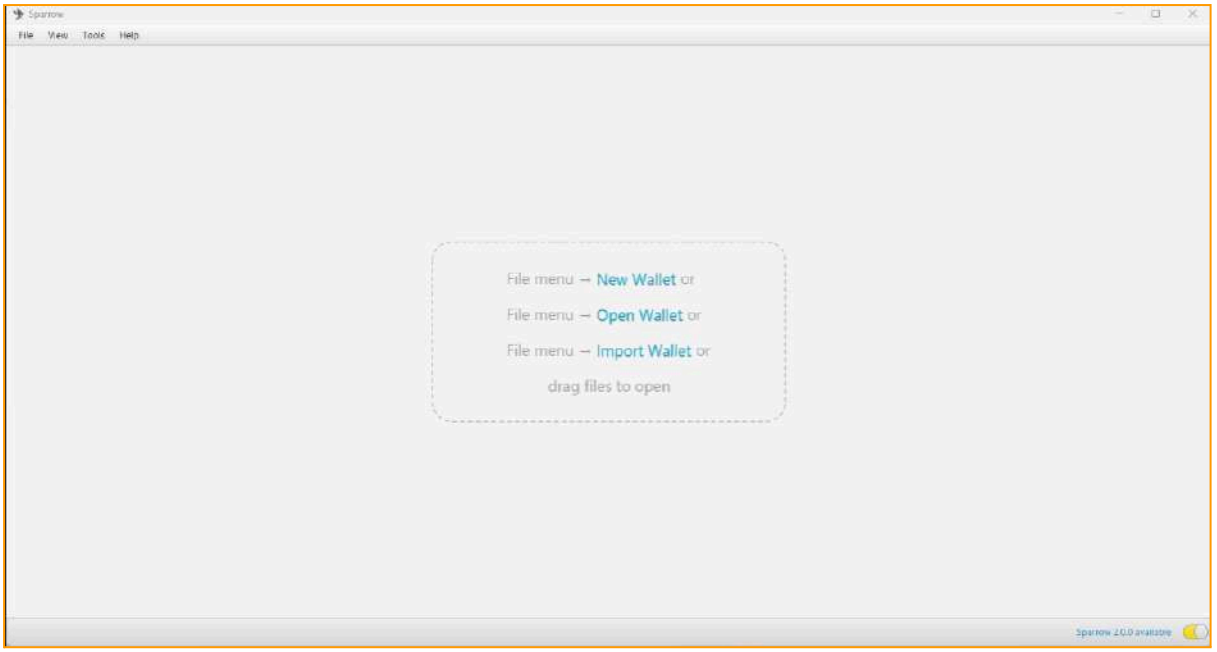
Bom, agora que você já entendeu a teoria, vamos pra prática!

Eu vou mostrar agora pra você como configurar uma carteira do zero, sacar Bitcoin da exchange para essa carteira e recuperar o saldo usando a seed phrase.

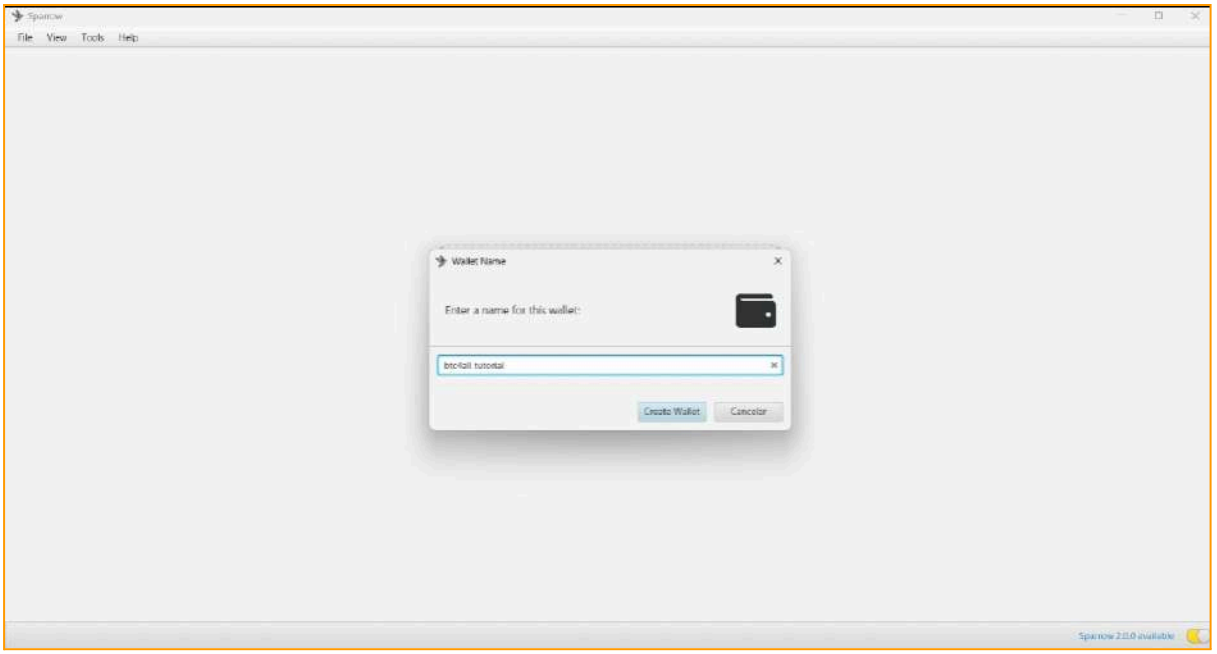
Pra esse tutorial nós escolhemos usar a Sparrow Wallet, porque é uma carteira muito versátil e completa tanto para iniciantes quanto para usuários avançados. Ela é auto custodial, de código aberto e funciona muito bem como carteira coordenadora entre diversas marcas de carteiras hardware: jade, ledger, trezor, coldcard, seed signer, krux… enfim… praticamente todas as hardwares funcionam com a Sparrow. A diferença é que as carteiras que tem um software próprio como ledger e trezor, de qualquer forma pedem que você baixe o software ledger live ou o trezor suite para fazer as atualizações de firmware do dispositivo antes de conectar com a Sparrow.

Ela também oferece recursos como criar multisigs, fazer transações air gapped, PSBT, gerenciar e consolidar UTXO, possibilidades que focam em aumentar segurança e privacidade da carteira. Lembrando então que a Sparrow é uma carteira apenas de desktop, não tem um aplicativo para celulares nem IOS e nem Android. Eu vou deixar o link aqui na tela para você baixar e também uma lista com outras carteiras para você testar e ver qual você se adapta melhor.

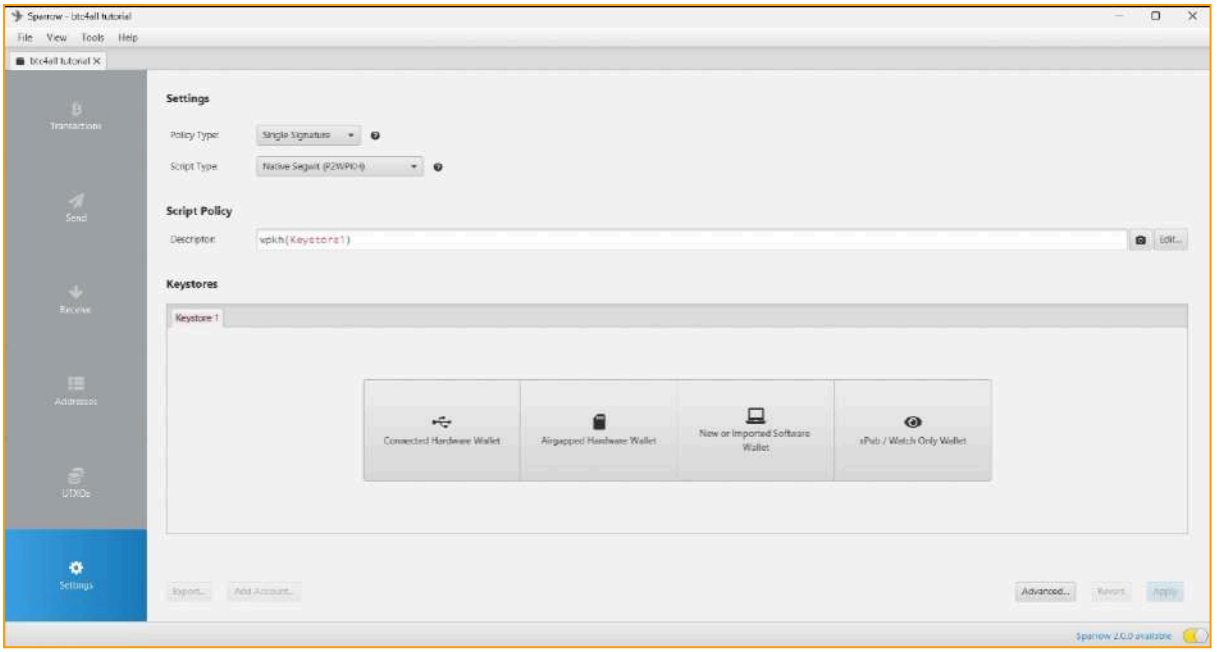
Vamos começar configurando a Sparrow. O primeiro passo é baixar a Sparrow e instalar o software.



