



Como criar uma carteira multisig com Krux, Jade, Seedsigner e Sparrow



A segurança da autocustódia em Bitcoin melhora drasticamente quando usamos uma carteira multisig. Mas confiar toda a segurança em um único fabricante de hardware wallet ainda deixa espaço para falhas. A solução? Multisig com dispositivos de diferentes fornecedores — especialmente quando esses dispositivos são DIY, de código aberto e auditáveis.

Este tutorial mostra como criar uma configuração multisig multivendor usando apenas dispositivos DIY: Krux, SeedSigner, e Jade. Combinando diferentes projetos e abordagens, reduzimos a superfície de ataque e evitamos depender de qualquer software, firmware ou empresa específica.

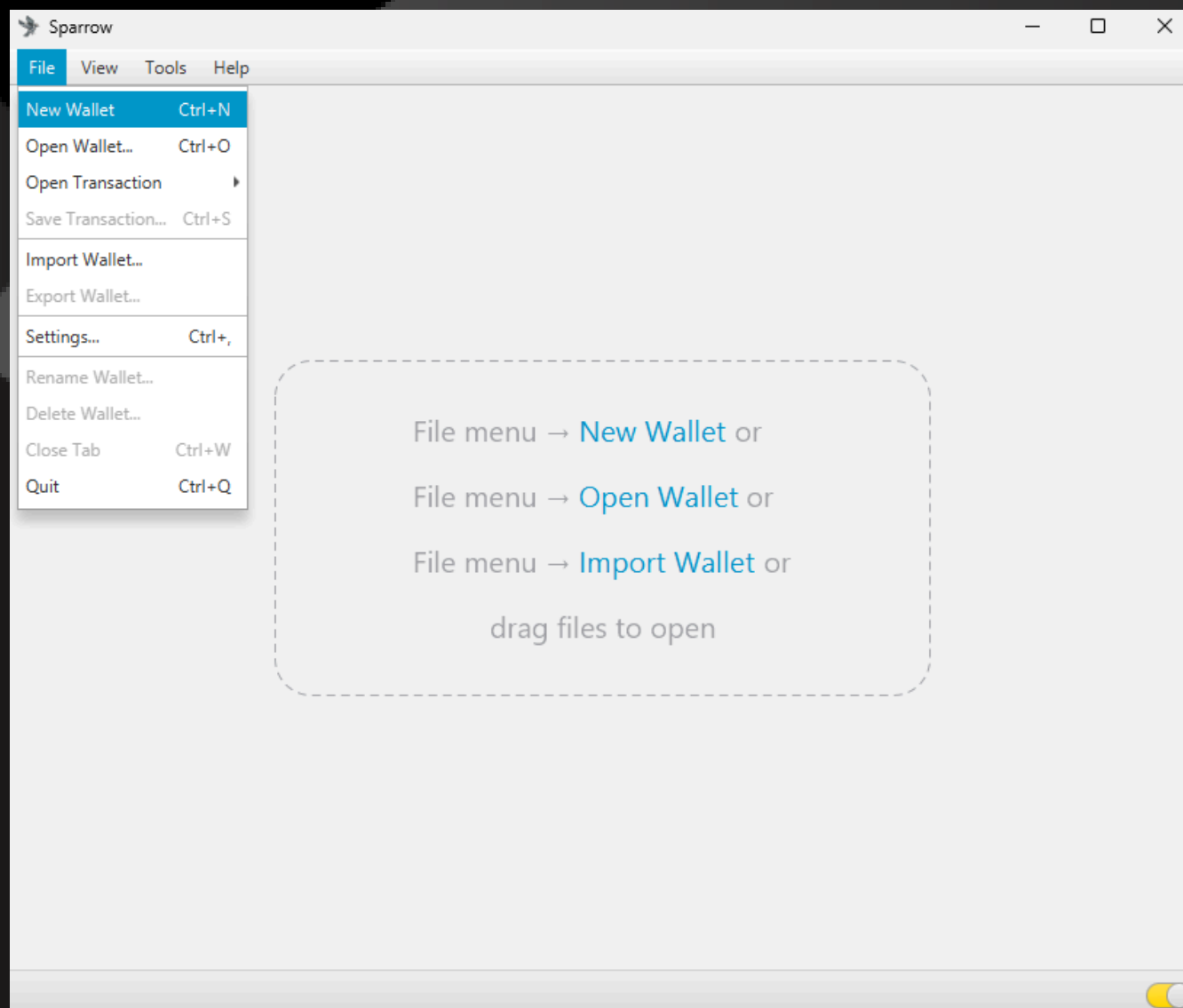
Você aprenderá a gerar suas seeds offline, montar uma multisig multivendor (diferentes fabricantes), exportar os dados entre os dispositivos e assinar transações de forma segura e independente. Tudo isso com ferramentas acessíveis, reutilizáveis e totalmente sob seu controle.

Se seu objetivo é ter uma custódia verdadeiramente soberana, resistente a falhas e livre de intermediários, essa abordagem é um dos caminhos mais sólidos.

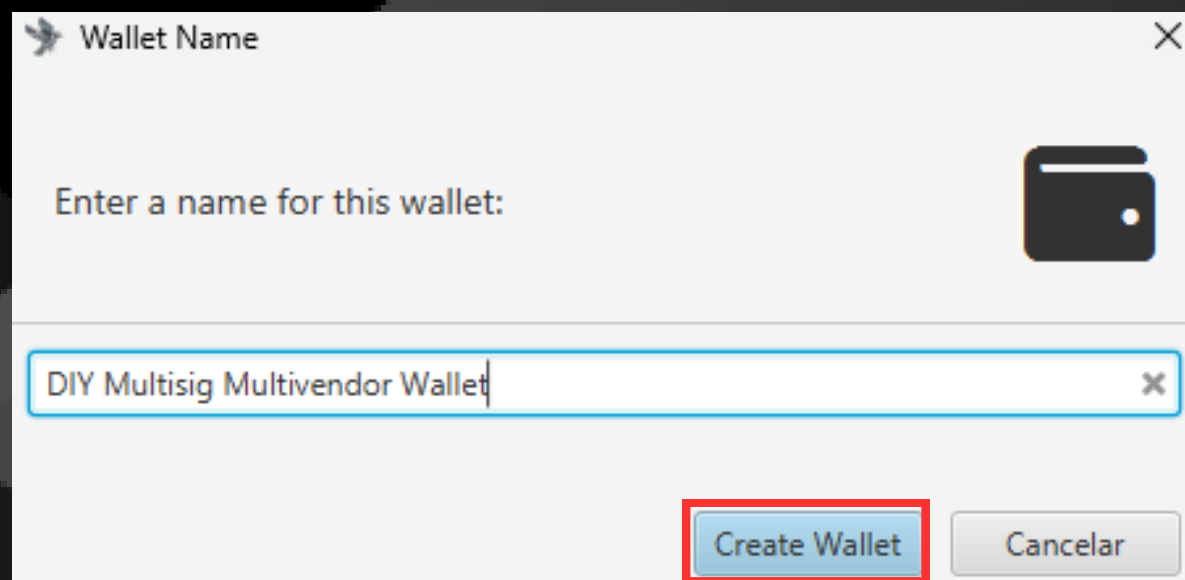
OBS: Para este tutorial será necessário ter a Sparrow instalada em um computador com câmera, caso ainda não tenha instalado, consegue através do tutorial #1

Com a Sparrow já instalada em seu computador, vamos agora realizar a criação de uma carteira multisig

Clique em “File” e depois em “New Wallet”



Dê um nome a esta carteira e clique em
“Create Wallet”



The image shows a 'Wallet Name' dialog box with a title bar containing a small icon and the text 'Wallet Name' and a close button. The main area contains the text 'Enter a name for this wallet:' and a wallet icon. Below this is a text input field containing 'DIY Multisig Multivendor Wallet'. At the bottom, there are two buttons: 'Create Wallet' (highlighted with a red rectangle) and 'Cancelar'.

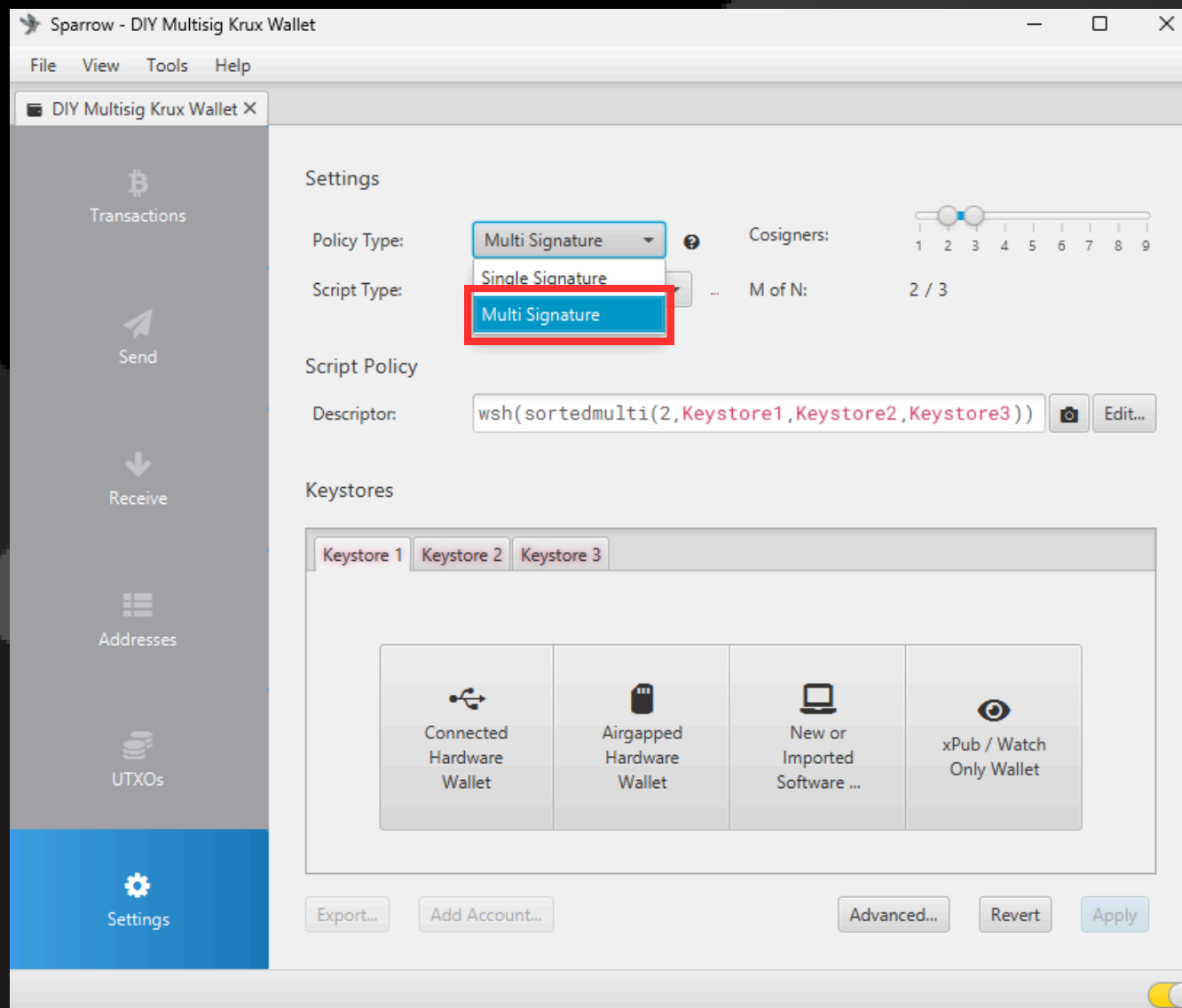
Wallet Name

Enter a name for this wallet:

