O QUE SÃO CARTEIRAS BIP-85 E PARA QUE SERVEM

As carteiras BIP-85 são carteiras determinísticas, por outras palavras são carteiras filhas de uma carteira mãe BIP-39, as vulgares carteiras de 12, 24 palavras.

Numa carteira BIP-85, a sua entropia é gerada através de um calculo matemático complexo. Tendo como base a Seed da Wallet mãe, sendo o processo inverso impossível de calcular. Quero com isto dizer que, a partir de uma Wallet BIP-85 não se consegue obter a fonte da sua origem, o que torna bastante seguro o seu uso em diferentes tipos de cenários.

Caso a Seed BIP-85 seja comprometida, a Seed mãe estará sempre segura, bastando gerar outra Wallet usando um Index diferente e mover os fundos que possam existir para a nova carteira.

Uma Wallet BIP-39 consegue gerar no total 10.000 carteiras BIP-85. Outra vantagem é que não precisa de fazer o backup da Seed em papel ou metal, bastando saber o seu respectivo Index, que começa em 0 e termina em 9999, o que prefaz o total de 10.000 carteiras possíveis de gerar.

Então pergunta o caro leitor, para que serve ter uma Wallet BIP-85?

- Para importar numa software Wallet, tipo BlueWallet ***https://bluewallet.io***, não havendo a necessidade de fazer o backup e permitindo usar como carteira para pagar ou receber Bitcoin onchain, layer1 no smartphone ou no computador com a SparrowWallet ***https://sparrowwallet.com/download***
- Criar uma Wallet para um familiar que ainda domina pouco Bitcoin, ou pouco responsável, ou até para queles que são muito esquecidos .
- Uma carteira para receber donativos
- Uma carteira para usar com paynym ***https://alexemidio.substack.com/p/o-paynym-bip47-e-uma-implementacao***
- Carteira para usar com compras P2P
- Carteira de salto entre Exchanges e carteira mãe

No mercado existem várias Hardware Wallets que permitem gerar carteiras BIP-85, como é o caso da famosa Coldcard.

10/05/2024 ₿itcoinPle₿e LNURL: bitcoinplebe@Wallets.fyoumoneypod.com

O QUE SÃO CARTEIRAS BIP-85 E PARA QUE SERVEM

E para quem não tem ainda uma Hardware Wallet, é possível gerar uma Wallet BIP-85 por software?
Sim, claro. Existem duas excelentes ferramentas que o permitem fazer.

https://iancoleman.io/bip39 do Ian Coleman
***https://bitcoiner.guide/Seed* do Bitcoiner Guide**

Uma nota importantíssima para sua segurança. Só deve utilizar estas ferramentas num ambiente totalmente off-line com um sistema operativo amnésico como o caso do ***TAILS https://tails.net/install/download/index.pt.html*** sem cabo de rede ou ligação WI-FI.