Aí é só abrir a Sparrow e clicar em “new wallet” para criar uma nova carteira.



Agora é só escolher um nome personalizado para essa carteira, vou digitar “btc4all tutorial” e clicar em “create wallet”.

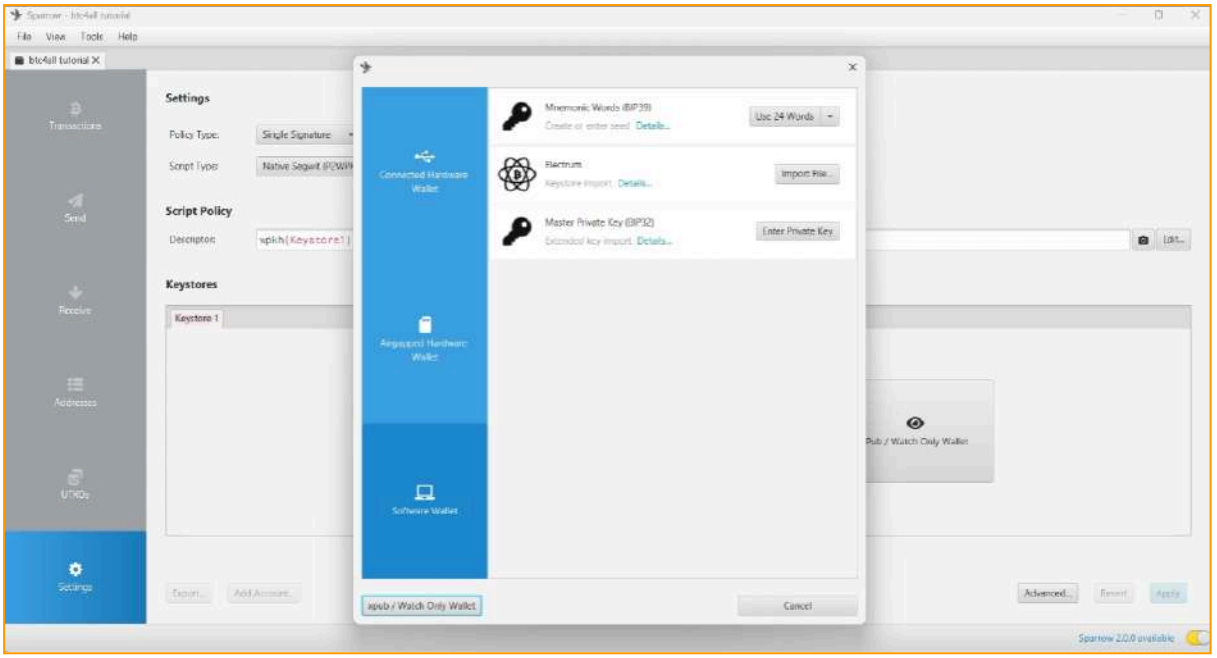


Essa é a página inicial da Sparrow. Observa como a coluna da esquerda tá cinza e só as configurações estão em azul. Significa que ela está zerada e é preciso criar uma carteira, importar ou conectar uma para que você consiga acompanhar saldos, receber e enviar Bitcoin.

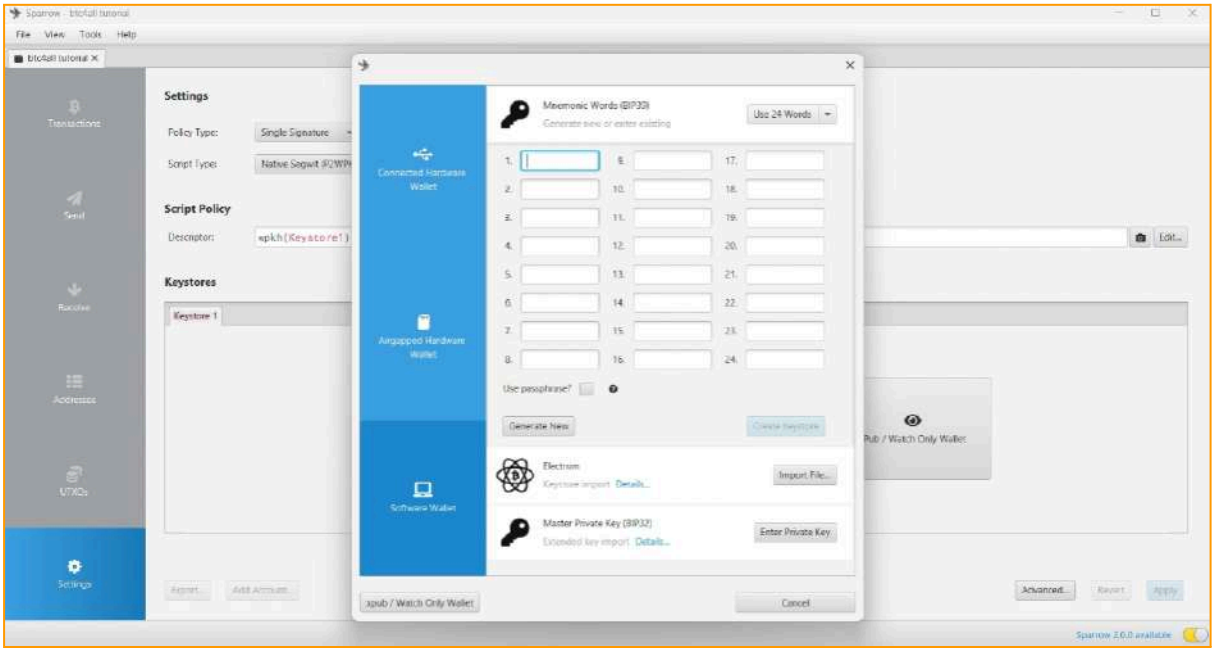
Ali em “settings” mostra o tipo de configuração: single sig. Essa configuração significa que você precisa de apenas uma chave para assinar as transações dessa carteira e apenas uma lista de palavras para recuperar o saldo. Abaixo aparece o tipo de script e mais alguns detalhes técnicos.

Observa como no campo keystore aparecem quatro caixas com diferentes opções. Essas são formas de usar a Sparrow. Você pode conectar o seu dispositivo hardware wallet na Sparrow e movimentar os saldos através dela. Você pode criar uam carteira air gapped em que você nunca precisa plugar o dispositivo no computador para assinar as transações. Você pode criar do zero ou importar uma carteira que você já tenha e usar a Sparrow como uma hot wallet ou você pode criar uma carteira watch only, para apenas acompanhar o saldo e não movimentar nada.