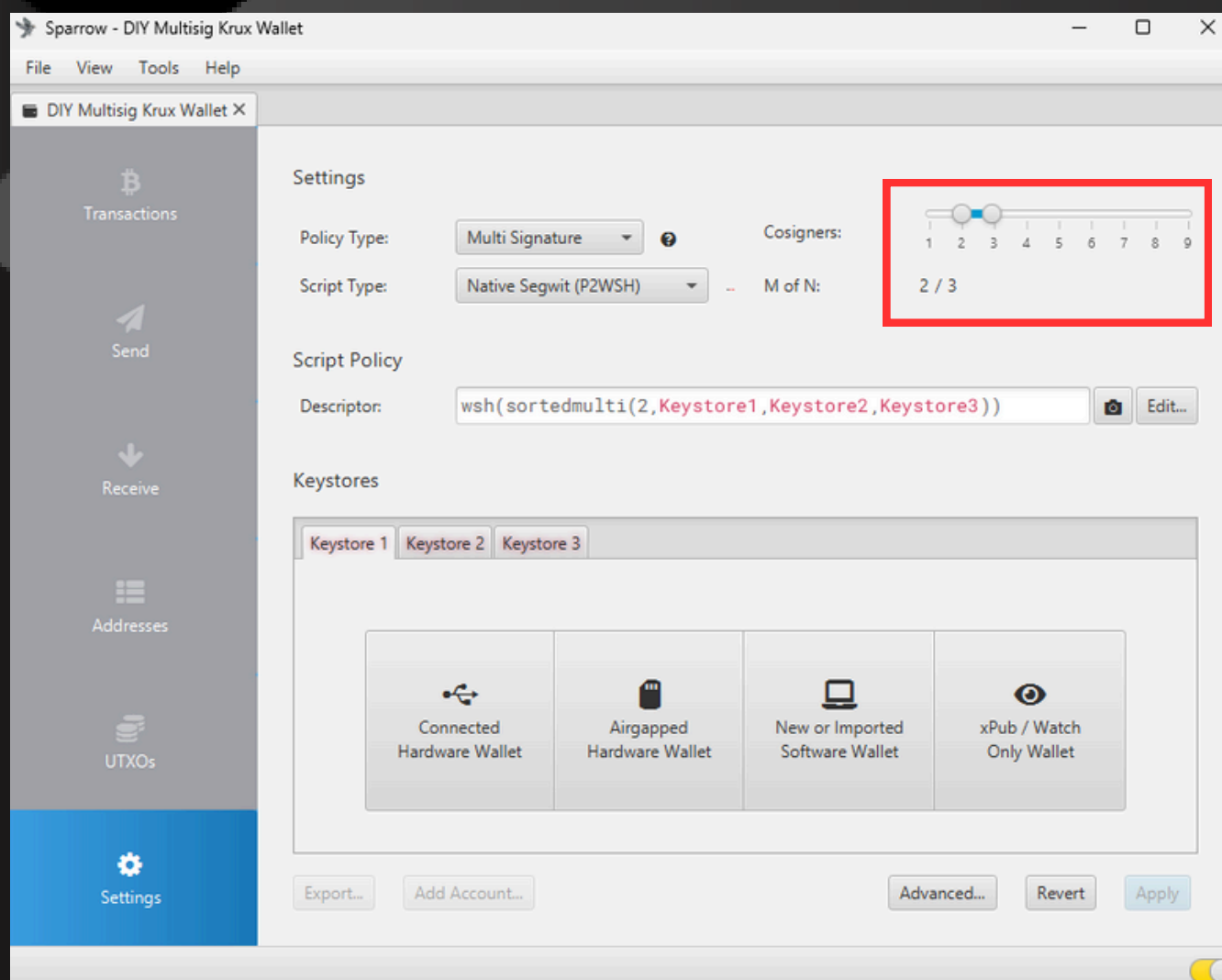
DIY Multisig Multivendor Wallet

Create Wallet Cancelar

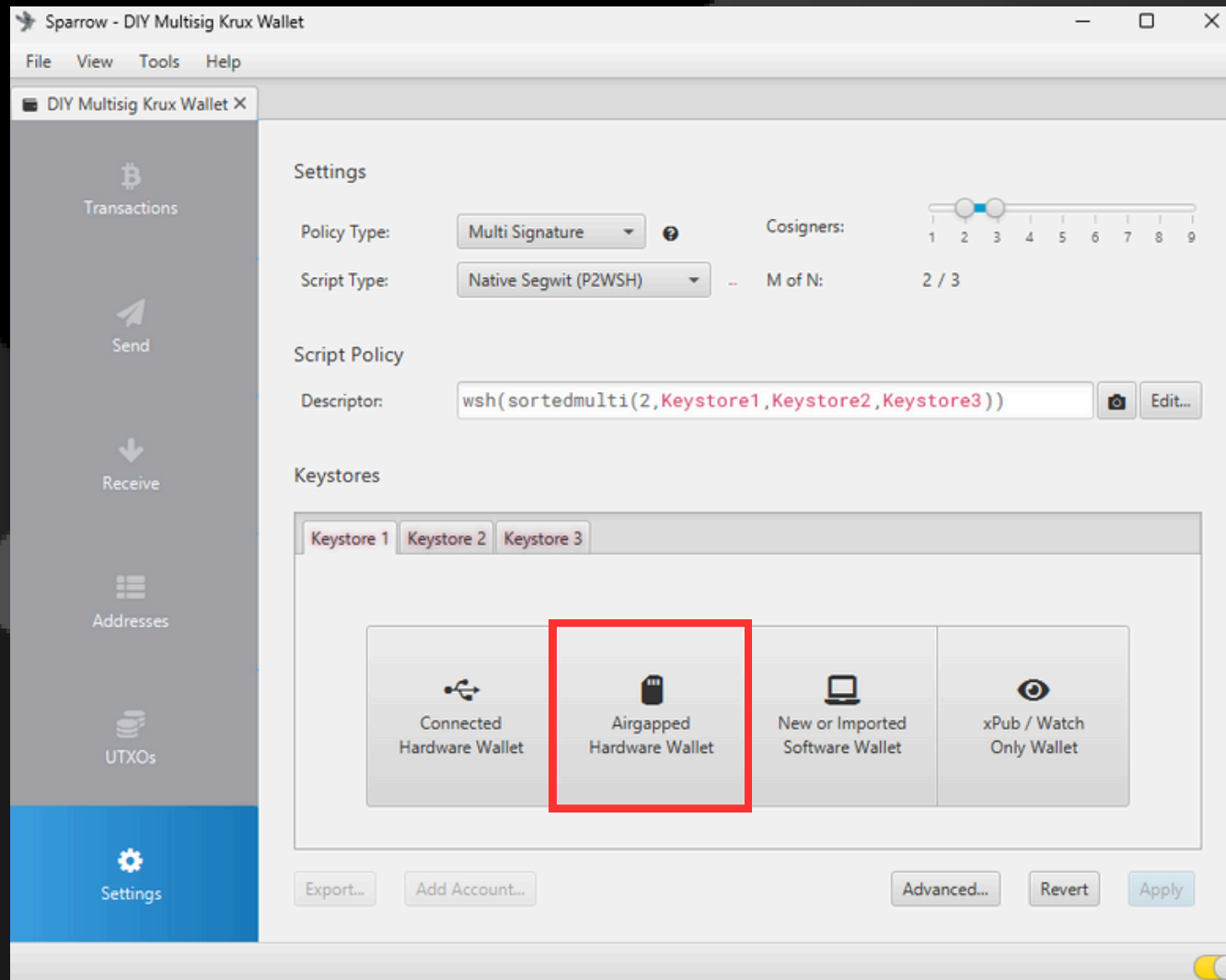
Aqui vamos seleccionar “Multi Signature”



Em uma carteira multisig 2 de 3, existem três co-signers, que podem ser pessoas diferentes ou dispositivos distintos. Para movimentar os fundos, é necessário que pelo menos dois desses três co-signers assinem a transação.



Agora vamos adicionar as chaves para assinatura, vamos começar com a Krux



Após entrar em sua carteira krux

@ cBBa4cal
Mainnet
Single-sig
m/84'/0' /0'
Sem Senha

Carregar Carteira

Senha

Customizar

< Voltar

vamos clicar em
“Customizar”

m/84'/0'/0'

Rede

Single/Multisig

Tipo de Script

Conta

◀ Voltar

“Clique em
Single/Multisig”



Single-sig

Multisig

“Clique em **Multisig**”

m/48'/0'/0'/2'

Rede

Single/Multisig

Tipo de Script

Conta

◀ Voltar

Note agora que
agora o 'derivation
path' foi alterado
para m/48'/0'/0'/2'

m/48'/0'/0'/2'

Rede

Single/Multisig

Tipo de Script

Conta

< Voltar

Vamos agora pegar
a chave pública
estendida.

Vamos clicar em
“Voltar”

@ cBBa4cal
Mainnet
Single-sig
m/84'/0' /0'
Sem Senha

Carregar Carteira

Senha

Customizar

◀ Voltar

Agora vamos clicar
em “Carregar
Carteira”

@ cBBa4cal

Backup de Mnemônico

Chave Pública Estendida

Carteira

Endereço

Assinar

Desligar

Agora em “Chave
Pública Estendida”

Clique em “ZPUB - Código QR”



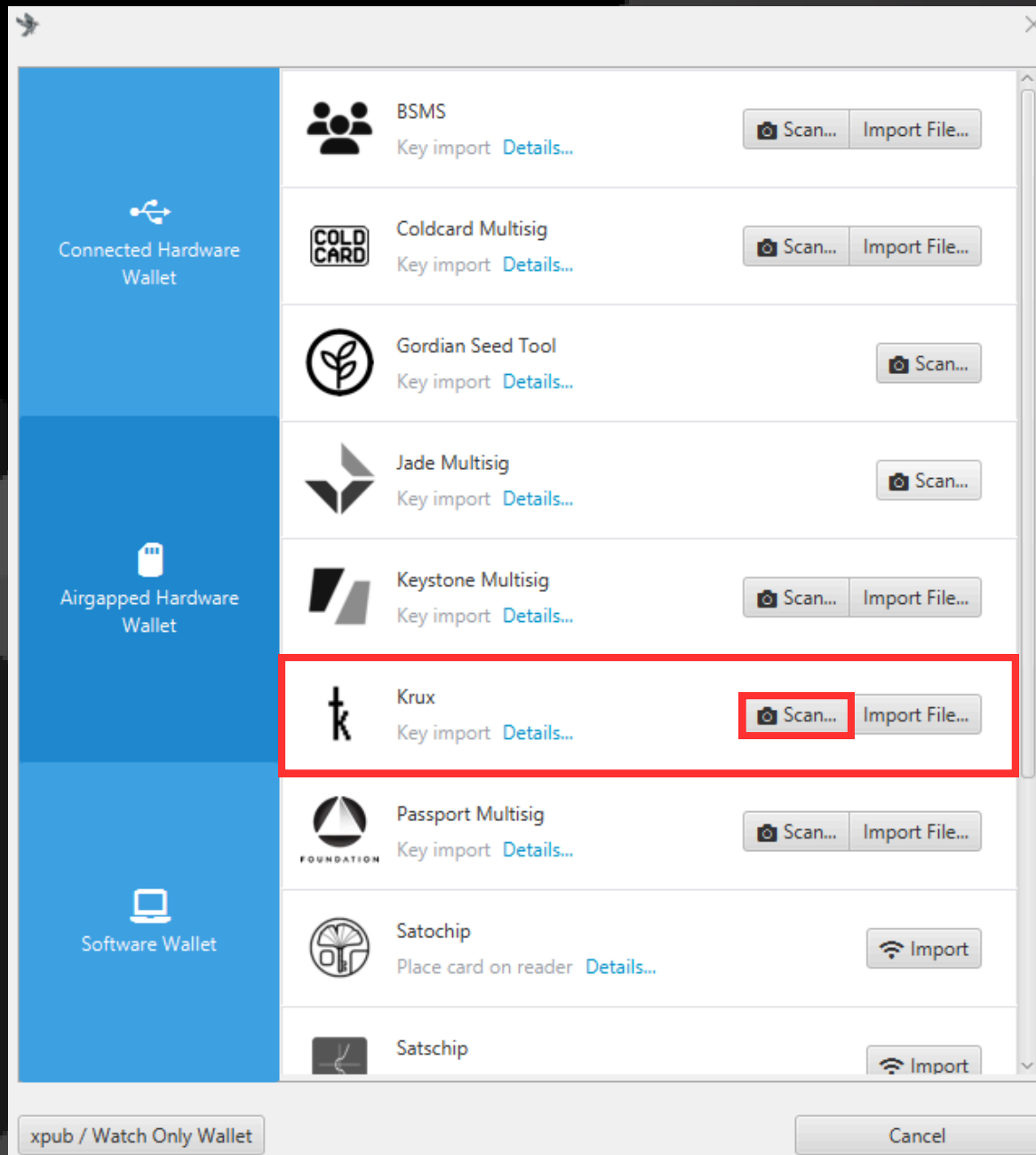
ZPUB permite que você compartilhe informações de sua carteira, como endereços de recebimento, sem expor suas chaves privadas, garantindo assim a segurança dos seus Bitcoins.



