

Dúvidas Sobre BIP 39 e 44: Como Recuperar Suas Criptomoedas em Carteiras Diferentes?



Fala Defizeros👋, tudo bem por aí?

“O que acontece se a empresa Ledger vir a falência ou deixar de existir?” Ou “E se a Metamask sumir de repente? Ela irá levar minhas criptomoedas junto?” Estas são algumas perguntas que muitos investidores iniciantes acabam tendo e, para responder esta e algumas outras dúvidas, lhe trouxemos este artigo!

Pois existe uma coisa chamada **BIP 39 e 44** que em geral: tratam-se de protocolos de compatibilidade, onde muitas associam-se! Com isso, se alguma dessas carteiras deixar de existir, você poderá recuperar seus Bitcoins / Tokens em outras carteiras compatíveis.

Bora conhecer um pouco mais sobre o BIP 39 e 44!👀

📌 O que são carteiras BIP 39?

As **Carteiras BIP39** são uma parte importante do ecossistema de criptomoedas, especialmente quando trata-se de armazenar e recuperar chaves privadas. Vamos entender melhor: **BIP39 (Bitcoin Improvement Proposal 39)**:

- A BIP39 é um **padrão** que permite criar **frases mnemônicas** para recuperar carteiras de Bitcoin;
- Essa frase mnemônica é uma **sequência de palavras** (geralmente 12, 18 ou 24) que serve como **backup** para recuperar sua carteira.



A imagem representa dois aliens cavando o próprio túmulo em 2039 após a Ledger declarar falência; até descobrirem que o BIP 39 e 44 podem salvá-los de tal infortúnio.

-
- Antes da BIP39, **as chaves privadas eram representadas por sequências alfanuméricas difíceis de lembrar**;
 - Com a BIP39, as chaves privadas são apresentadas como palavras comuns, facilitando a memorização e anotação;
 - Ao configurar uma carteira não custodial, você é orientado a anotar essas palavras na ordem em que surgem e mantê-las em um local seguro.

📌 O que são carteiras BIP 44?

1. Sobre o BIP44 (Bitcoin Improvement Proposal 44):

- O BIP44 é outro padrão que define **caminhos de derivação** para carteiras hierárquicas determinísticas (HD);
- Ele especifica como as carteiras geram chaves a partir da semente mnemônica;

- Carteiras como Ledger, Trezor e Keepkey **usam o padrão BIP39 para gerar a chave mestra e o BIP44 para derivar subchaves.**



E então esses aliens descobrem uma luz no fundo da cova! Essa luz chama-se: BIP 39 e 44

Em resumo, **a BIP39 simplifica o acesso aos seus fundos e a recuperação de carteiras, enquanto o BIP44 define como as chaves são derivadas para diferentes propósitos dentro da mesma carteira.** Ambos são essenciais para a segurança e usabilidade das carteiras de criptomoedas.

- Lembrando que devemos estar na **Última Temporada** para o **Airdrop da Grass ser Lançado**, com isso, você poderá garantir seus pontos instalando a Extensão em seu Navegador **Clicando Aqui!**

📌 Quais carteiras são compatíveis com a BIP 39 e 44?

Aqui estão algumas **carteiras compatíveis** com os padrões **BIP39 e BIP44** que separamos para vocês:

- **Carteiras de Hardware:**
 - **Ledger:** Um dispositivo físico que suporta BIP39 e é popular para armazenar criptomoedas com segurança;

- **Trezor:** Outro hardware wallet confiável que segue os padrões BIP39 e BIP44;
- **Keepkey:** Um terceiro exemplo de carteira de hardware que utiliza esses padrões.



- **Carteiras de Software (Desktop):**

- **Electrum:** Uma carteira de desktop leve e versátil que é compatível com BIP39;
- **Exodus:** Uma carteira de software com interface amigável que também suporta BIP39;
- **Atomic Wallet:** Outra opção que segue os padrões BIP39 e BIP44.

- **Carteiras Móveis (Android / iOS):**

- **Coinomi:** Uma carteira móvel que permite gerenciar várias criptomoedas e é compatível com BIP39;
- **Trust Wallet:** Uma carteira móvel popular que suporta BIP39 e é fácil de usar! > [Tutorial](#)
- **MyEtherWallet (MEW):** Embora seja mais conhecida para Ethereum, também é compatível com BIP39 e BIP44.

📌 **Posso recuperar minhas criptomoedas que estão na Trezor na Ledger?**

Sim, você poderá recuperar suas criptomoedas da Trezor na Ledger (e ao contrário também é verdadeiro) usando os padrões BIP39 e BIP44. **Aqui estão os passos:**

- **Recuperação da Trezor:**
 - **Anote a frase mnemônica** (palavras-chave) que você gerou ao configurar sua Trezor. Essa frase é compatível com o BIP39;
 - Certifique-se de que sua Ledger esteja configurada e pronta para uso.



- **Configuração da Ledger:**
 - Configure sua Ledger seguindo as instruções da fabricante;
 - Durante a configuração, você terá a opção de **restaurar uma carteira existente**. Escolha essa opção.