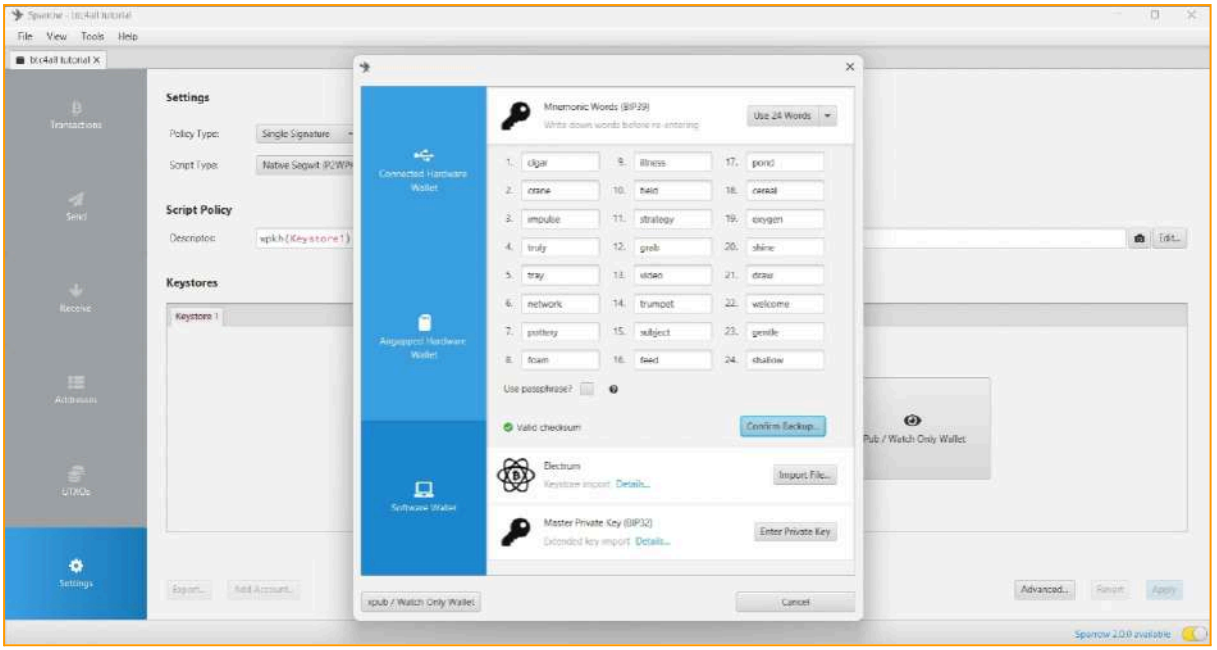
Eu vou clicar em “New or imported software wallet” para criar uma carteira do zero e te mostrar como funciona a criação das chaves.



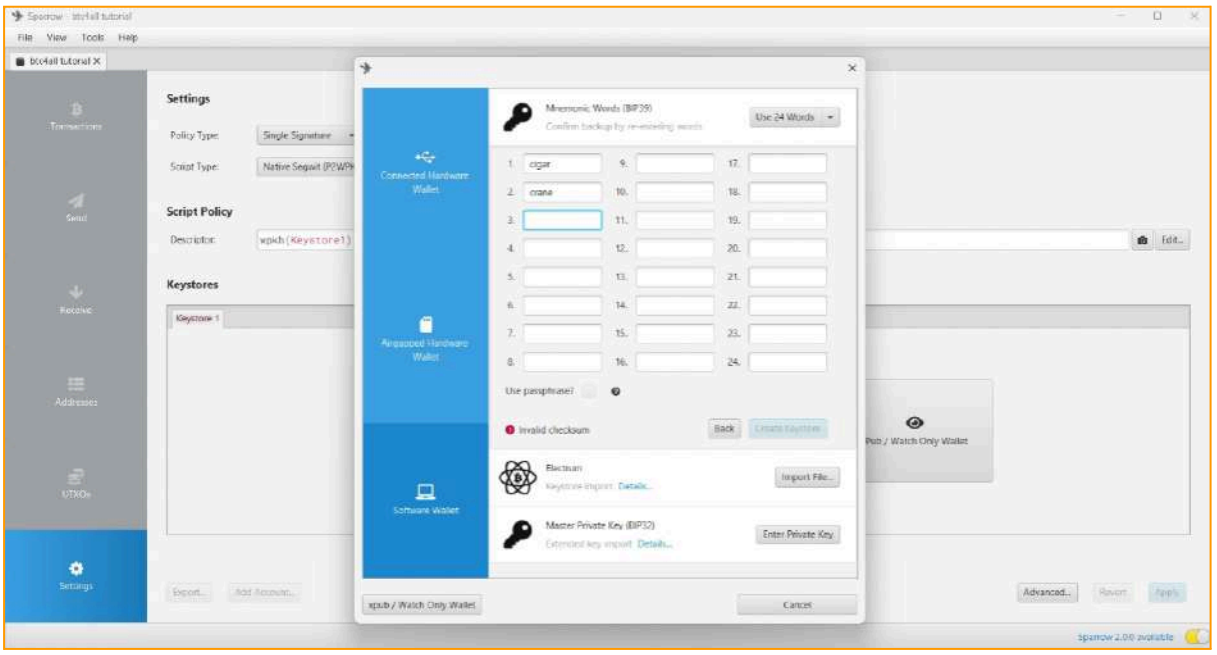
Aqui aparecem algumas formas de criar as palavras de recuperação da carteira. Eu vou clicar na primeira opção Mnemonic Words em “use 24 words”.



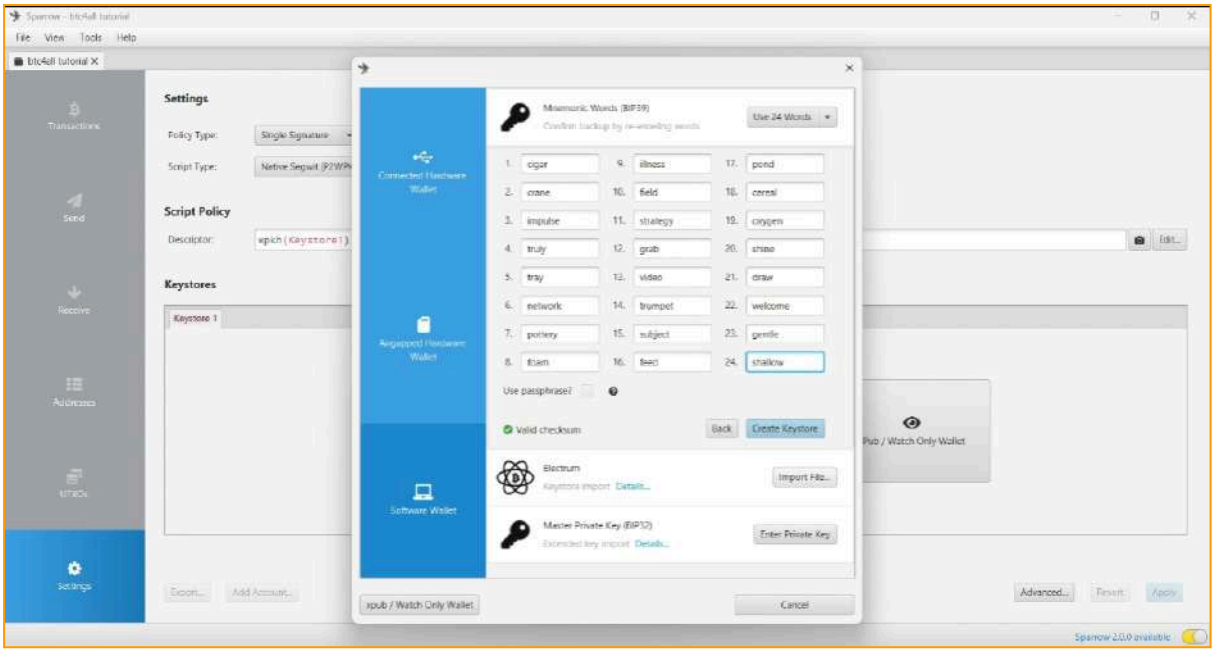
Aqui aparece a lista de palavras vazias. Vou clicar em “Generate new” para a carteira gerar as minhas palavras.