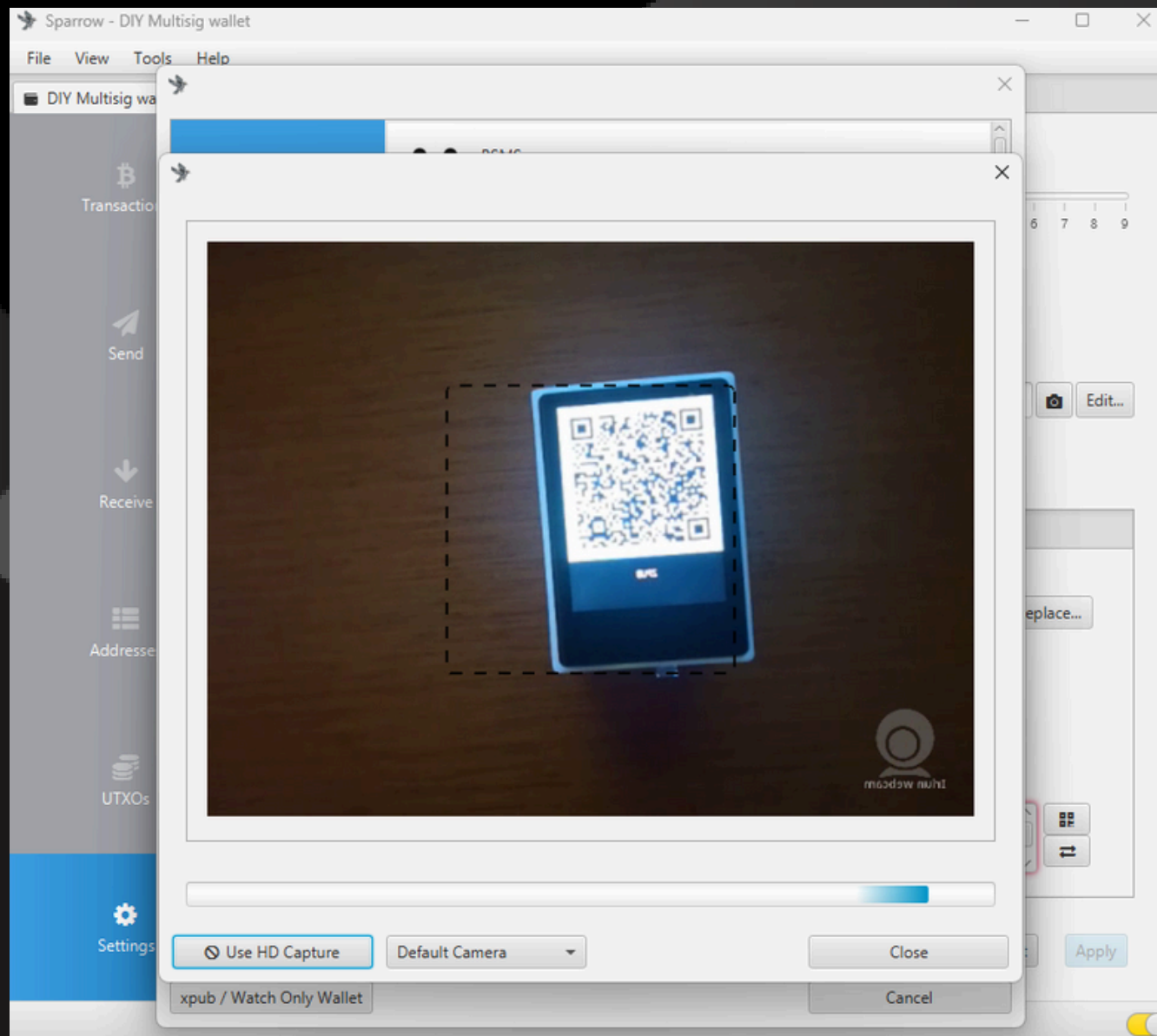
ZPUB

Agora vamos ler o
código QR com a
câmera do computador,
diretamente na Sparrow

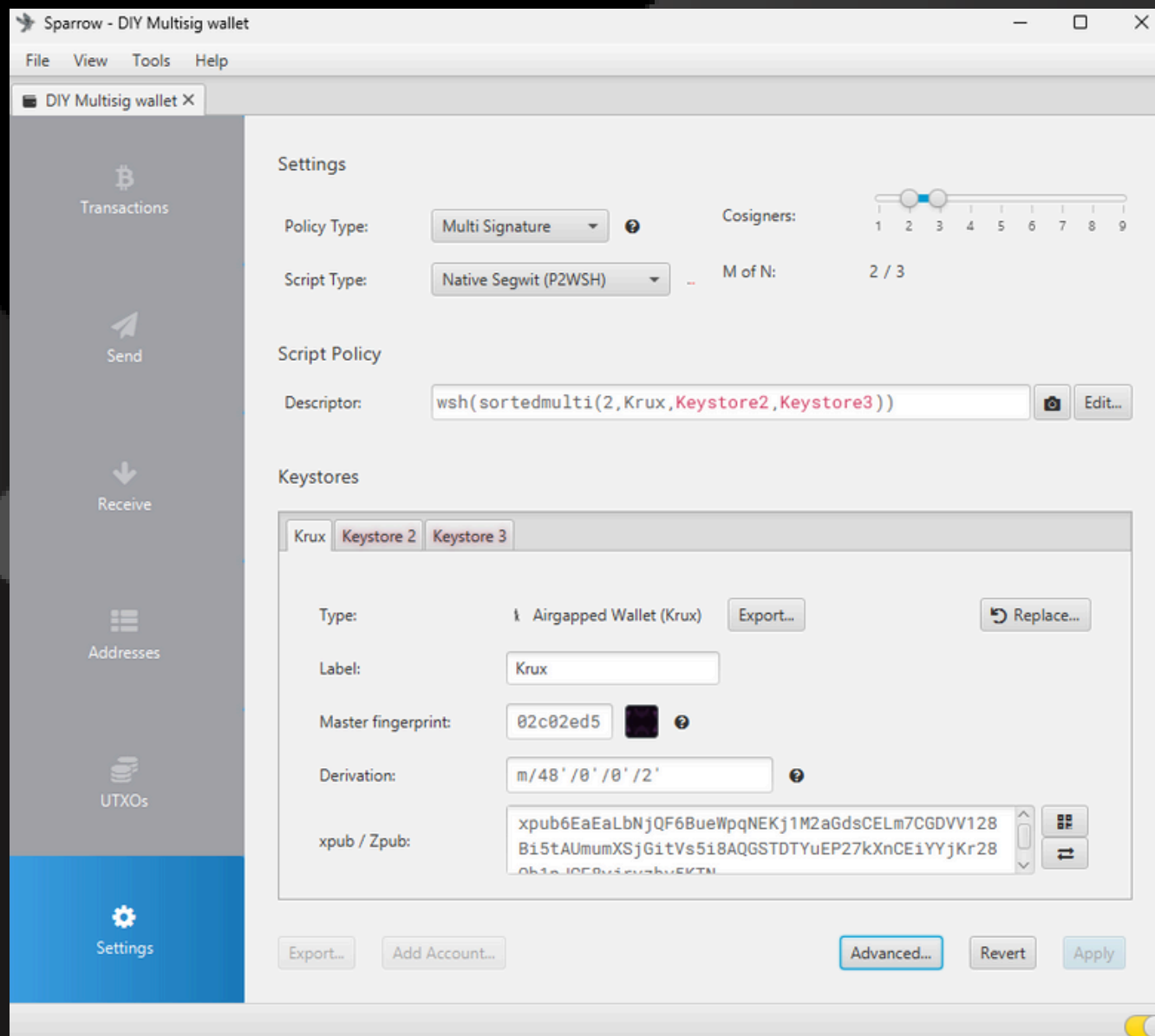
Na Sparrow, vamos clicar em Scan



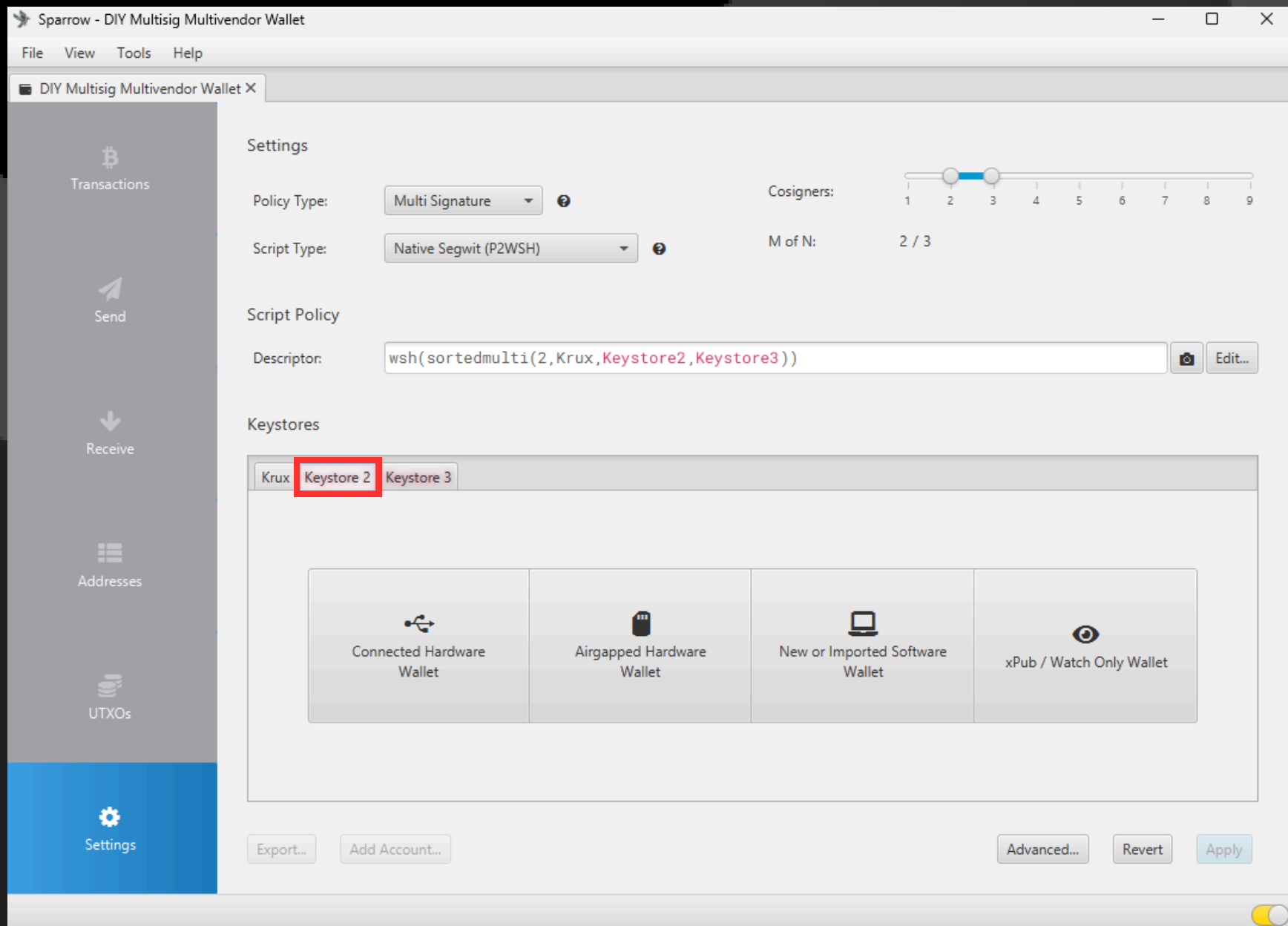
Realizar o Scan da Zpub



Após scanear a Zpub, a Sparrow irá aparecer assim:



Agora vamos adicionar a SeedSigner, clicando em “Keystore 2”



Acesse sua carteira e
clique em “Export Xpub”





Agora vamos clicar em Multisig

Agora em “Native Segwit”



Agora vamos selecionar “Sparrow”



Aqui aparecerá um aviso sobre a carteira de visualização, dizendo que poderá visualizar todas as transações futuras



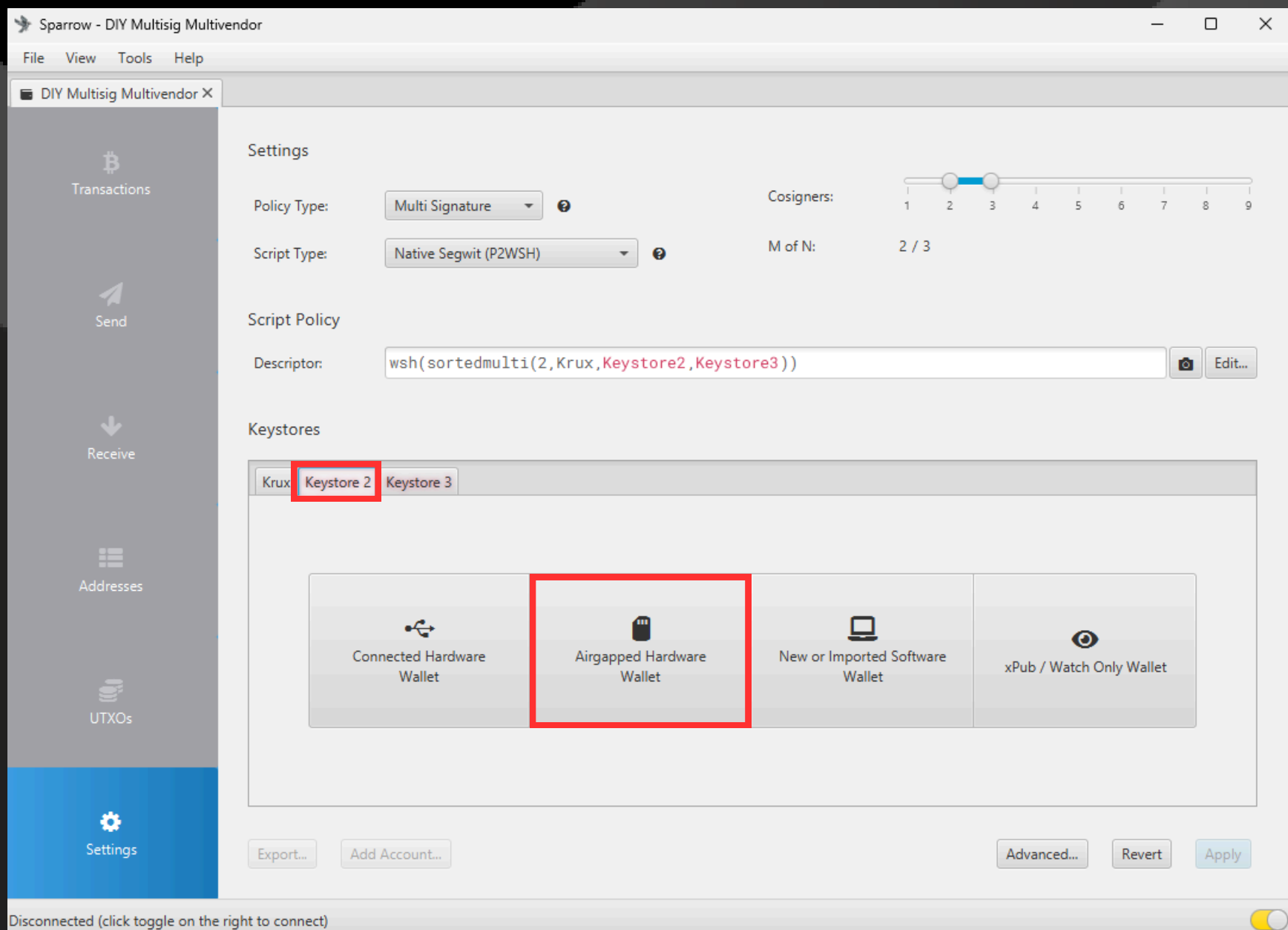
Confirme em “**I Understand**”

Clique em “Export Xpub”





Agora vamos voltar à Sparrow e ler o Qr Code gerado



Clique em “Scan”

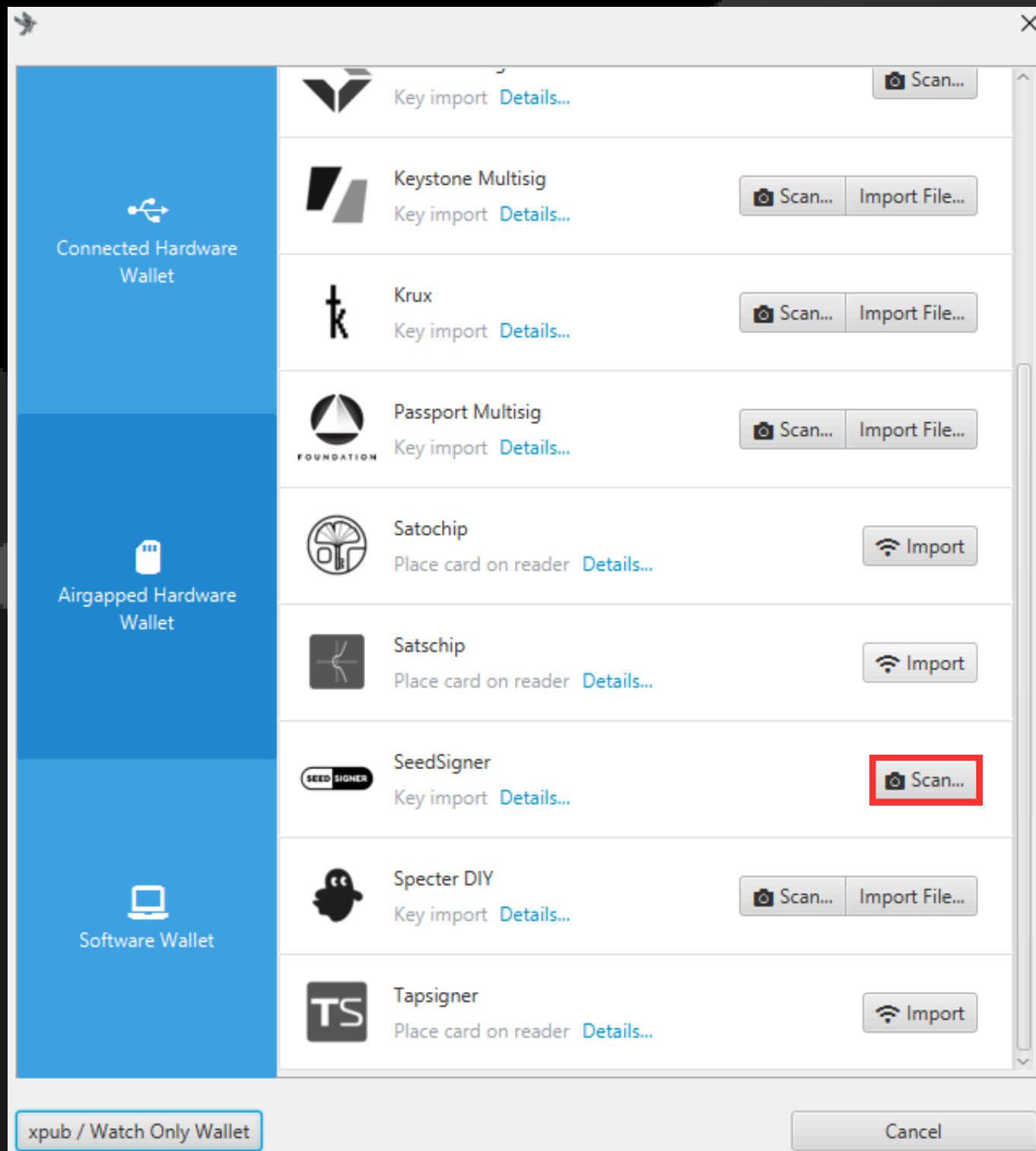
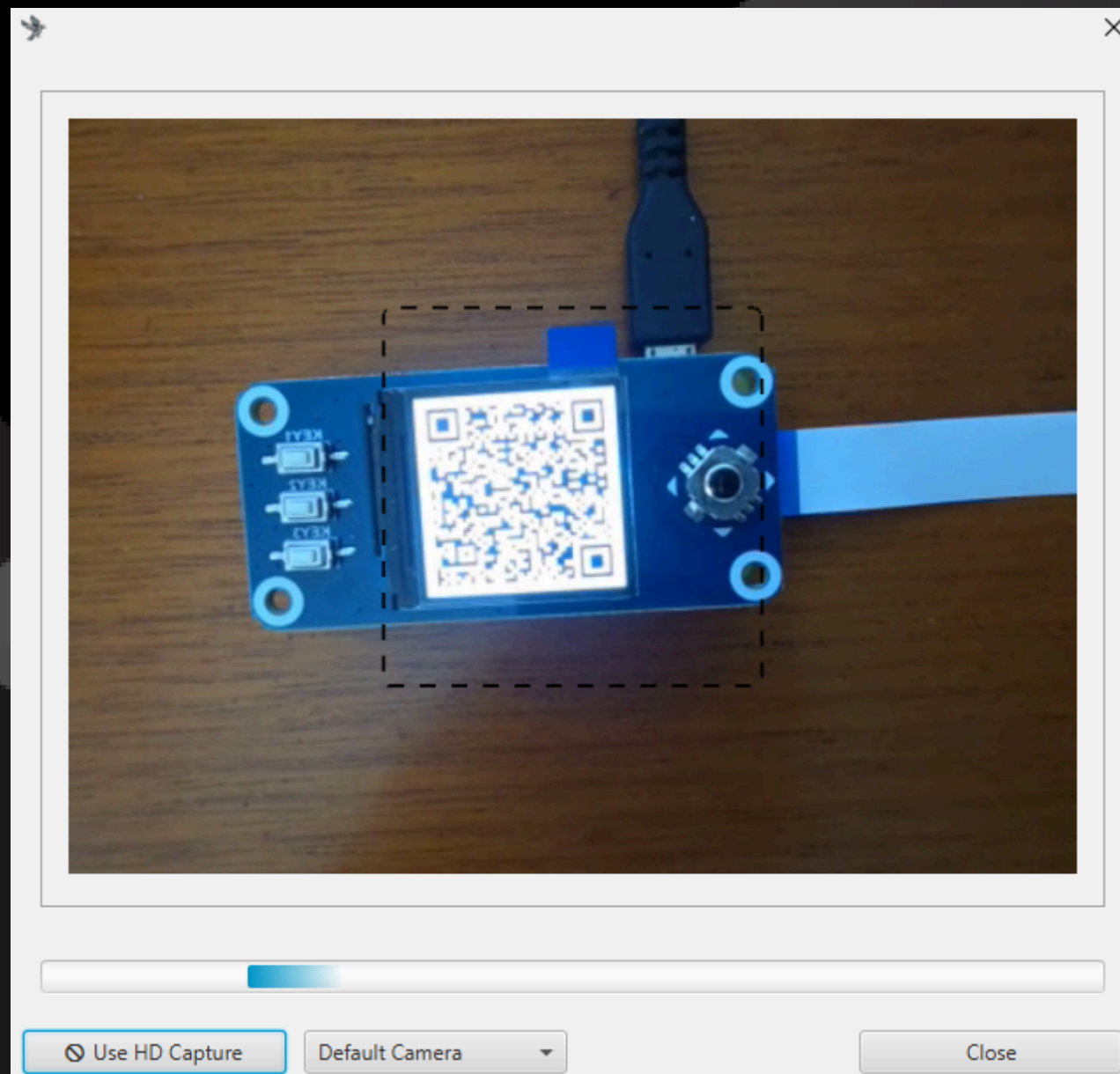
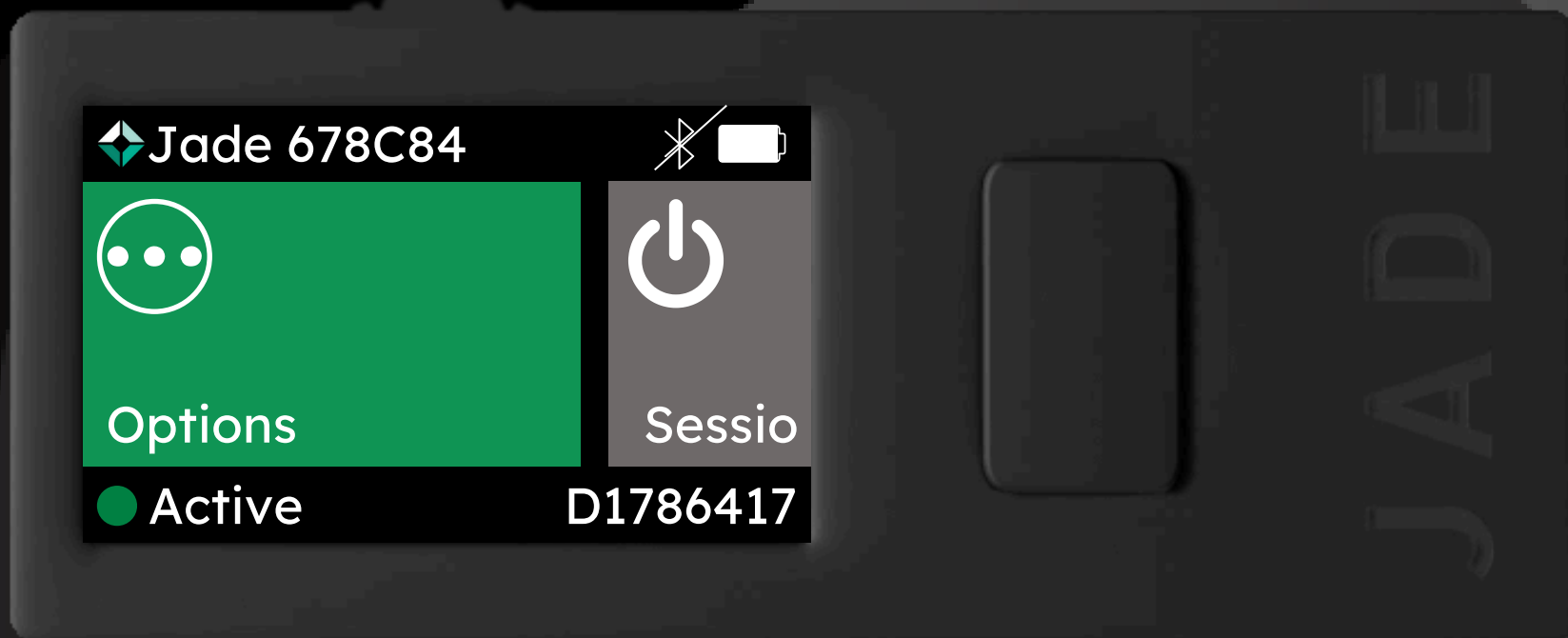


