santacroce tech

visão de mercado

6/MARÇO/2025

ÍNDICE

INTRODUÇÃO

Nossa quarta newsletter explora a autocustódia de Bitcoin, um conceito frequentemente confundido com carteiras de hardware — dispositivos projetados para interagir com a rede Bitcoin. No entanto, como demonstraremos nesta análise, a segurança depende menos do dispositivo em si e mais do processo de configuração.

Muitos usuários, até mesmo os experientes, costumam focar demais na complexidade da frase-senha ou no uso de múltiplos dispositivos de autenticação. Embora essas sejam medidas de segurança importantes, eles frequentemente ignoram um elemento-chave: um backup físico confiável.

Na prática, a segurança é tão forte quanto seu elo mais fraco, reforçando a necessidade de uma abordagem bem estruturada.

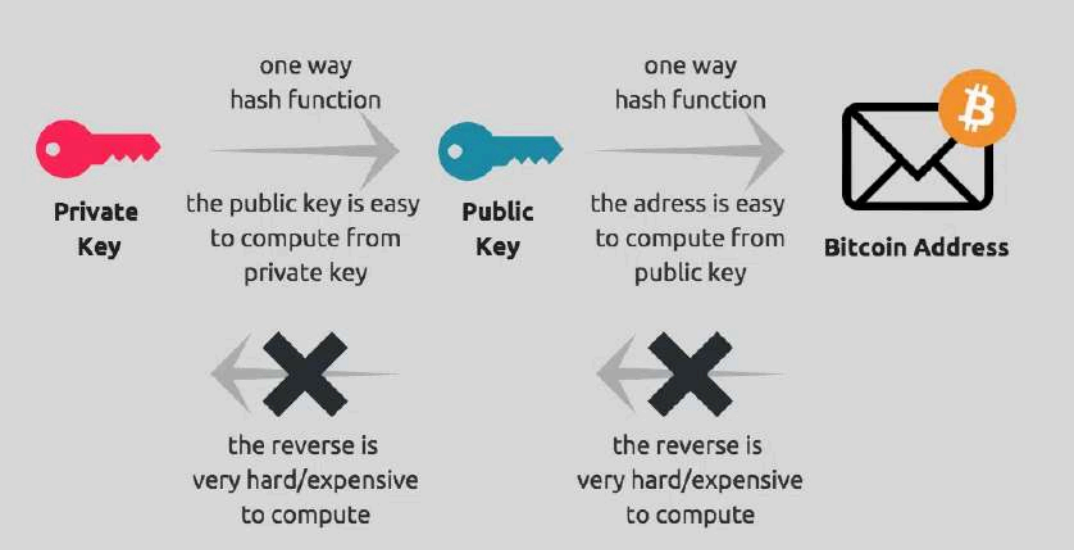
Se você nunca usou uma carteira de criptomoedas antes, não se preocupe. Este guia abordará os fundamentos e fornecerá instruções passo a passo para gerar e armazenar suas senhas de forma segura. Vamos começar!

Roberto Santacroce Martins
Programador, Fundador @ Santacroce Tech

COMO O BITCOIN É MOVIMENTADO E PROTEGIDO?

Uma carteira de Bitcoin consiste em milhões de endereços conectados através de chaves públicas e privadas. O gerenciamento da carteira é simplificado usando uma chave-mestra, conhecida como "*seed phrase*", uma sequência de palavras que concede acesso e controle sobre todos os endereços dentro da carteira.

Ao realizar uma transação, o software da carteira gera um código criptografado contendo detalhes essenciais, como os endereços do remetente e do destinatário e o valor da transação. Isso garante que nenhum dado privado ou senha seja compartilhado enquanto a transação se propaga pela rede Bitcoin, mantendo as informações do usuário seguras.