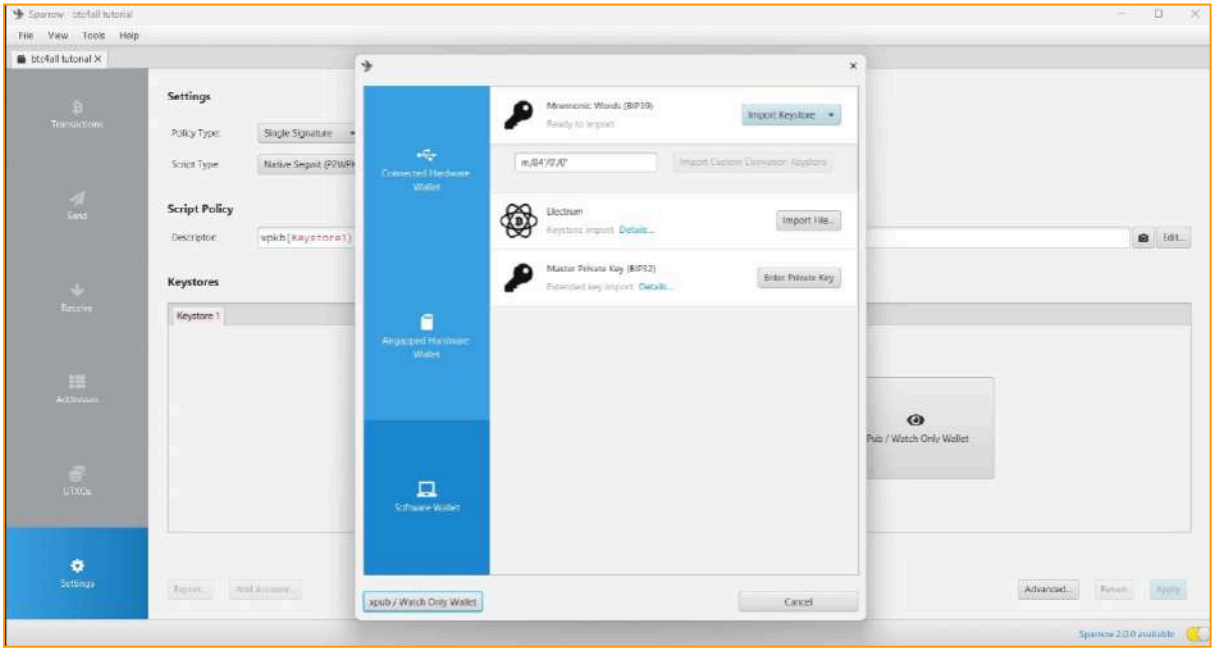
Palavras geradas. Agora é só anotar elas com cuidado na ordem em que aparecem. Vou fazer isso e clicar em “Confirm Backup” para confirmar que eu anotei tudo.



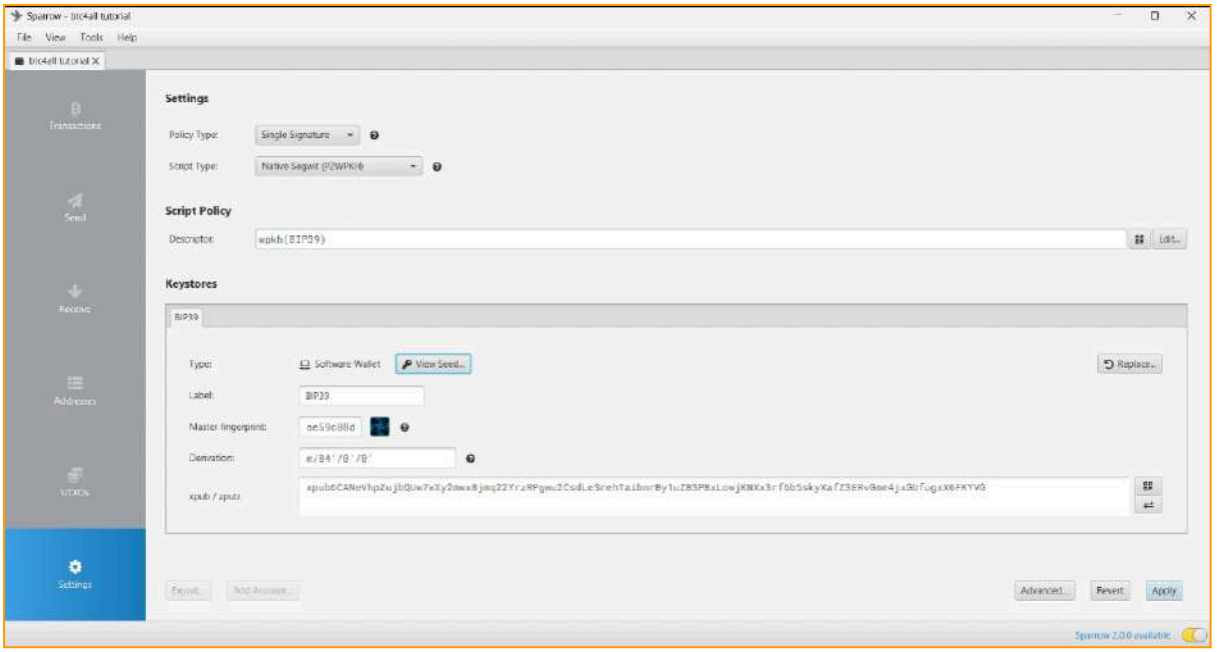
A Sparrow pede pra digitar as palavras e assim confirmar que eu realmente anotei tudo. Observa que até eu finalizar o processo o ícone “Checksum” aparece como inválido.



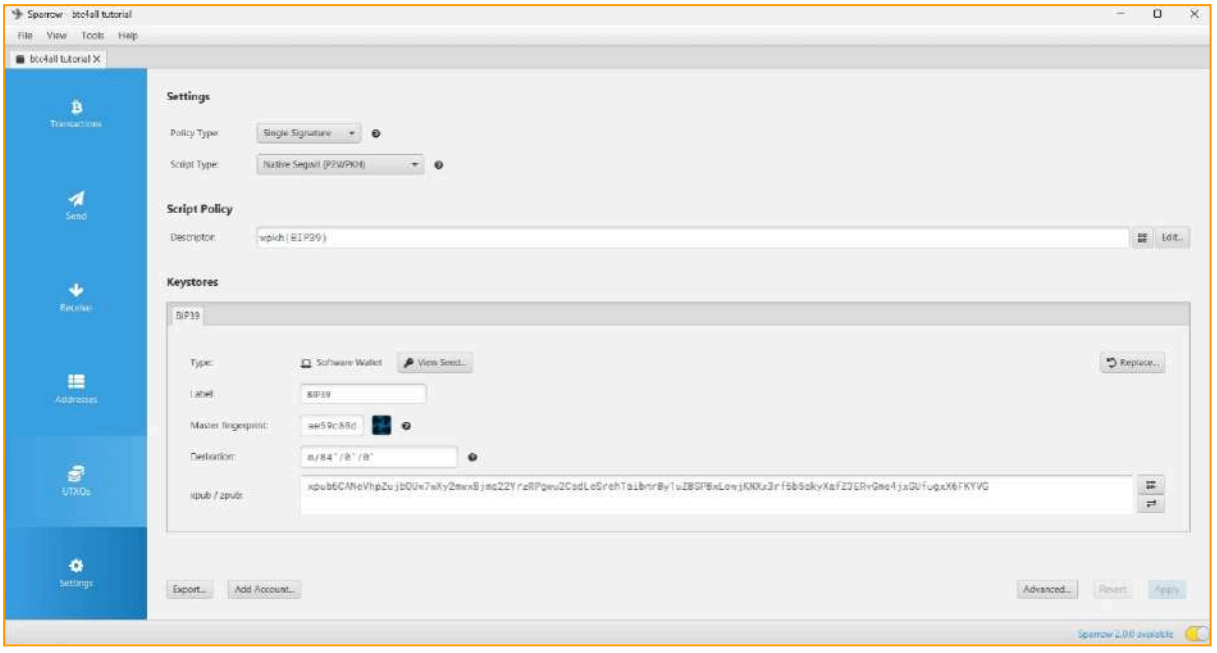
Ao inserir a última palavra da seed phrase, o checksum muda para válido, sinalizando que foi inserida uma sequência de palavras válida para uma carteira de Bitcoin. O próximo passo é clicar em “Create Keystore” no box azul.



E depois em “import keystore”.