-
- **Inserção da Frase Mnemônica:**
 - Na Ledger, insira sua frase mnemônica (BIP39) na **ordem correta**;
 - A Ledger usará essa frase para derivar as chaves privadas e públicas associadas à sua carteira Trezor.



- **Verificação e Acesso aos Fundos:**
 - Após inserir a frase mnemônica, a Ledger deve mostrar os endereços de sua carteira Trezor;
 - Verifique se os endereços correspondem aos da sua Trezor original;
 - Agora você pode acessar seus fundos na Ledger usando a mesma chave privada da Trezor.

📌 Também posso recuperar minhas criptomoedas que estão na Metamask para a Rabby?

Sim, você pode recuperar suas criptomoedas da MetaMask na Rabby seguindo os passos adequados. Então perceba que também é possível fazer a recuperação com outras criptomoedas além do Bitcoin. Aqui está o que você precisa fazer:

- **Frase de Recuperação Secreta (SRP):**
 - A MetaMask gera uma frase de recuperação secreta (SRP) de 12 palavras quando você configura sua carteira;
 - Essa frase é crucial para recuperar sua carteira e seus fundos em qualquer outra plataforma compatível com BIP39.



- **Restaurando na Rabby:**
 - Instale a carteira Rabby (se ainda não tiver feito);
 - Durante a configuração da Rabby, escolha a opção para **importar uma carteira existente**;
 - Insira sua SRP da MetaMask na ordem correta;
 - A Rabby usará essa SRP para derivar as chaves privadas e públicas associadas à sua carteira MetaMask.
-

- **Verificação e Acesso aos Fundos:**
 - Após importar a SRP, **verifique se os endereços da Rabby correspondem aos da sua MetaMask original**.
 - Agora você pode acessar seus fundos na Rabby usando a mesma chave privada da MetaMask.
-

📌 **Existe algum risco ao transferir fundos entre carteiras usando este método?**

Transferir fundos entre carteiras usando os padrões BIP39 e BIP44 **é geralmente seguro**, mas é importante considerar alguns pontos:

- **Precisão da Frase Mnemônica:**

- Ao inserir a frase mnemônica (SRP) ou palavras-chave, verifique se você digitou corretamente. Qualquer erro pode resultar na perda de acesso aos seus fundos.



- **Segurança do Ambiente:**
 - Certifique-se de estar em um ambiente seguro e livre de malware ao realizar a importação;
 - Evite fazer isso em computadores públicos ou dispositivos comprometidos.

-
- **Confiança nas Carteiras:**
 - Use apenas carteiras confiáveis e bem estabelecidas;
 - Evite carteiras desconhecidas ou suspeitas.

-
- **Chaves Privadas:**
 - Lembre-se de que, ao importar sua SRP ou frase mnemônica, você está essencialmente transferindo suas chaves privadas para outra carteira;
 - Mantenha essas informações seguras e não compartilhe com ninguém.

-
- **Teste Pequenas Quantidades:**

- Antes de transferir grandes quantias, **teste com uma pequena quantidade** para garantir que tudo funcione conforme o esperado.

Em resumo, se você seguir as melhores práticas de segurança e verificar cuidadosamente cada etapa, a transferência de fundos entre carteiras usando esses métodos: **é seguro**.

📌 O que fazer em caso de erro durante a importação da frase mnemônica?

Se você encontrar um erro durante a importação da frase mnemônica, **siga estas etapas**:

- **Verifique a Ortografia:**
 - Confirme se você digitou as palavras corretamente **e na ordem exata**;
 - Erros de digitação podem resultar em problemas de acesso à carteira.



- **Tente Novamente:**
 - Às vezes, erros simples podem ocorrer. Tente importar novamente a frase mnemônica;
 - Certifique-se de estar usando a carteira correta (por exemplo, MetaMask ou Rabby).
-

- **Consulte a Documentação:**
 - Verifique a documentação oficial da carteira que você está usando;

- Procure por guias específicos sobre como importar uma carteira existente.

—

- **Contate o Suporte:**
 - Se o erro persistir, entre em contato com o suporte da carteira;
 - Eles podem fornecer orientações específicas com base no problema que você está enfrentando.

Lembre-se de manter suas informações seguras e não compartilhar sua frase mnemônica com ninguém além de você mesmo. Caso o suporte da carteira peça suas chaves privadas, **desconfie na hora e JAMAIS as compartilhe!**

—

Conclusão:

Defizeros, como puderam ver, **não há motivos para se preocupar caso uma Metamask ou Ledger deixem de existir**, pois suas chaves estão diretamente ligadas com a **Blockchain** e empresa nenhuma poderá “roubar” suas criptomoedas.

—

Com isso, **você poderá fazer o teste de “recuperar” suas chaves da Metamask na Trust Wallet**, por exemplo. O processo em si é muito simples e universal: basta acessar a carteira baseado nas palavras sementes já criadas anteriormente **que você terá seus fundos visíveis.**

—

***Feito por Lucas Lippe, o Alien Mafioso! 🛸**