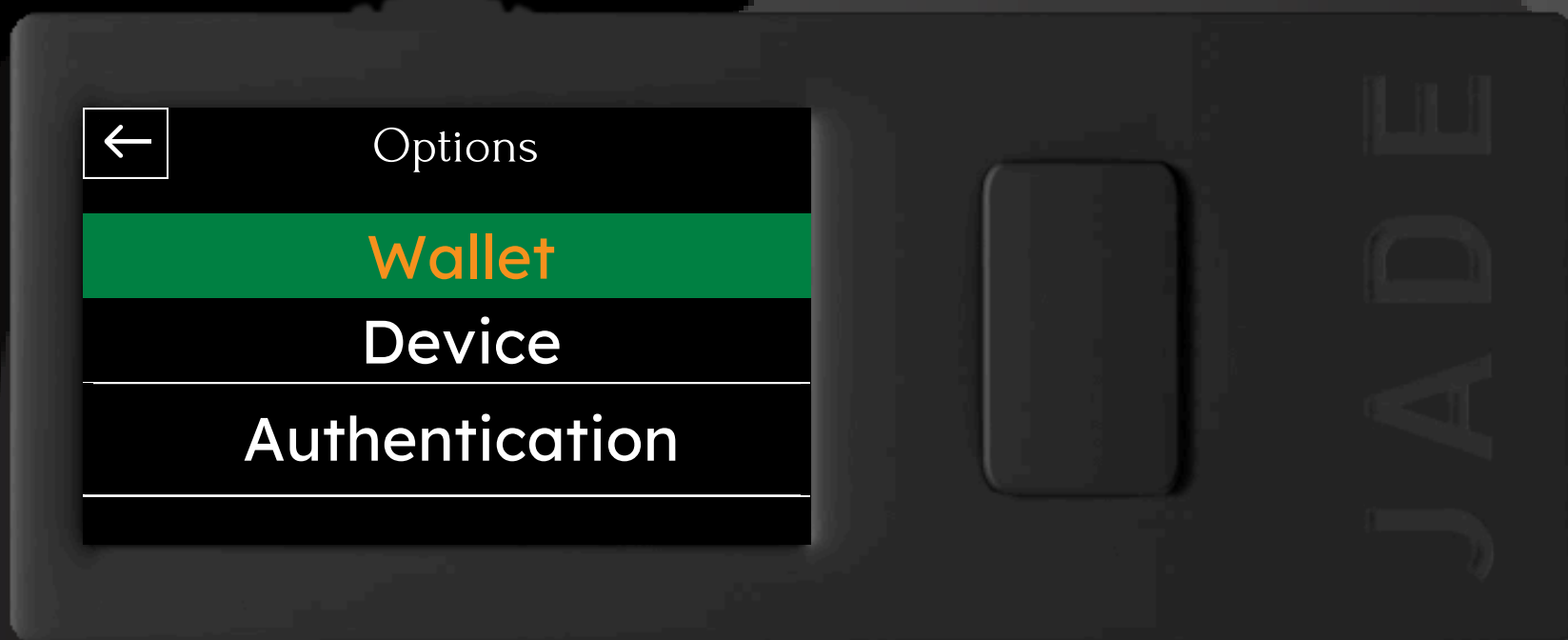
Imagem do processo



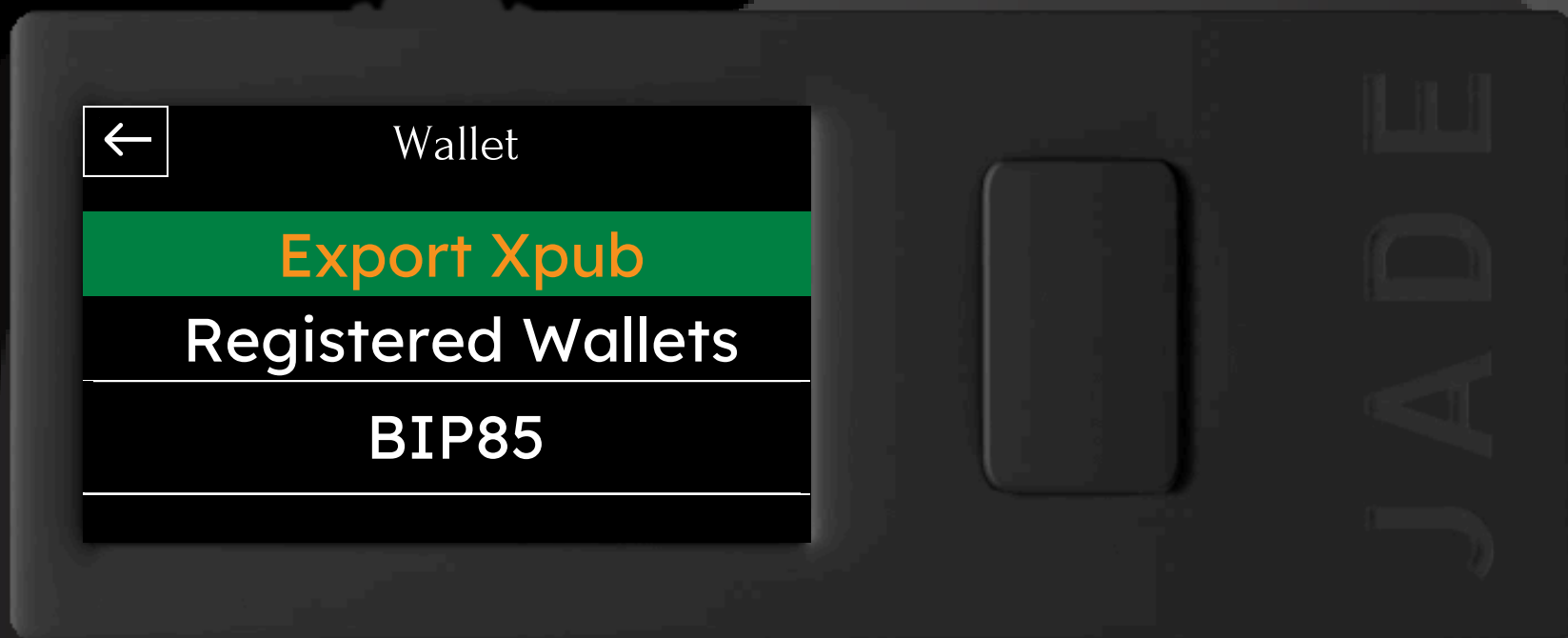
Agora para adicionar a Jade vamos
precisar acessar o dispositivo já
desbloqueado, entrar em “Options”



Agora em “Wallet”



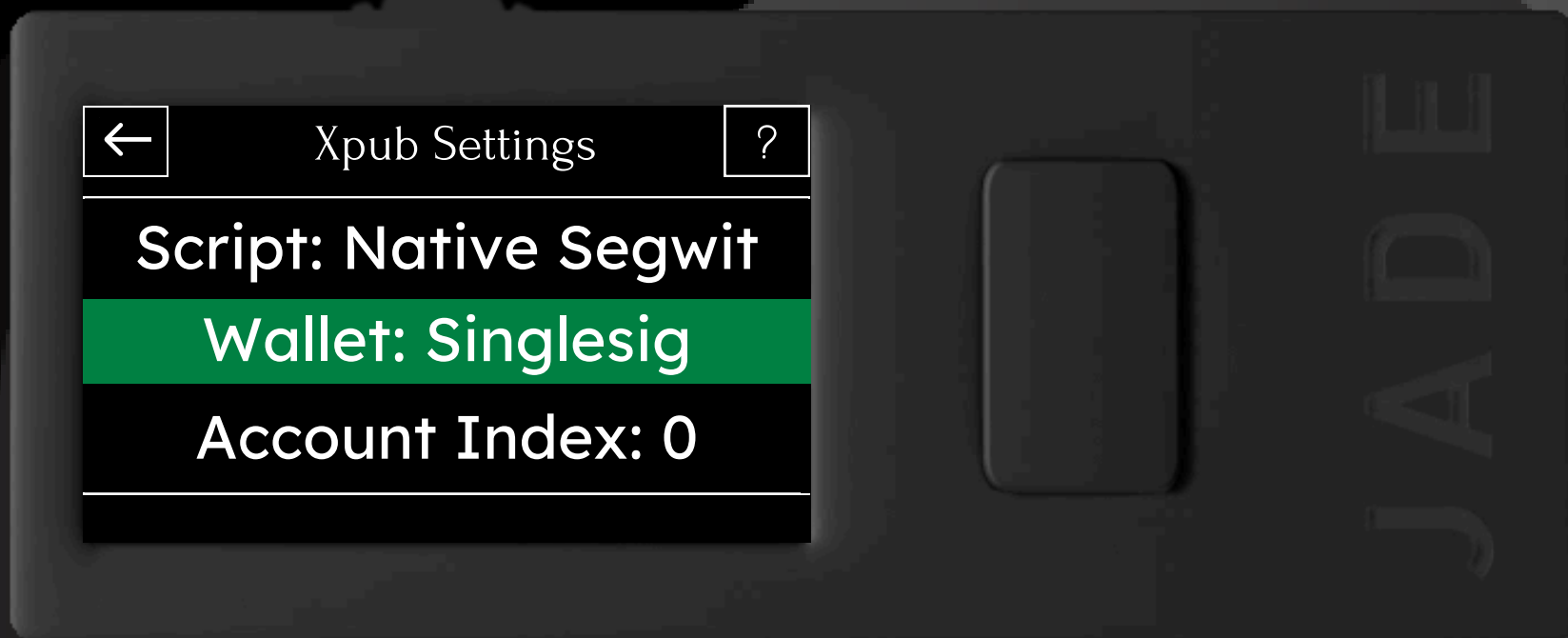
“Export Xpub”



Vamos clicar em “options”



Vamos clicar em “**Wallet: Singlesig**”



E vamos seleccionar “Multisig”