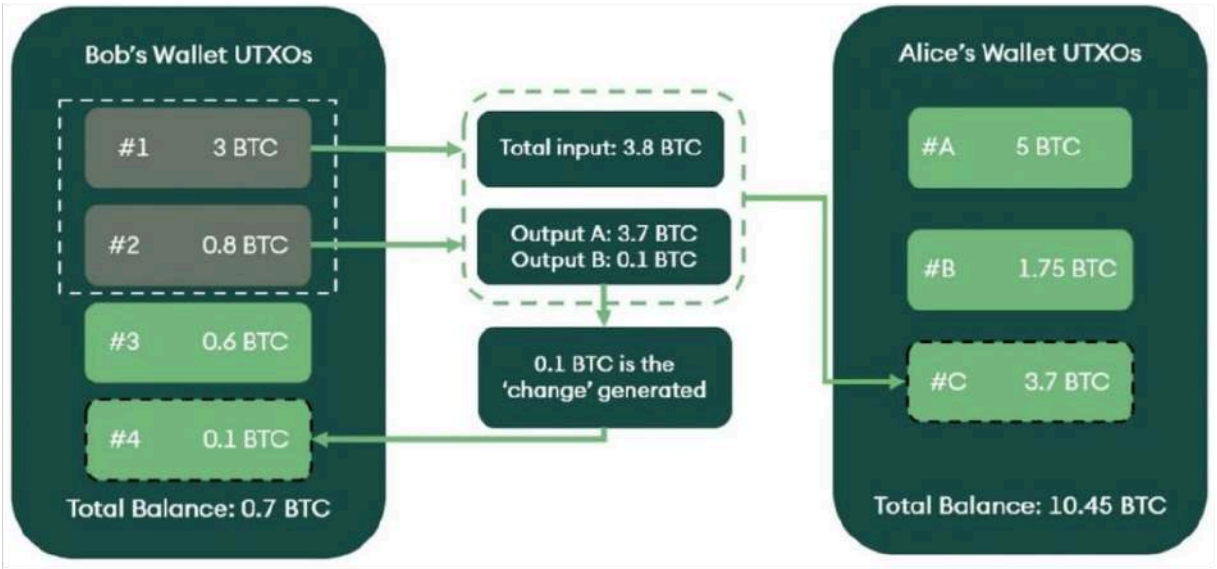


Conceitos de chave pública e privada. Fonte: Mycryptopedia

COMO O GASTO DE BITCOIN É RASTREADO?

Uma carteira de Bitcoin interage com a rede gerenciando “Saídas de Transação Não-Gastas” (UTXOs, em inglês), que representam o Bitcoin disponível em um endereço. Quando uma transação é iniciada, a carteira seleciona os UTXOs necessários para gastar, combinando-os se preciso. Cada UTXO corresponde a uma saída não-gasta de uma transação anterior.

A carteira gera uma nova transação, assina-a com a chave privada para provar a posse dos UTXOs e a transmite para a rede Bitcoin. Os mineradores então verificam e a incluem em um bloco. A carteira monitora continuamente as saídas gastas e não-gastas, atualizando assim o saldo em tempo-real.