Feito. Os dados da seed que eu gerei e todas as chaves foram importados. Agora é só clicar em “Apply” no canto direito inferior da tela. A carteira vai perguntar se eu quero criar uma senha para proteger a carteira caso alguém tenha acesso ao meu computador. Eu vou clicar “no password”, sem senha, mas é indicado que você tenha uma senha para ter mais uma camada de segurança na sua carteira.

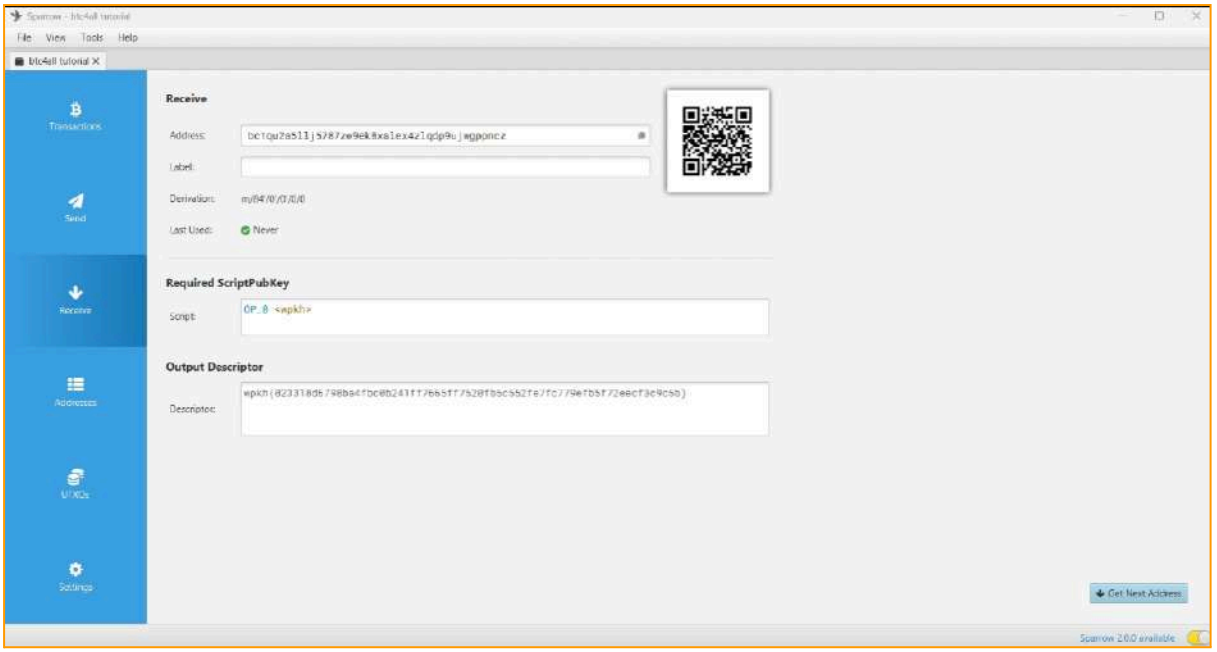


Observa agora como a coluna da esquerda de repente ficou azul. Quer dizer que agora a carteira está pronta para receber Bitcoin, enviar e gerenciar endereços.

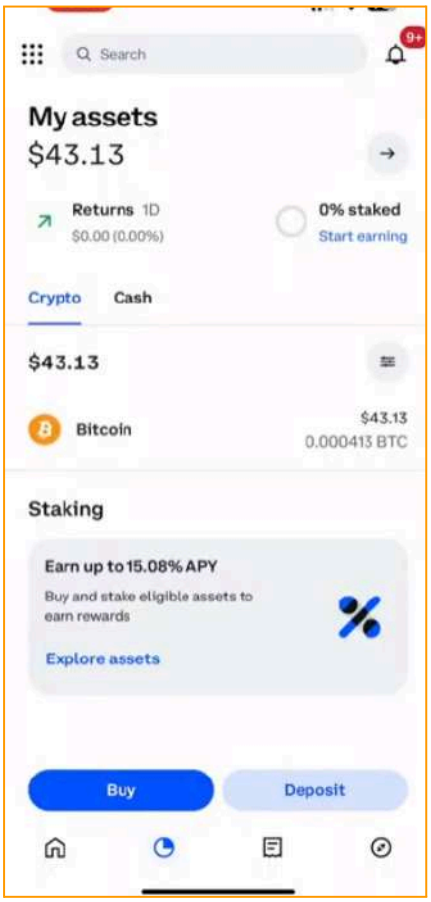
Bom, agora eu vou mostrar como você vai enviar Bitcoin para essa carteira e recuperar ela para testar se está tudo certo antes de enviar valores maiores. É importante fazer isso para

você identificar se está tudo funcionando direitinho antes de enviar todo o seu hodl para essa carteira.

Eu vou clicar em “receive”, receber.

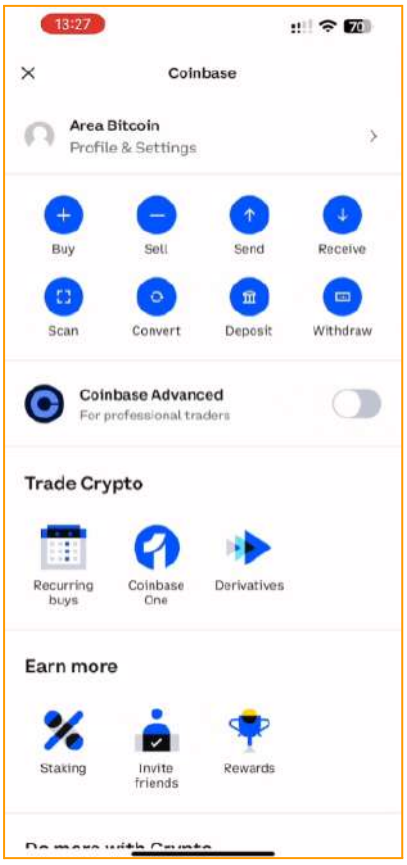


E vou copiar esse código que aparece no campo “address”. Esse aqui é o meu endereço na rede Bitcoin. E vou mostrar como você vai enviar Bitcoin aqui pra essa carteira recém criada. Pra isso eu vou sacar Bitcoin da exchange. Vou usar a Coinbase apenas como exemplo, mas o mecanismo é o mesmo em outras plataformas.

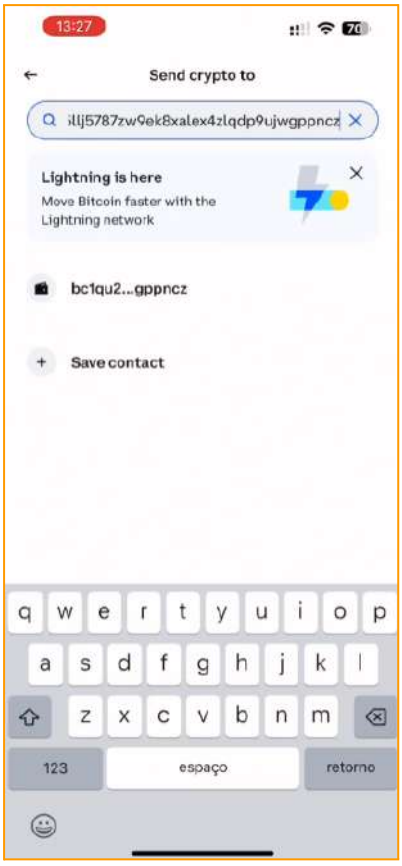


Bom, aqui eu tenho 43 dólares em Bitcoin, cerca de 260 reais, e vou sacar esse valor da corretora.

Pra isso eu vou clicar na grade no canto esquerdo da tela.