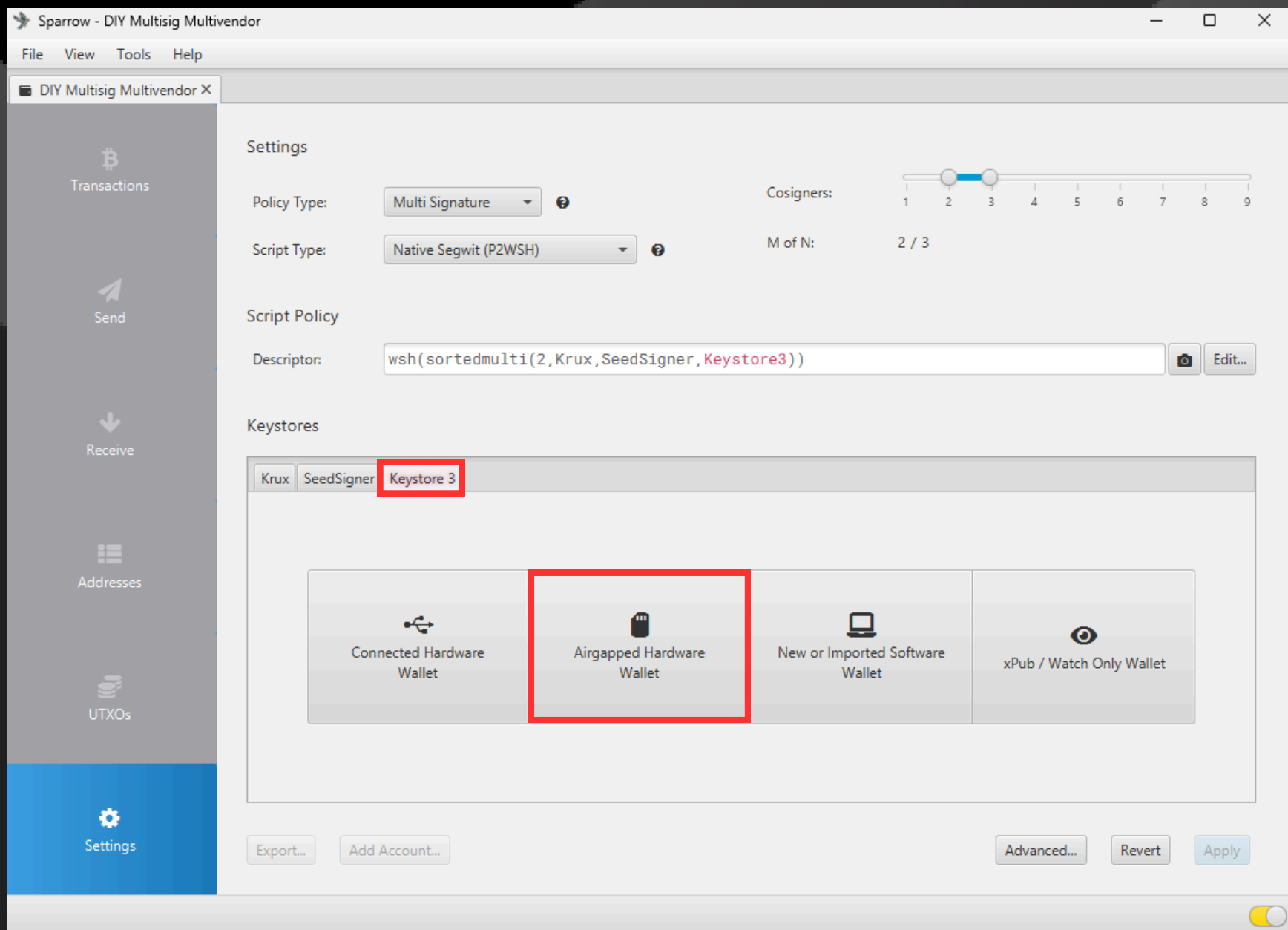
Agora vamos retornar ao QR code, vamos selecionar a seta no canto superior esquerdo, conforme a imagem:



Deixe neste tela enquanto retornamos à
Sparrow



Agora vamos adicionar a Jade



Vamos selecionar “Scan”, no campo da “Jade Multisig” e realizar a leitura do QR code do dispositivo

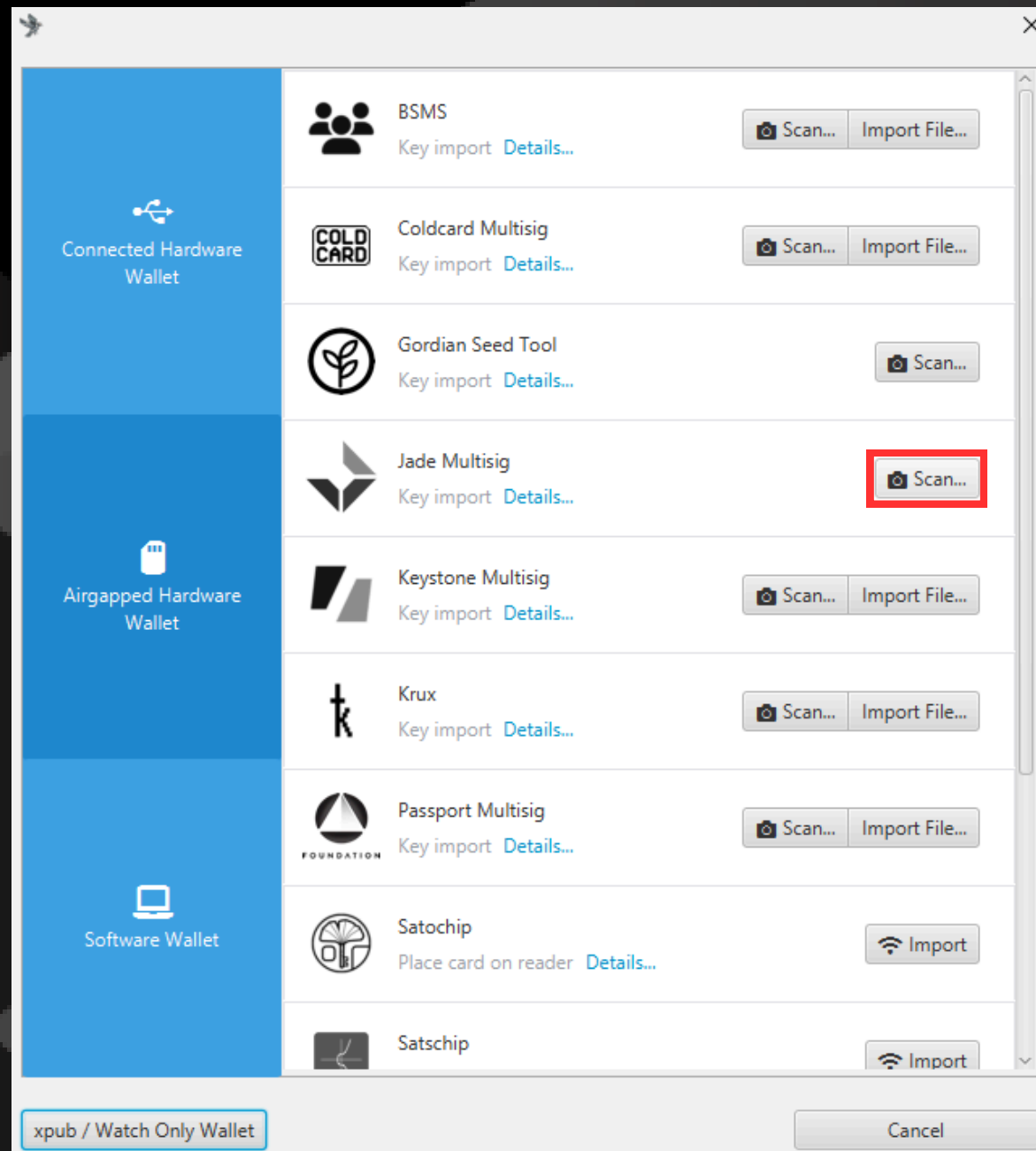
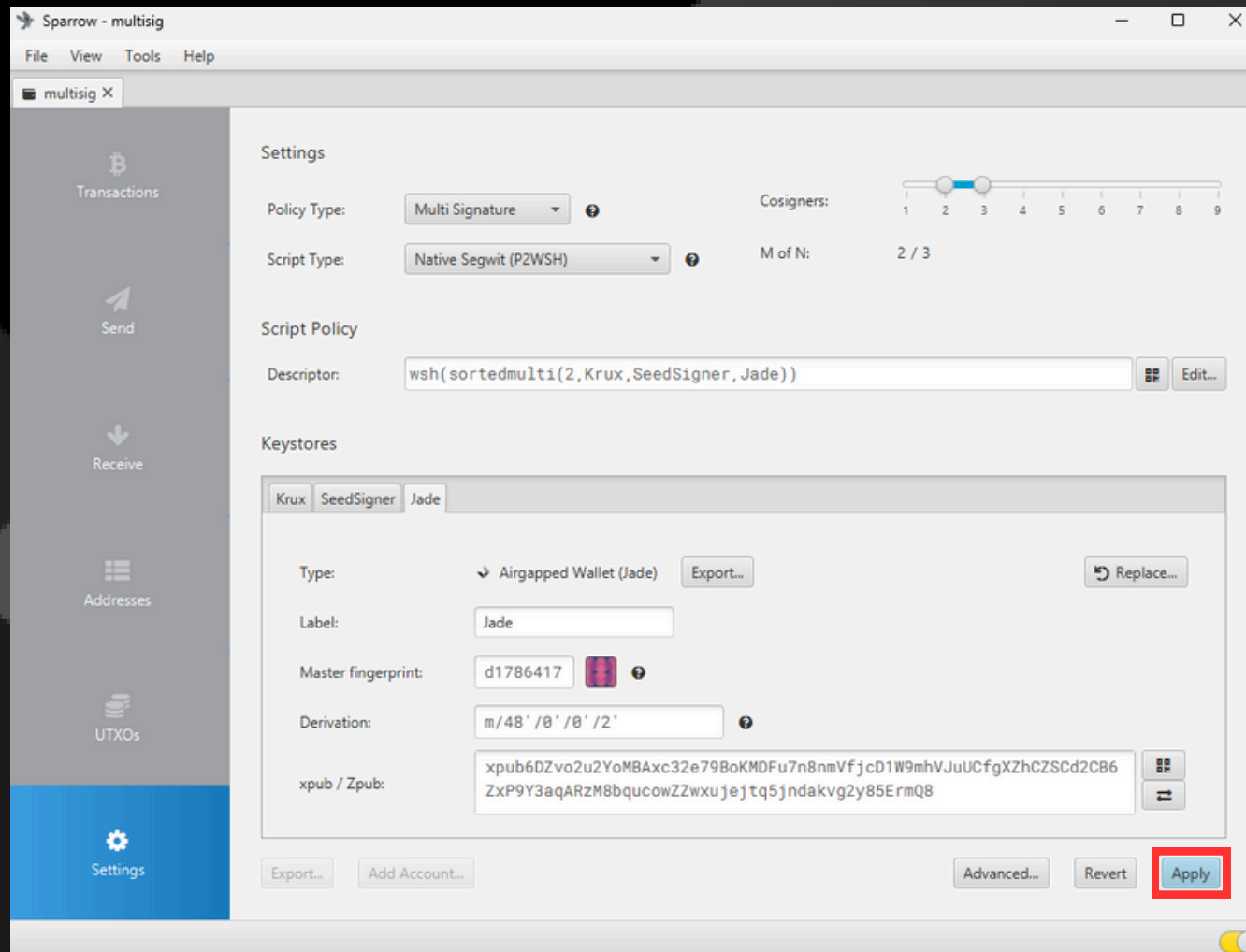


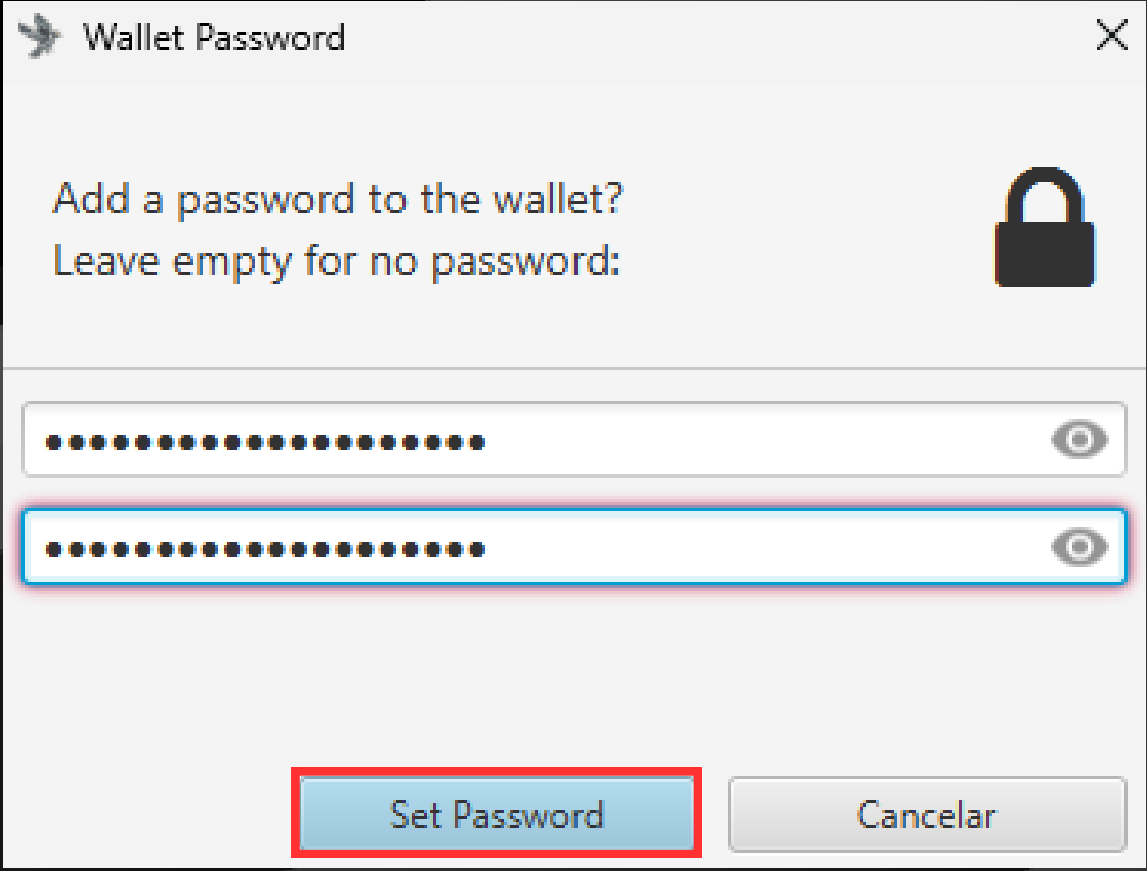
Imagem do processo



Configuradas as chaves, vamos agora clicar em “Apply”



Agora poderá escolher uma senha para adicionar a sua carteira da Sparrow, basta inserir uma senha robusta, e clicar em “Set Password”



The image shows a dialog box titled "Wallet Password" with a close button (X) in the top right corner. The main text asks "Add a password to the wallet?" and "Leave empty for no password:". To the right of the text is a padlock icon. Below the text are two password input fields, each with a series of dots and a toggle eye icon on the right. The second input field is highlighted with a red and blue border. At the bottom, there are two buttons: "Set Password" (highlighted with a red border) and "Cancelar".

Wallet Password

Add a password to the wallet?
Leave empty for no password:

.....

.....