Modelo de transação UTXO do Bitcoin. Fonte: Phemex

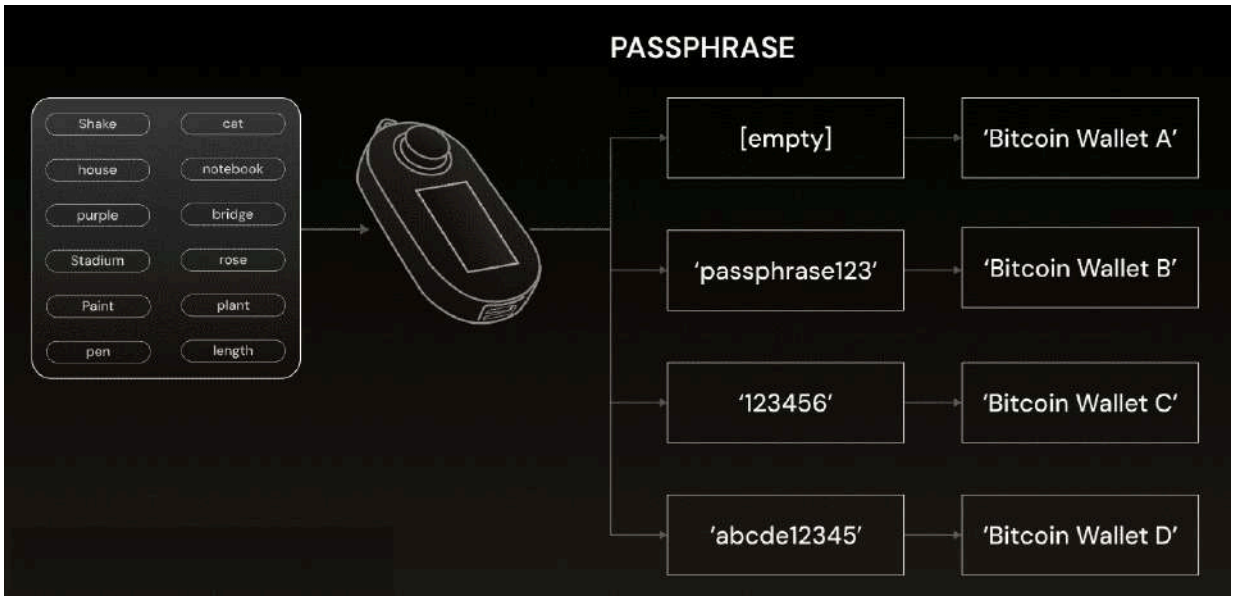
O QUE É MULTISIG E FRASE-SENHA?

Assinatura múltipla (*Multisig*) e frase-senha (*passphrase*) são recursos de segurança projetados para proteger carteiras de Bitcoin. Multisig exige múltiplas chaves privadas para autorizar uma transação, adicionando uma camada extra de segurança. Por exemplo, uma carteira pode exigir duas de três chaves para aprovar uma transação, evitando que um único indivíduo tenha controle total.

DINHEIRO SOBERANO: Multisig Jade/Blue Wallet

Já uma frase-senha (*passphrase*) oferece proteção adicional para uma chave privada. Mesmo que alguém obtenha acesso à chave mestra (*seed phrase*), não conseguirá acessar a carteira sem a frase-senha (*passphase*) correta. Ambos os recursos fortalecem a segurança ao exigir múltiplos fatores para acessar ou movimentar fundos.

BITCOIN DESBLOQUEADO: Trezor Safe 3 / Sparrow



Frase-senha de Bitcoin usada para gerar múltiplas carteiras. Fonte: Cypherock

COMO OBTER UMA BOA ENTROPIA?

[redacted]

Para uma entropia forte na geração de chaves mestra (*seed phrases*) de Bitcoin, um método offline é essencial. Um dispositivo Jade ou SeedSigner permite que os usuários rolem um dado de seis lados várias vezes, insiram os resultados e gerem uma chave-mestra segura. Como esses dispositivos permanecem offline, eles evitam ataques remotos. A *seed phrase* deve ser anotada, verificada e armazenada de forma segura, sem cópias digitais.

Outra abordagem é usar uma ferramenta BIP39 offline para transformar entropia em uma chave-mestra de 12/24 palavras. Instale um software de máquina virtual, como o VirtualBox, no seu PC/Mac e configure um ambiente Linux novo e isolado. Baixe a ferramenta BIP39 do Ian Coleman e transfira-a para a máquina virtual via USB. Execute o arquivo HTML no navegador da máquina virtual, insira sua entropia e gere a chave-mestra segura.