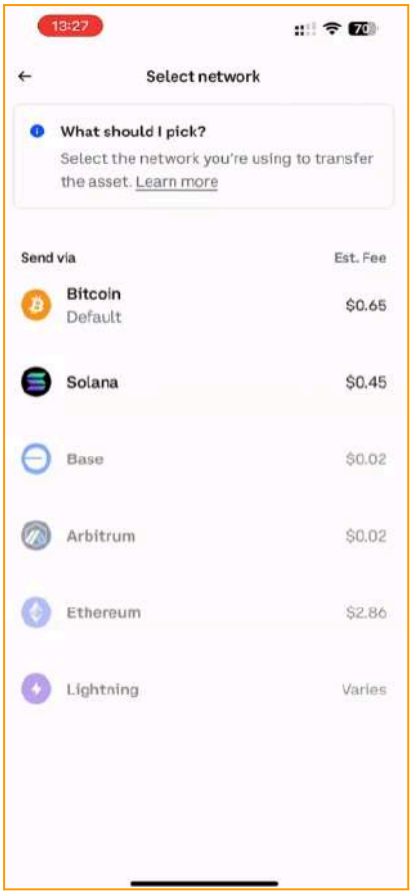


Depois clicar em “send”, enviar.

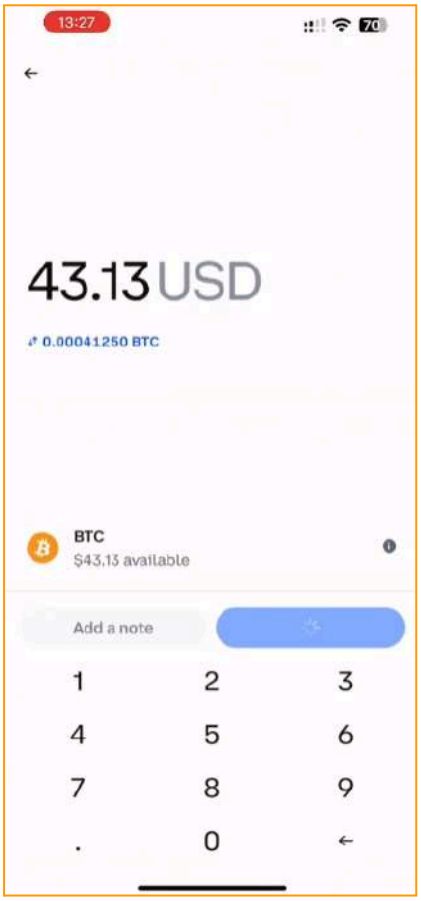


Vou colar o endereço bitcoin da Sparrow, que eu já tinha copiado, aqui nesse campo no topo da página.

Vou selecionar Bitcoin.



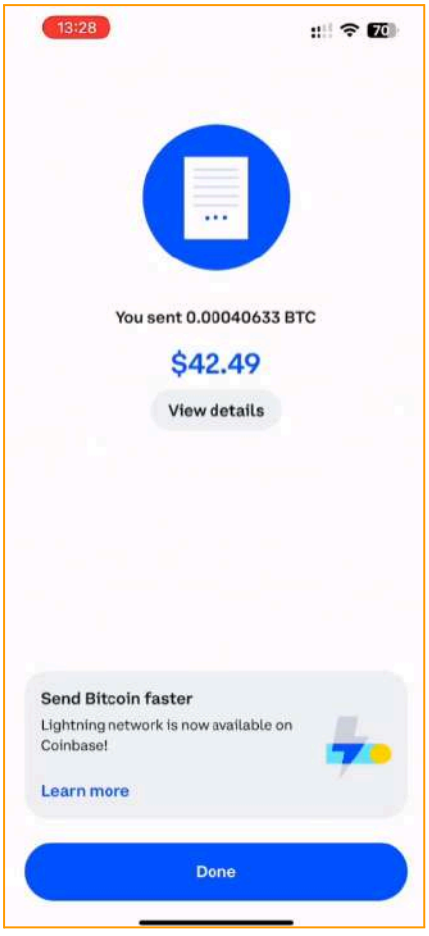
Depois selecionar pela rede Bitcoin. Todas as outras redes não são Bitcoin, cuidado pra não confundir.



Agora vou Inserir o valor que eu quero sacar e clicar em preview para ver se as informações estão corretas.

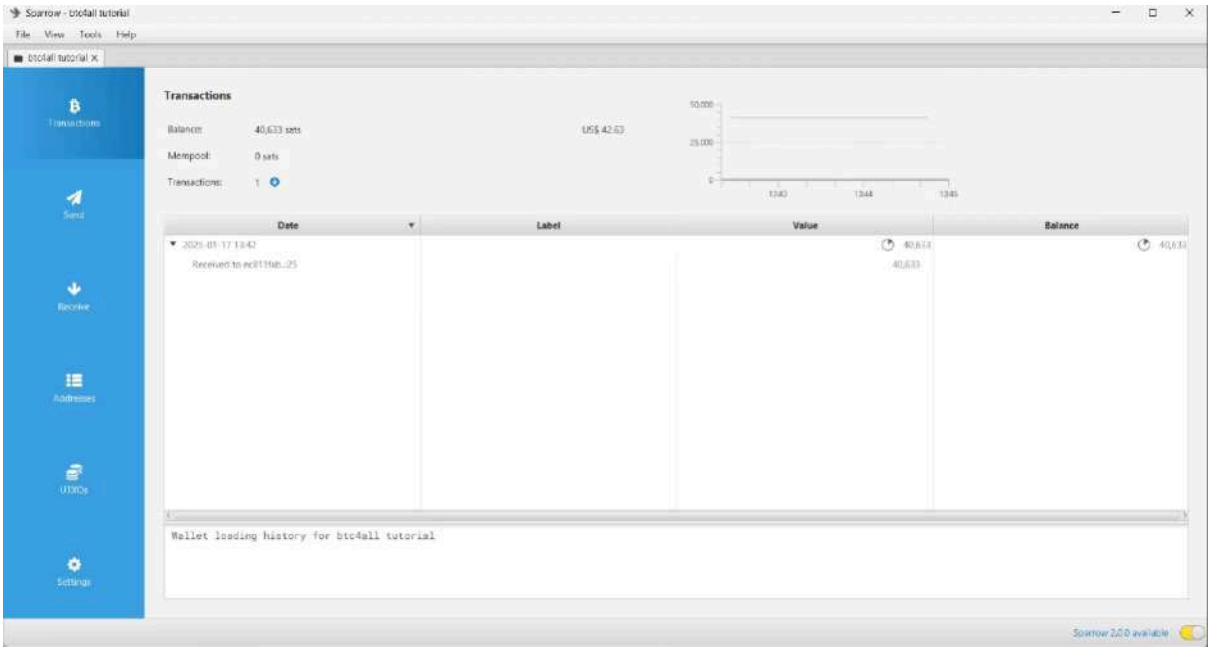
Tudo certo aqui.

Vou clicar em “Send now”, enviar agora.



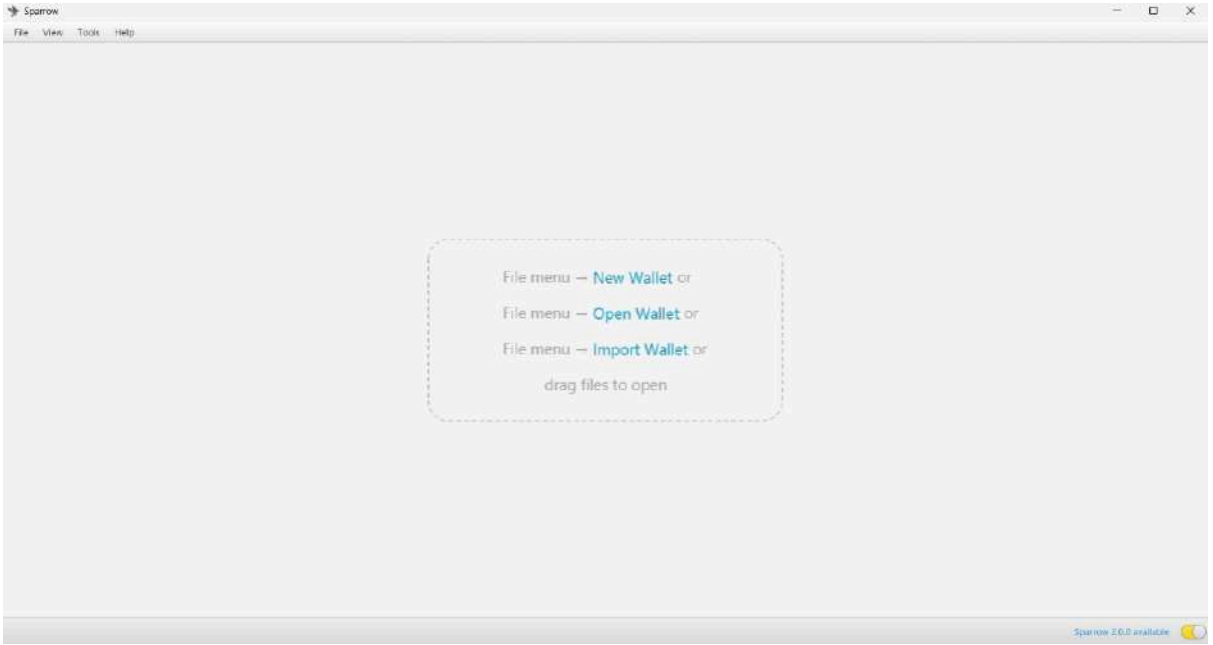
Feito. Saque confirmado.