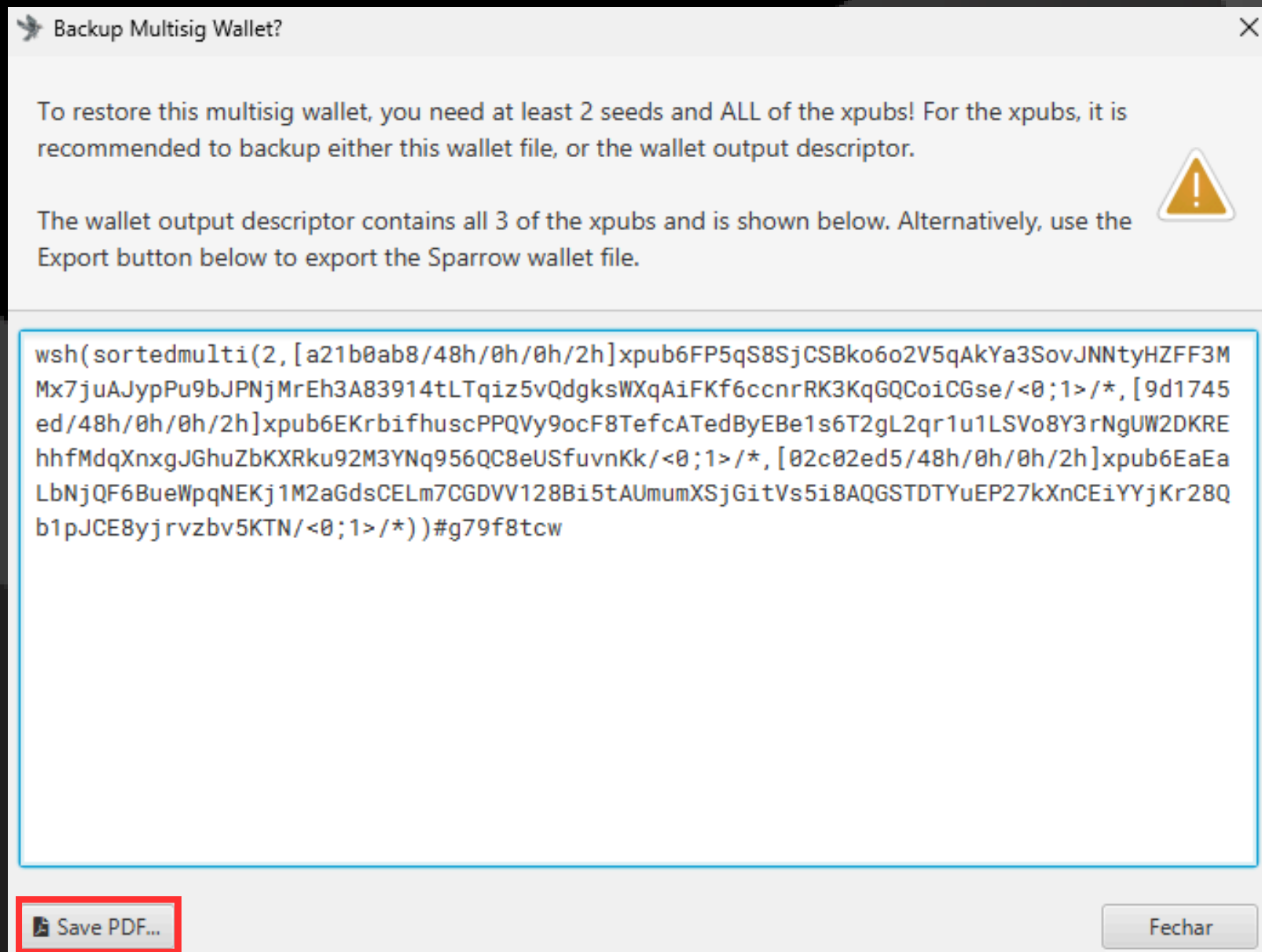
Set Password Cancelar

IMPORTANTE:

Após criar uma carteira multisig na Sparrow Wallet, você precisará fazer backup de pelo menos 2 seeds e de todos os xpubs para restaurá-la no futuro. Copie e guarde o descriptor mostrado na tela em um local seguro e offline ou clique em "Save PDF" para baixar o arquivo da carteira.

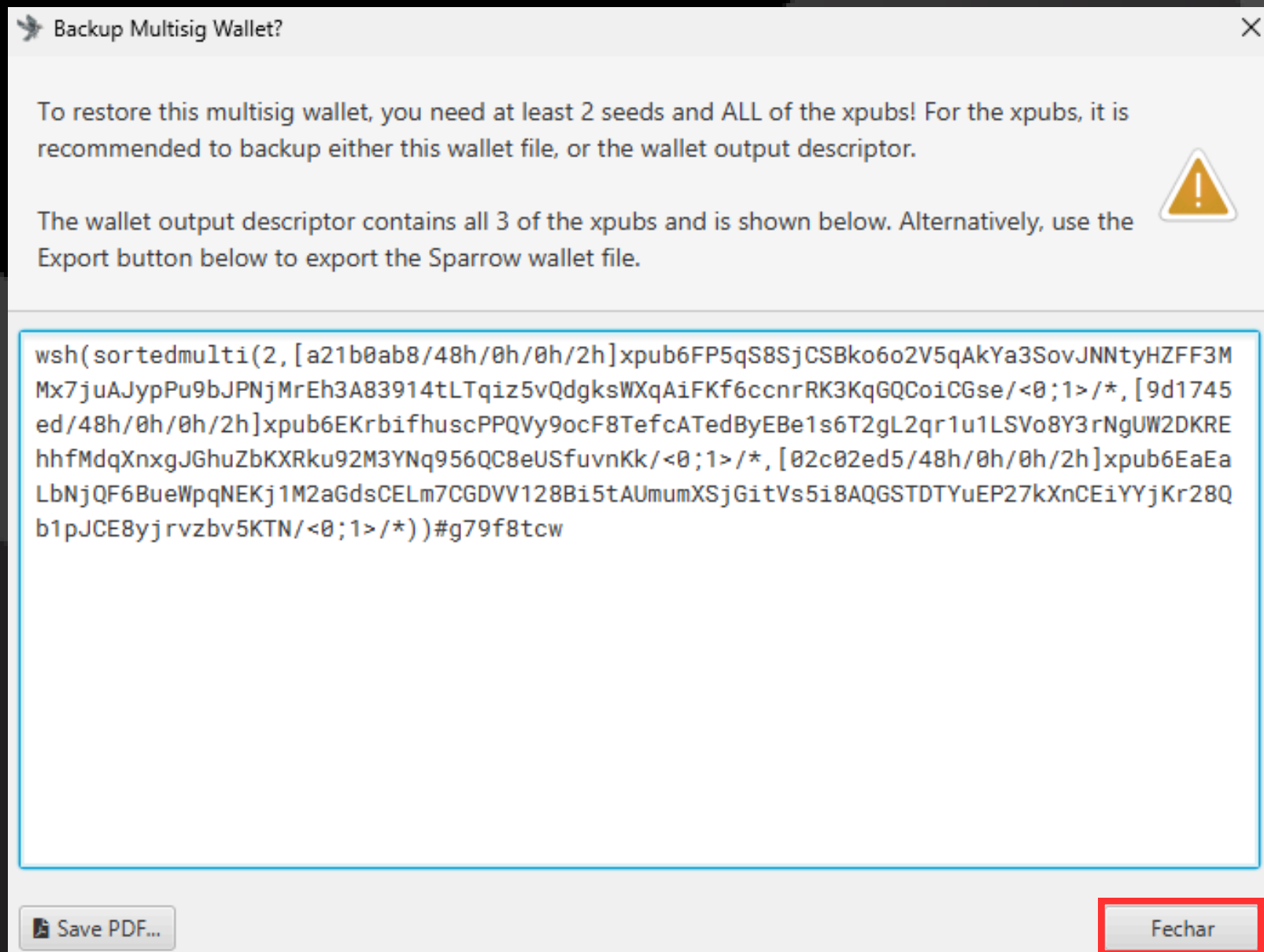
Armazenar o BSMS (Bitcoin Secure Multisig Setup) com segurança é essencial, pois ele contém informações fundamentais para recriar a configuração da carteira multisig em caso de perda ou troca de dispositivos. Sem ele, mesmo com as chaves privadas, pode ser impossível acessar os fundos, comprometendo a segurança e a continuidade da gestão dos bitcoins.

Clique em “Save PDF...”



Salve este pdf, pois ele será essencial em
nosso tutorial de número 4

Após salvar, clique em “Fechar”



Backup Multisig Wallet?



To restore this multisig wallet, you need at least 2 seeds and ALL of the xpubs! For the xpubs, it is recommended to backup either this wallet file, or the wallet output descriptor.



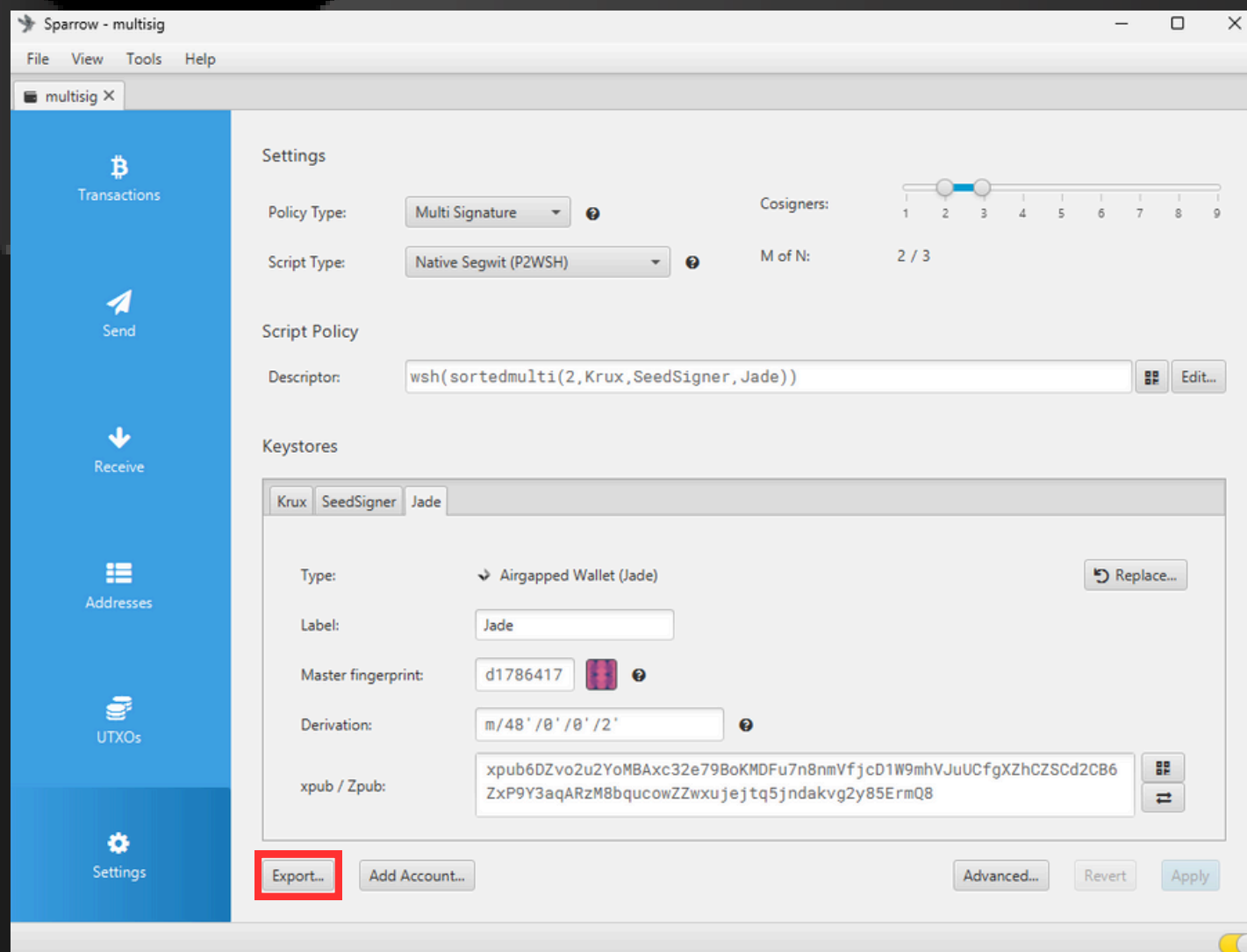
The wallet output descriptor contains all 3 of the xpubs and is shown below. Alternatively, use the Export button below to export the Sparrow wallet file.

```
wsh(sortedmulti(2,[a21b0ab8/48h/0h/0h/2h]xpub6FP5qS8SjCSBko6o2V5qAkYa3SovJNNtyHZFF3M  
Mx7juAJypPu9bJPNjMrEh3A83914tLTqiz5vQdgksWXqAiFKf6ccnrRK3KqGQCoicGse/<0;1>/*,[9d1745  
ed/48h/0h/0h/2h]xpub6EKrbifhuscPPQVy9ocF8TefcATedByEBE1s6T2gL2qr1u1LSVo8Y3rNgUW2DKRE  
hhfMdqXnxgJGhuZbKXRku92M3YNq956QC8eUSfuvnKk/<0;1>/*,[02c02ed5/48h/0h/0h/2h]xpub6EaEa  
LbnjQF6BueWpqNEKj1M2aGdsCElm7CGDvV128Bi5tAUmumXSjGitVs5i8AQGSTDTYuEP27kXnCEiYYjKr28Q  
b1pJCE8yjrzbv5KTN/<0;1>/*))#g79f8tcw
```

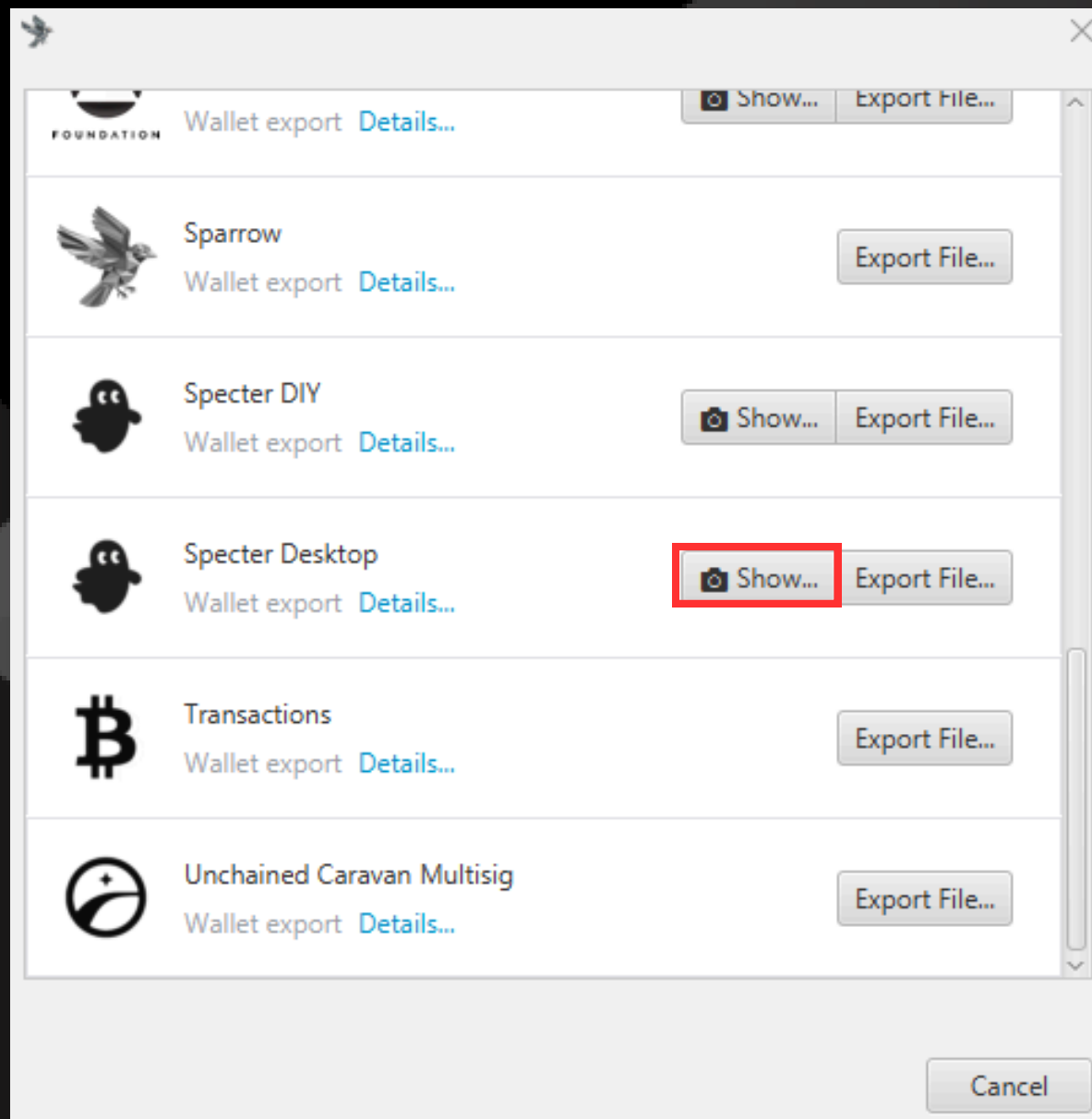
Save PDF...

Fechar

Vamos agora exportar o descritor da carteira para termos certeza de que fizemos todos os passos de forma correta. após memorizar, vamos clicar em “Export”



Vamos clicar em “Show”, na
“Specter Desktop”



Isso nos gerará um código QR, vamos precisar acessar a carteira com a devida fingerprint e realizar a leitura deste QR code



Vamos acessar sua carteira na Krux

@ cBBa4cal
Mainnet
Single-sig
m/84'/0' /0'
Sem Senha

Carregar Carteira

Senha

Customizar

◀ Voltar

Aqui vamos clicar em
“Customizar”

m/84'/0'/0'

Rede

Single/Multisig

Tipo de Script

Conta

◀ Voltar

“Clique em
Single/Multisig”



Single-sig

Multisig

“Clique em **Multisig**”

m/48'/0'/0'/2'

Rede

Single/Multisig

Tipo de Script

Conta

◀ Voltar

Note agora que
agora o 'derivation
path' foi alterado
para m/48'/0'/0'/2'

m/48'/0'/0'/2'

Rede

Single/Multisig

Tipo de Script

Conta

< Voltar

Clique em “Voltar”

@ cBBa4cal
Mainnet
Single-sig
m/84'/0' /0'
Sem Senha

Carregar Carteira

Senha

Customizar

◀ Voltar

Aqui vamos clicar em
“Carregar Carteira”

@ cBBa4cal

Backup de Mnemônico

Chave Pública Estendida

Carteira

Endereço

Assinar

Desligar

Agora em “Carteira”

@ cBBa4cal

Descritor de Carteira

Senha

Customizar

BIP85

◀ Voltar

Vá em “Descritor de
Carteira”

@ cBBa4cal

O descritor de saída da
carteira não foi encontrado.

Carregar um ?

Sim

Não

“Clique em **Sim**”

Carregar da Câmera

Carregar do cartão SD

◀ Voltar

Agora em
“Carregar da câmera”

Vamos ler este QR code gerado na Sparrow



Aqui poderá confirmar exatamente qual a Fingerprint de cada carteira participante da Multisig, no meu caso ficou assim:

DIY Multisig wallet

1. @ 02c02ed5
2. @ a21b0ab8
3. @ 9d1745ed

Confira os códigos e dê um clique na tela:

Agora poderá conferir também a Xpub de cada uma das carteiras que fazem parte da Multisig

DIY Multisig wallet

1. xpub6EKrbif..C8eUSfuvnKk

2. xpub6EaEaLb..yjrzbv5KTN

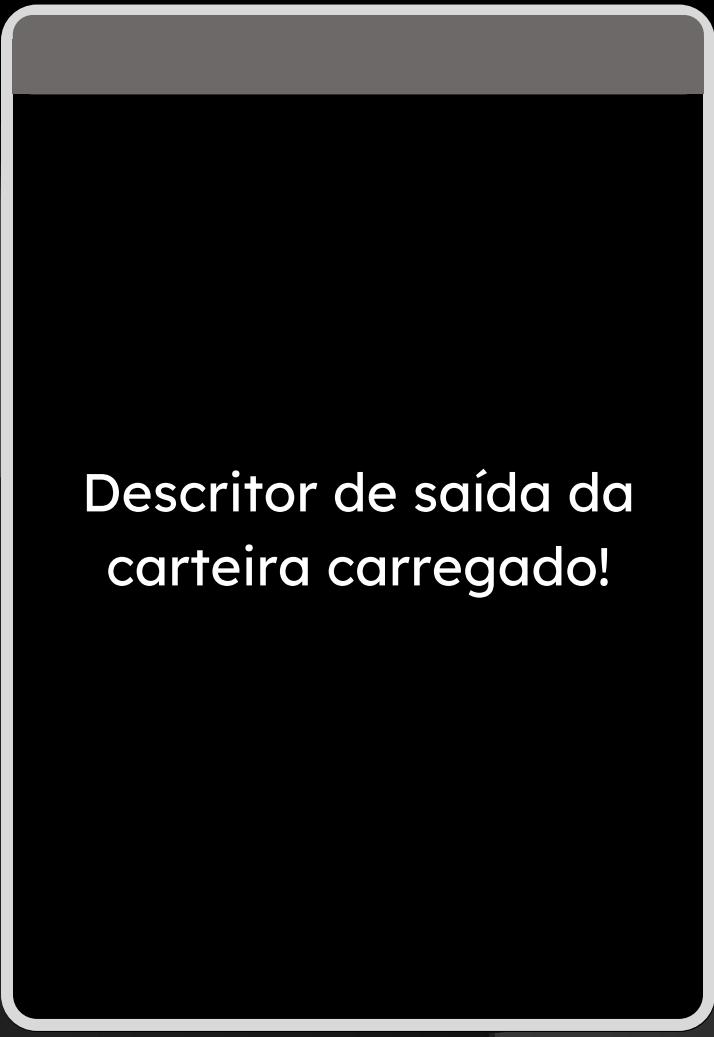
3. xpub6FP5qS8..KqGQCoicGse

Carregar ?

Sim

Não

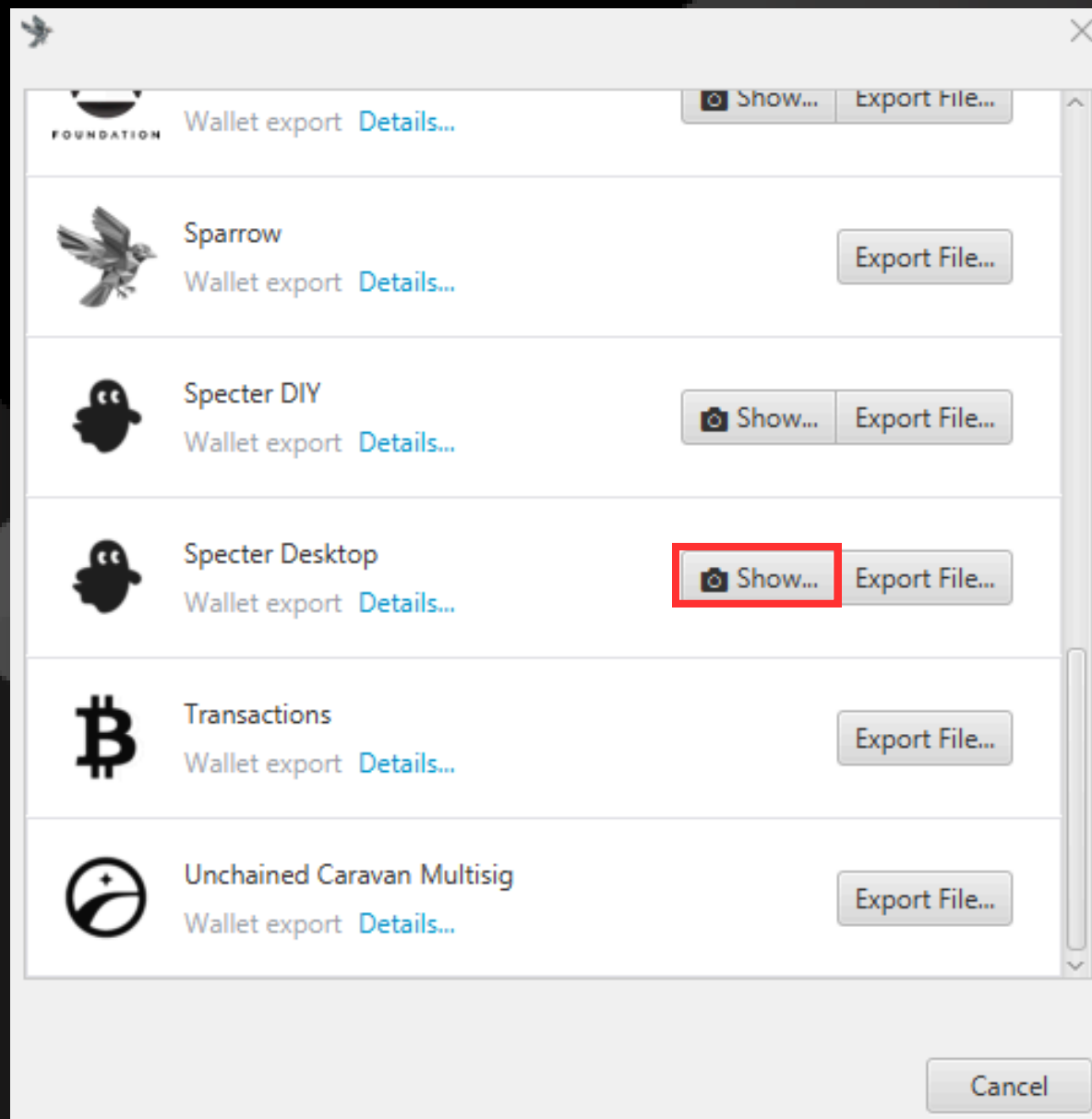
Confira os códigos e clique em “**sim**”:



Descritor de saída da
carteira carregado!

Uma breve
mensagem irá
aparecer:

Vamos agora adicionar o descritor também na SeedSigner



Vamos clicar em “Show”, na
“Specter Desktop”

E vemos realizar a leitura deste qr code



Para realizar a leitura do qr code, vamos em “Scan”



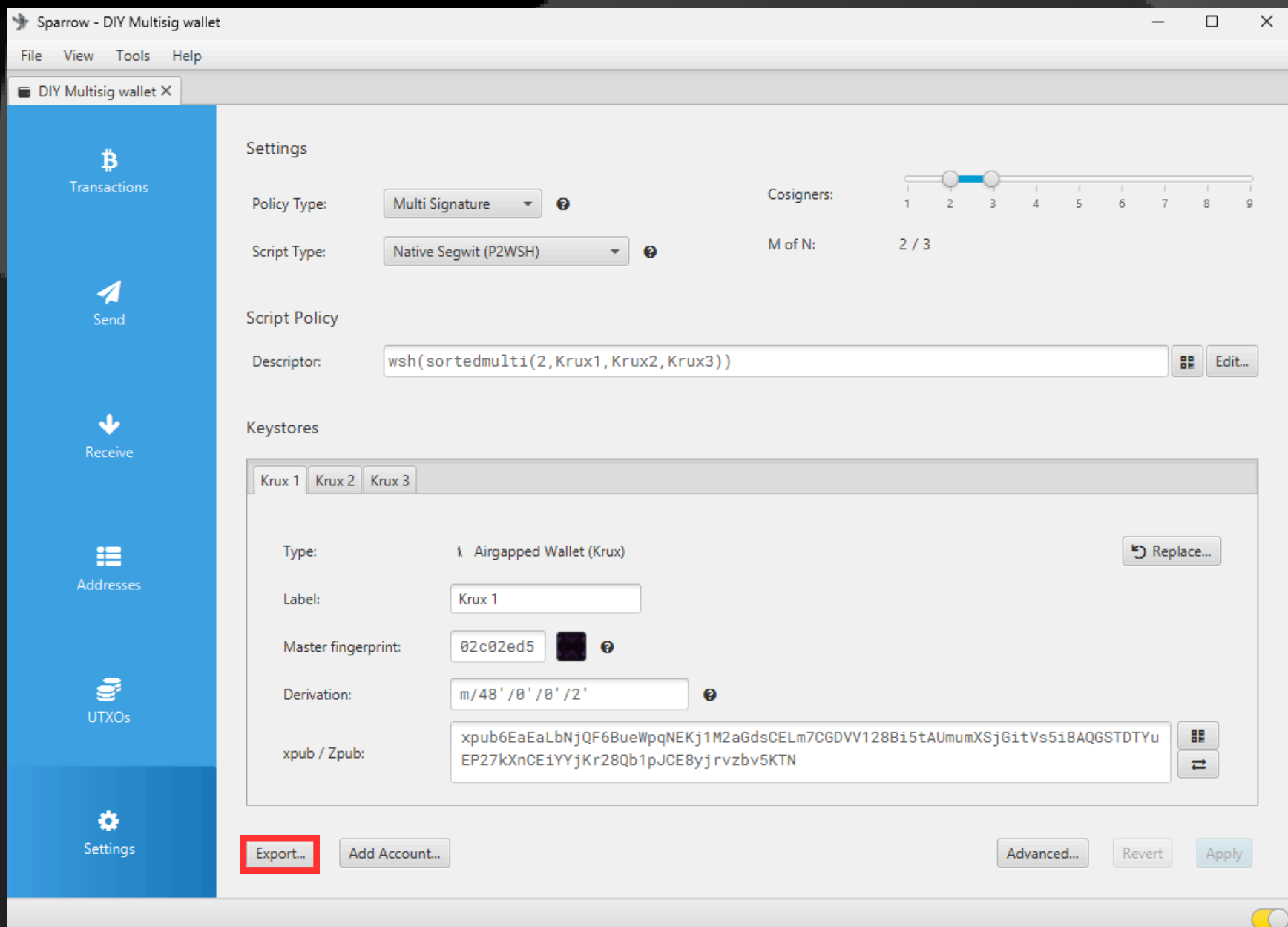
Confirme e clique em “ok”