Agora é só acompanhar na Sparrow quando o valor chegar. Deve levar alguns minutos pra rede processar essa transação.

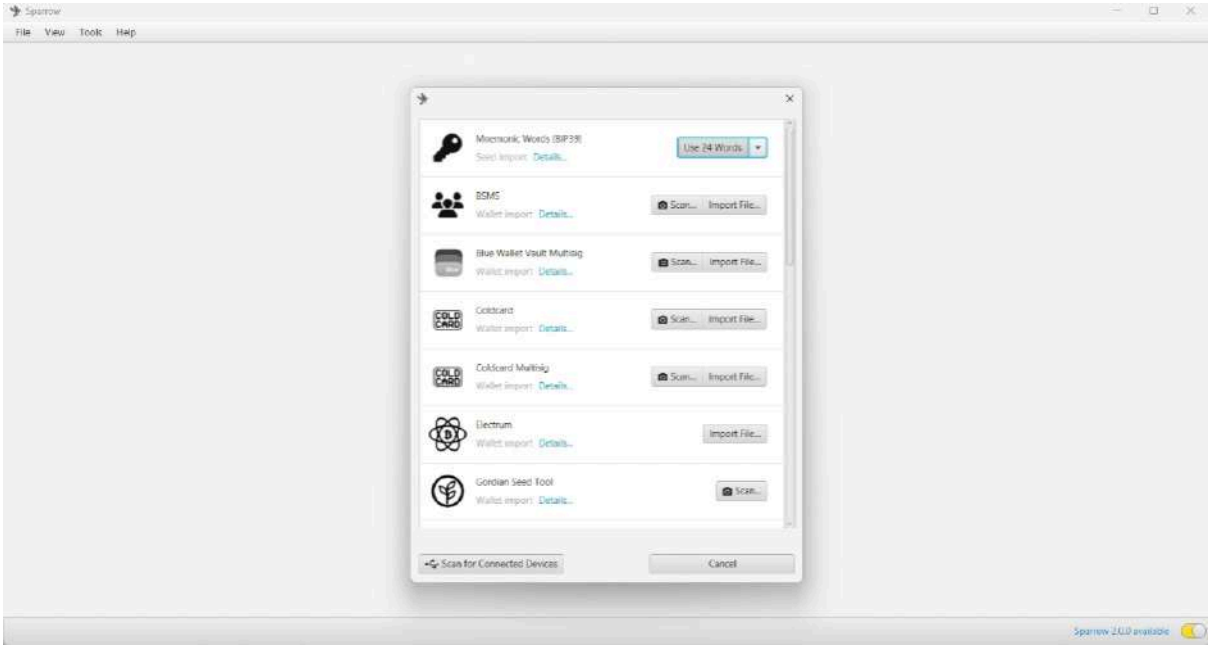


Feito, a transação chegou aqui na Sparrow: 40.633 satoshis agora estão sob a minha custódia.

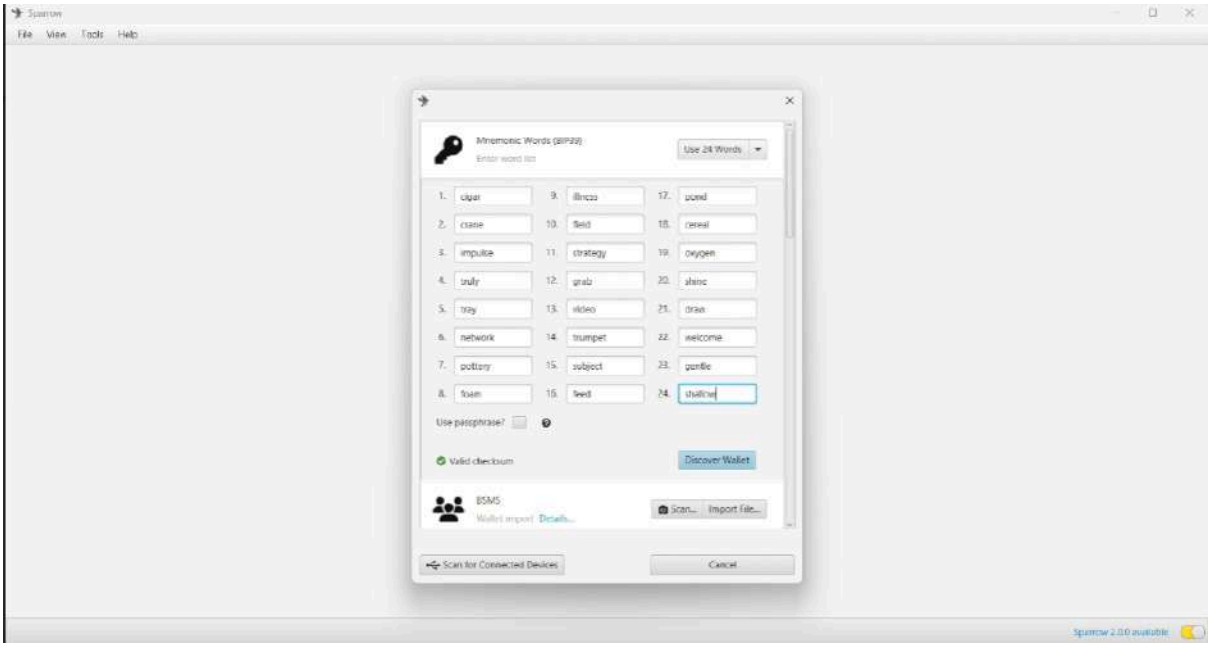
Agora nós vamos imaginar que eu perdi o acesso a esse saldo na carteira e vou recuperar ela do zero. E aí vamos ver se o saldo vai reaparecer.



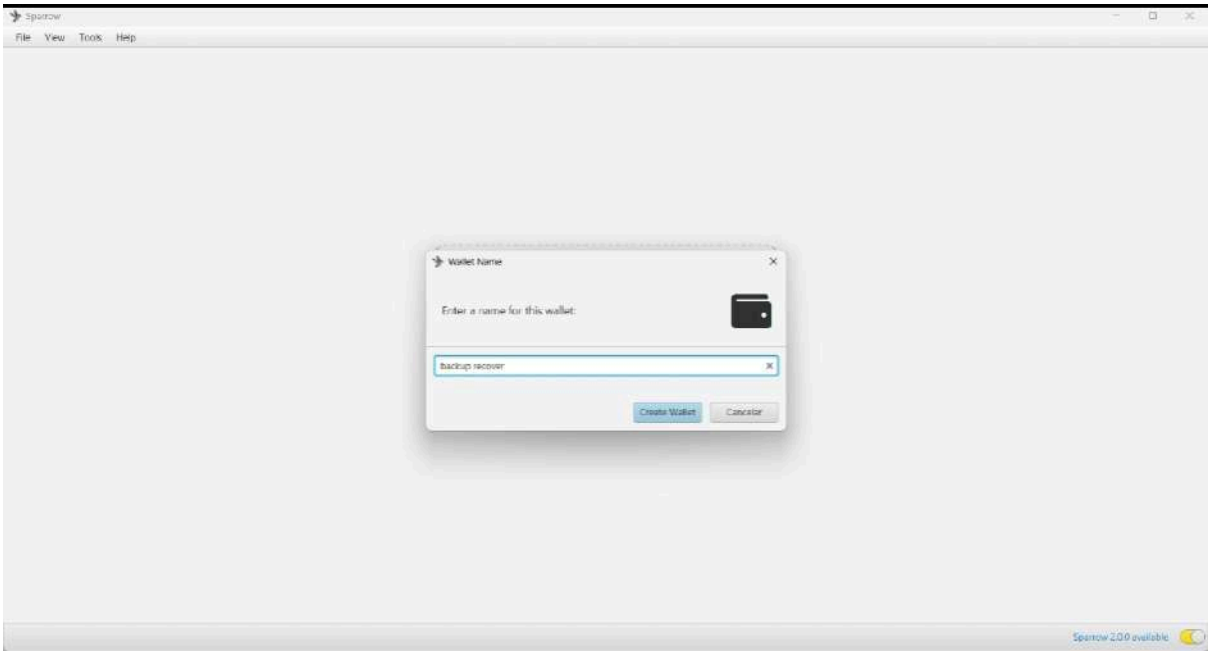
Fechei a carteira que eu criei antes e vou clicar na terceira opção “import wallet”, importar wallet.