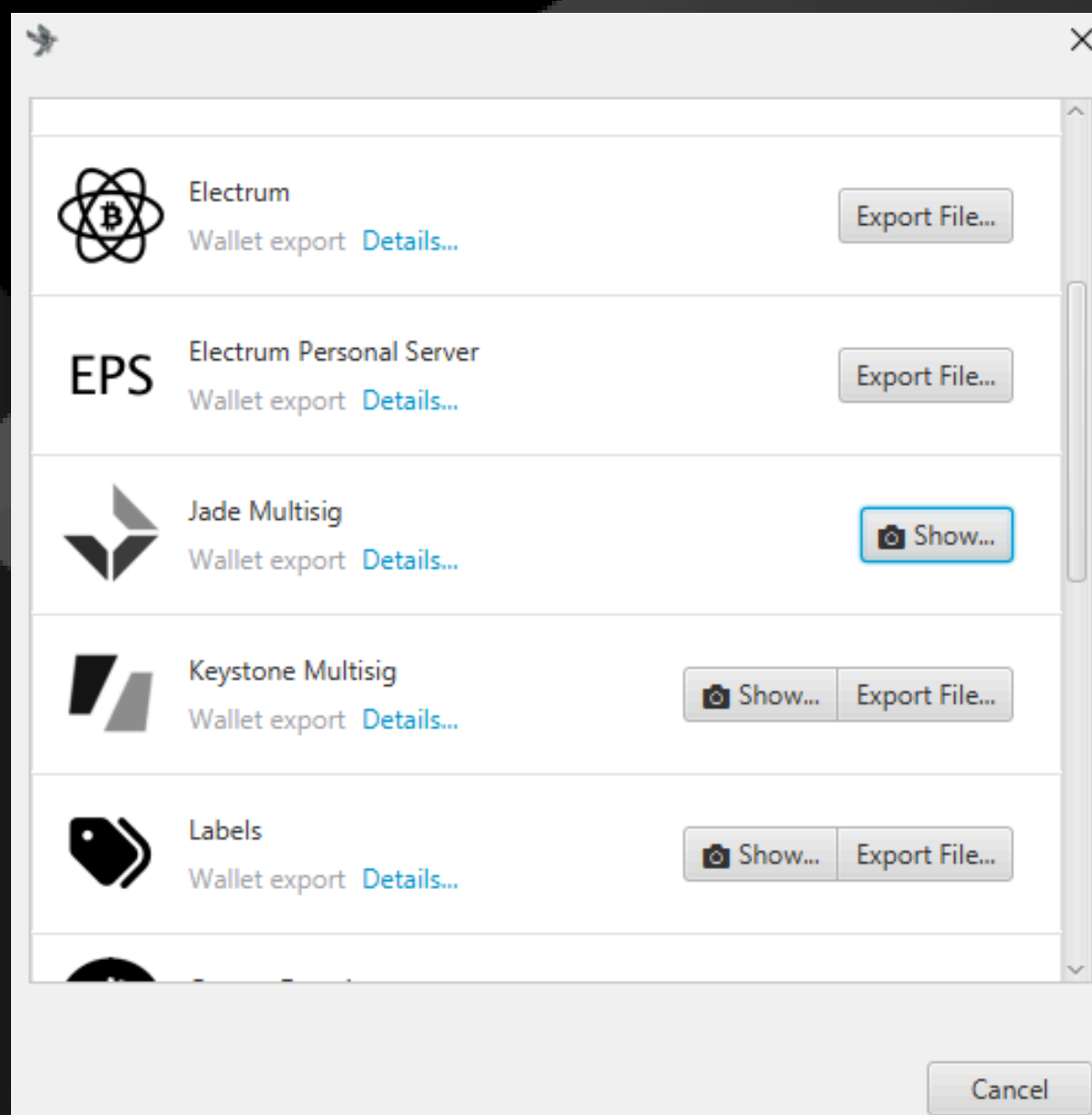
Confirme e clique em “ok”



Para a Jade, vamos clicar em “Export”



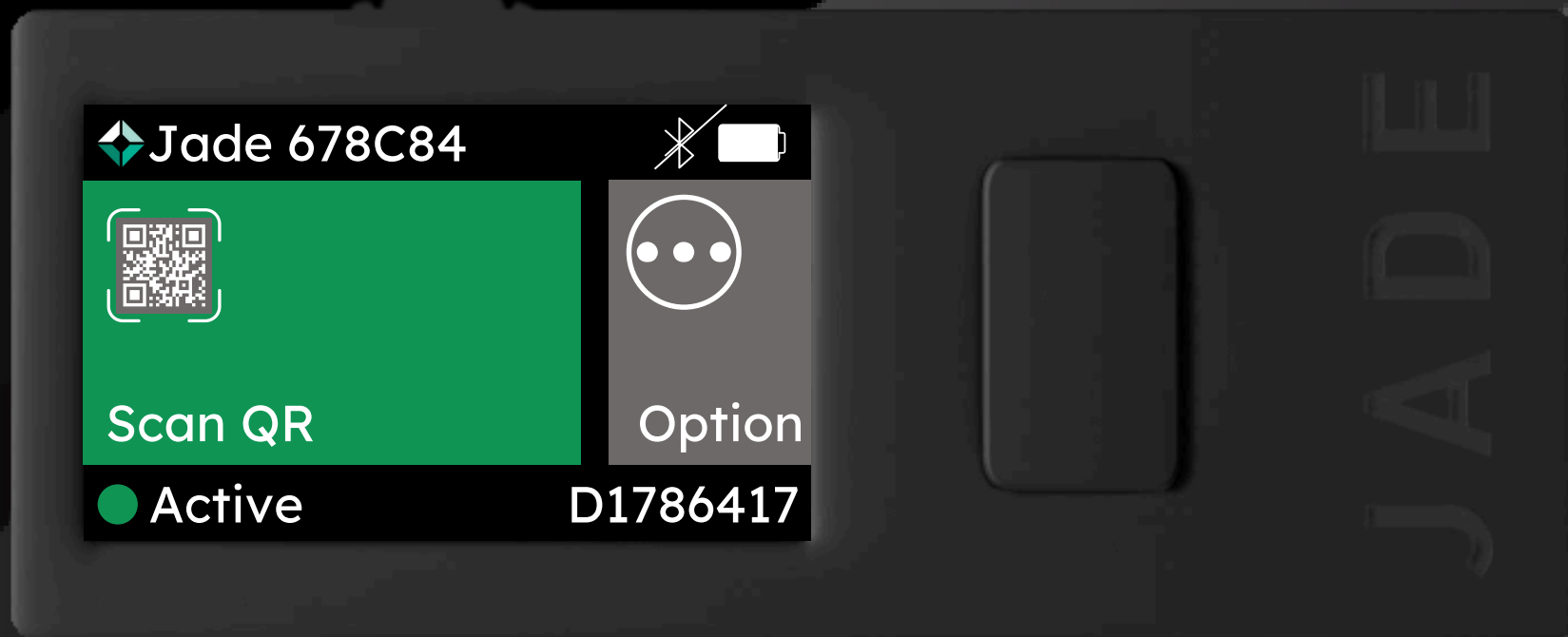
E agora em “Show” no campo “Jade Multisig”



Vamos então ler este QR Code gerado na tela:



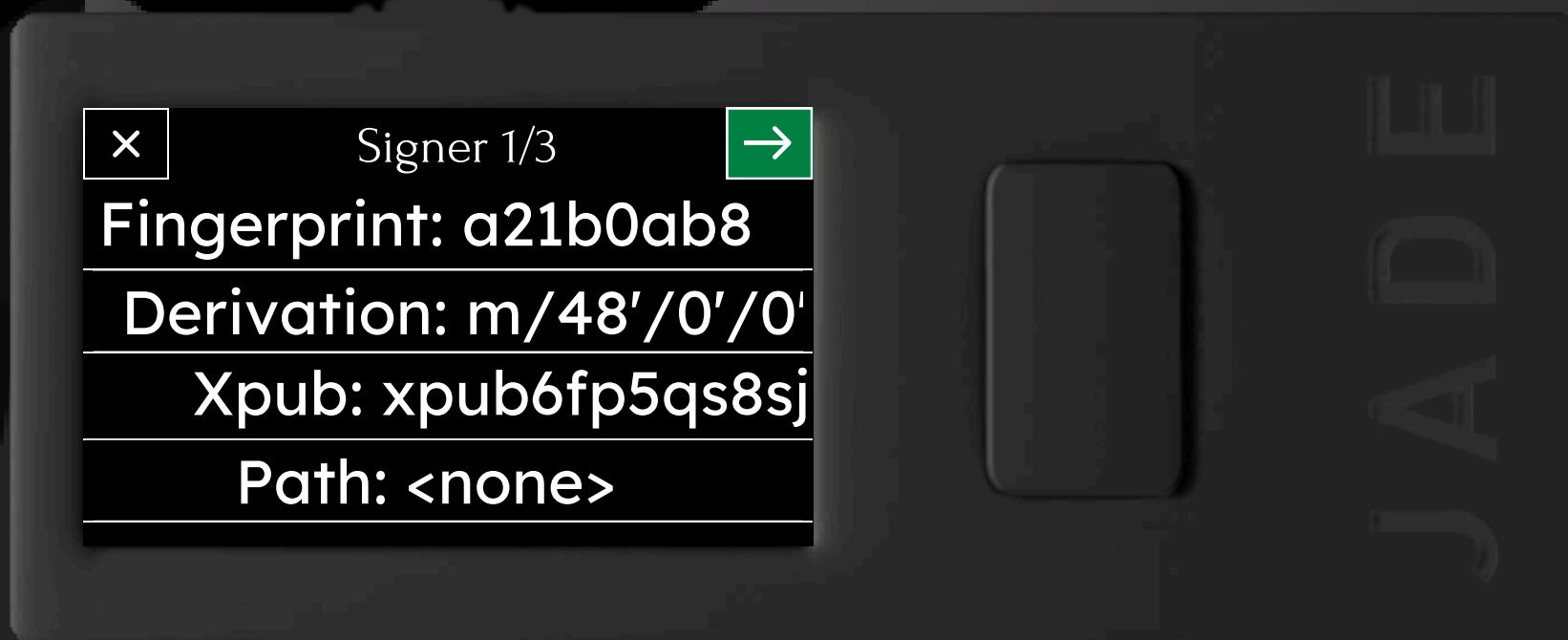
Vamos selecionar “Scan QR” e realizar a leitura



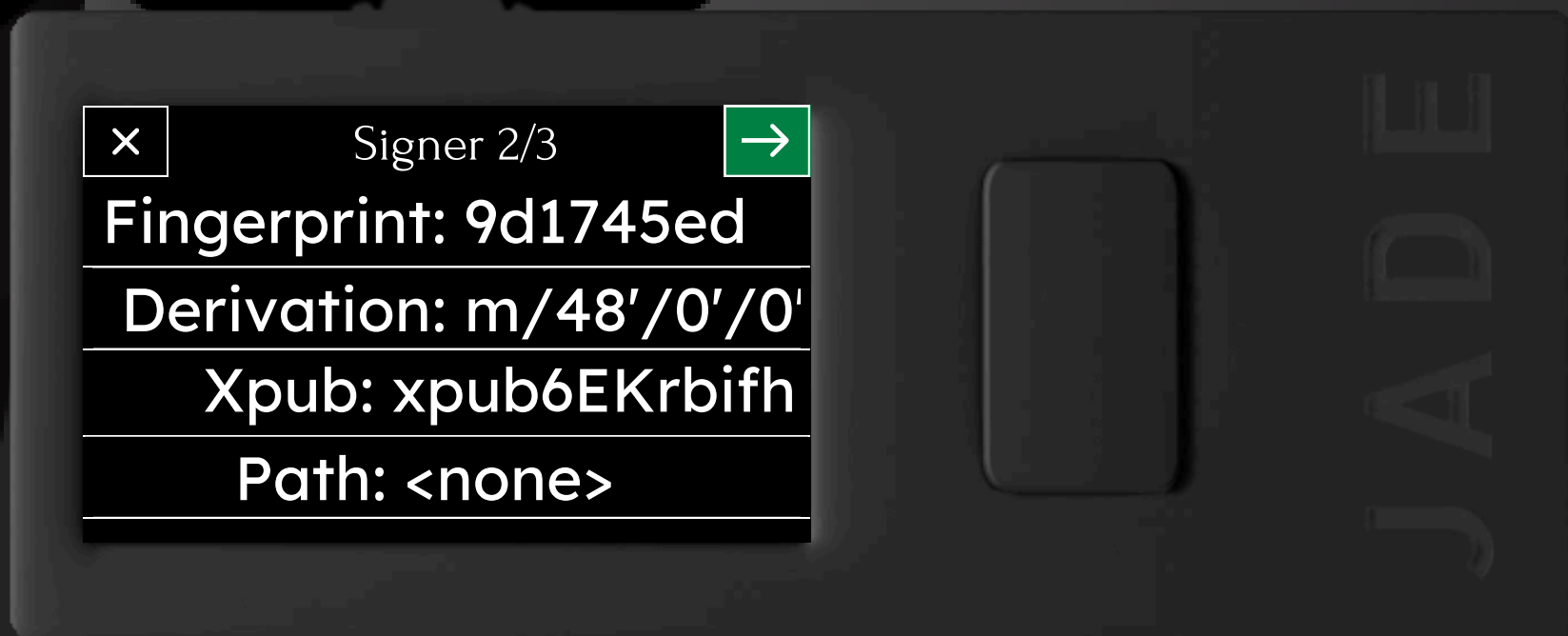
Clique no canto superior direito, conforme
mostra a imagem:



Aqui ele mostrará os dados de todos os assinantes. Confirme os dados e clique para seguir
Assinante 1



Aqui ele mostrará os dados de todos os assinantes. Confirme os dados e clique para seguir
Assinante 2



Aqui ele mostrará os dados de todos os assinantes. Confirme os dados e clique para seguir
Assinante 3

×	Signer 3/3 *	→
Fingerprint: d1786417		
Derivation: m/48'/0'/0'		
Xpub: xpub6DZvo2u		
Path: <none>		



JADE

Com todos os assinantes confirmados,
vamos confirmar o registro do descritor,
clikando no canto superior direito,
conforme mostra a imagem



Você acaba de aprender como configurar uma carteira multisig 2 de 3 com Krux, SeedSigner e Jade, integrando esses dispositivos à Sparrow Wallet.

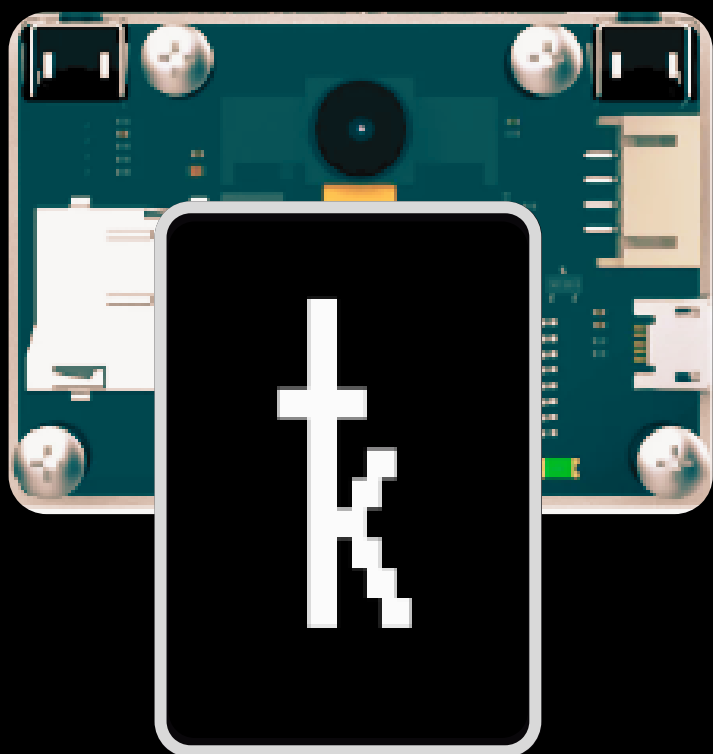
Vimos como gerar as chaves públicas de forma segura, montar os descritores corretamente e carregar toda a configuração para que sua multisig funcione de forma confiável.

Essa estrutura distribuída oferece uma camada extra de segurança e soberania — mesmo que um dos dispositivos seja perdido ou comprometido, seus fundos continuam protegidos.

No próximo tutorial, vamos colocar essa multisig em ação: você aprenderá como receber e enviar transações, assinando com os dispositivos necessários e garantindo que tudo funcione de ponta a ponta.

Se você chegou até aqui, está construindo uma base sólida para a verdadeira autocustódia. Até lá!

Sabemos que Multisig é um processo mais robusto, caso tenha alguma dúvida não hesite em nos chamar, estamos aqui para te ajudar!



GARANTA A MÁXIMA
SEGURANÇA

Compre na **DIY LAB**

WWW.DIYSECLAB.IO