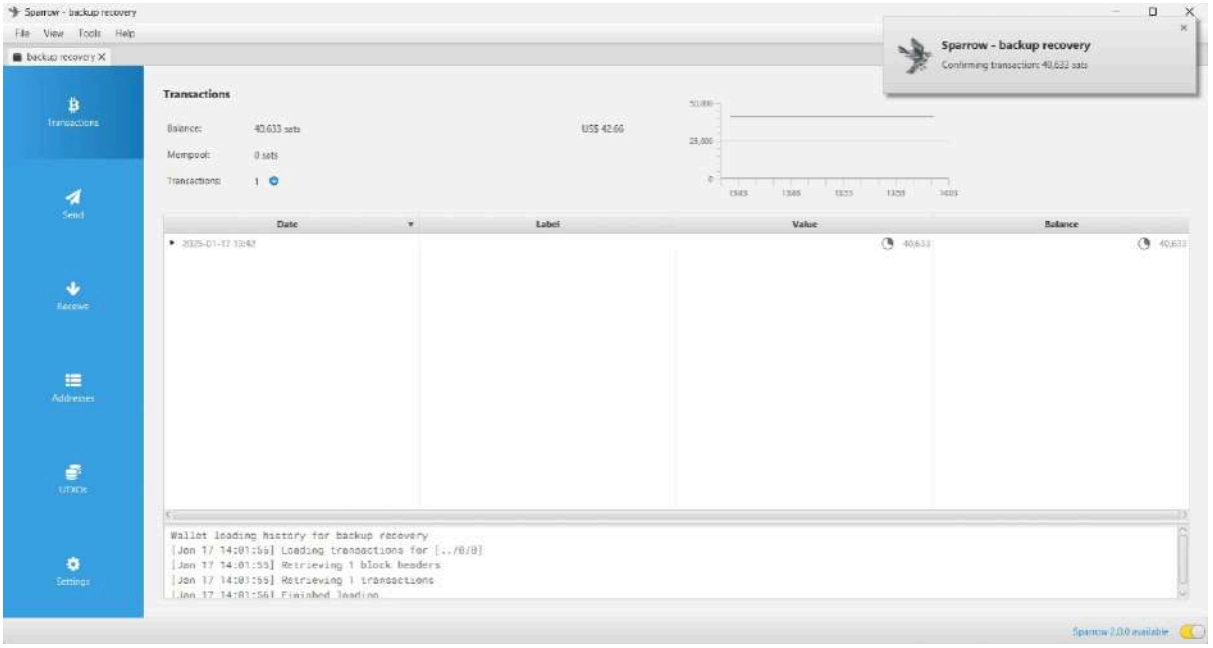
Vai aparecer várias formas de recuperação. Vou na primeira, que é a forma como eu gerei antes com 24 palavras.



Agora é só inserir as mesmas palavras que eu anotei quando criei a carteira anterior e clicar em “Discover wallet”, encontrar carteira.

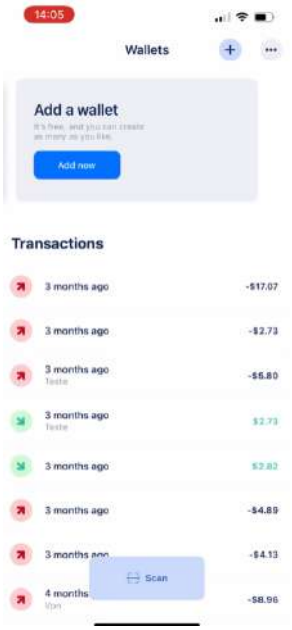


Vai pedir para eu criar um nome pra essa carteira que eu quero importar. Vou digitar “backup recovery”, carteira recuperada, e clicar em “Create wallet”.

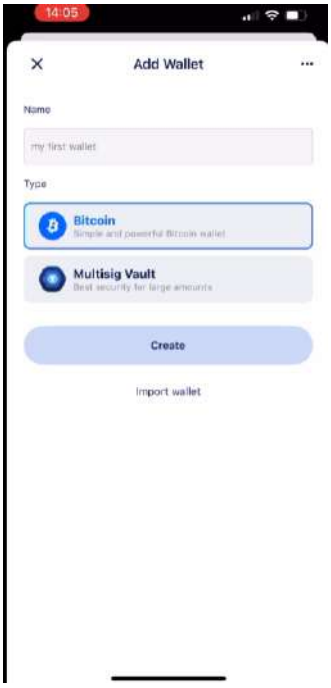


Feito. A Sparrow puxou todos os dados, as chaves e o meu saldo em bitcoin.

Agora eu vou fazer o mesmo processo de recuperação em uma carteira diferente da Sparrow para você ver como independente do aplicativo ou software que você use, é possível recuperar o seu saldo em Bitcoin se você tiver a sua lista de palavras de backup. Então eu vou recuperar essa mesma carteira na Blue wallet, uma carteira de celular bem conhecida e muito fácil de usar.



Vou abrir a minha Blue Wallet no celular e clicar em “Add Now”, para criar uma nova carteira.



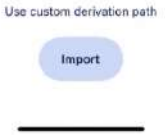
Vou selecionar a última opção “import wallet”, importar carteira.

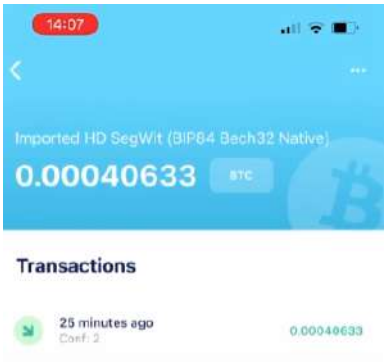
Caso você queira criar uma carteira do zero, é só selecionar Bitcoin e depois em “Create”. Mas agora eu quero recuperar a carteira que eu criei na Sparrow, por isso vou direto lá na opção de importar.

Vou digitar aqui as 24 palavras que eu gerei na Sparrow na ordem e cuidando para digitar certinho, e clicar em “import” quando terminar.

Olha aí, a Blue Wallet encontrou a carteira.

Vou clicar em “import”.





Clicando nela aparece o saldo que eu transferi da Coinbase.

Essa é a maravilha do Bitcoin, como é open source você pode recuperar o seu saldo em qualquer dispositivo que siga as mesmas regras iniciais que você usou na hora de gerar as suas chaves.

Agora que você já passou por todas as aulas do Bitcoin4All, você está pronto para colocar a mão na massa, começar a acumular e a desbravar o mundo do Bitcoin.

Espero que você tenha gostado do Bitcoin4All e que este tenha sido apenas o começo da sua jornada de aprendizado, afinal, Bitcoin não é apenas uma tecnologia, é um universo de conceitos que une economia, criptografia, redes descentralizadas e inovação contínua. A cada dia, novos desenvolvimentos e ideias surgem, desafiando nossas noções tradicionais de dinheiro e soberania.

Compartilhe esse curso com amigos, parentes e outras pessoas que também tem curiosidade e querem aprender sobre Bitcoin.

Até uma próxima e Opt Out!