Wicked Smart Bitcoin: Geração de seed por rolagem de dados

Crypto Guide: Geração de carteira BIP39 com confiança zero

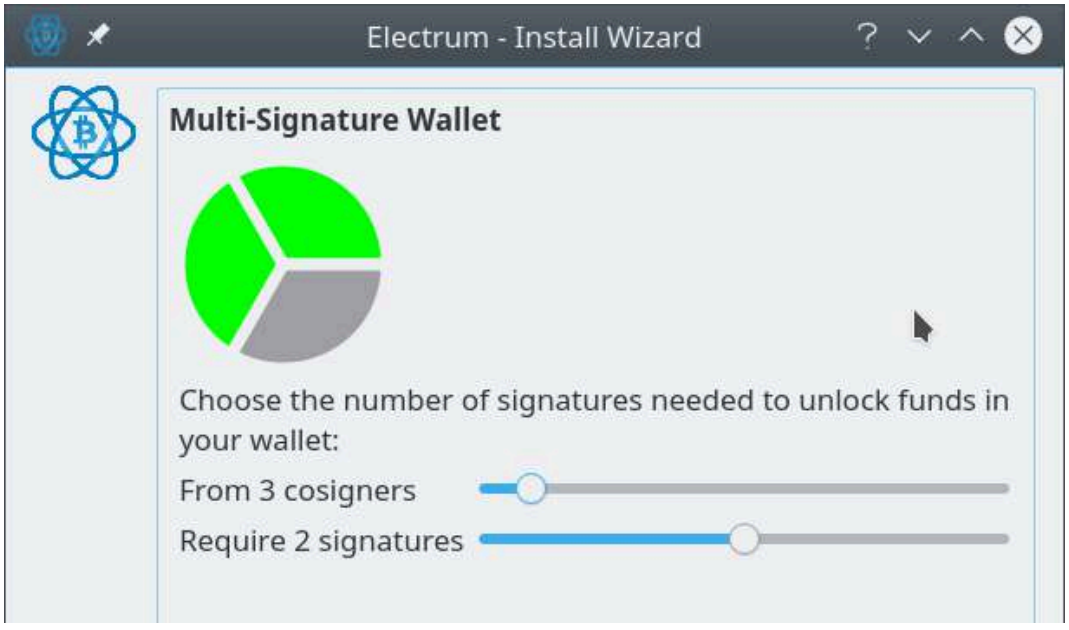
VALE A PENA USAR MULTISIG?

[redacted]

Depende. Para a maioria dos usuários, uma frase-senha (*passphrase*) oferece segurança suficiente, resolvendo 90% dos riscos potenciais sem a complexidade do multisig. No entanto, se armazenar a chave-mestra (*seed phrase*) de forma segura for difícil, o Multisig torna-se uma opção viável. Ele é especialmente útil para planejamento de herança e carteiras corporativas, onde várias partes precisam de controle de acesso. Instituições frequentemente usam multisig para evitar um único ponto de falha.

Idealmente, um recurso de bloqueio por tempo deveria estar em vigor — permitindo, por exemplo, que um multisig 2-de-3 reverta para 1-de-3 após um período definido. Isso garante acesso emergencial enquanto mantém a segurança. Embora o multisig adicione proteção, ele também aumenta a complexidade da configuração e os desafios de recuperação.

BITCOIN EDUCATION: Bitcoin com bloqueio de tempo + Multisig Decrescente



Configuração de carteira multisig usando Electrum

VALE A PENA USAR UMA CARTEIRA FÍSICA?

Uma carteira física (*hardware wallet*) vale a pena, mas não deve ser considerada confiável para a geração de chaves-mestra (*seed phrase*). Em vez disso, usar rolagens de dados ou métodos offline garantem uma entropia mais forte, mantendo a compatibilidade com a maioria das carteiras físicas. Para a maioria dos usuários, a principal diferença entre os dispositivos disponíveis está na experiência do usuário e no software, mais do que na segurança.

As opções incluem Trezor, SeedSigner, Krux, Jade, KeepKey, BitBox02 e Passport. Sempre compre diretamente do fornecedor oficial — nunca de marketplaces de terceiros, para evitar riscos de adulteração. Idealmente, escolha métodos sem conexão (air-gapped) para transações, como códigos QR, cartões de memória ou câmeras, reduzindo a exposição a possíveis vulnerabilidades.

Crypto Guide: Tutorial Trezor

Southern Bitcoiner: Tutorial BitBox02

Examplos de carteiras físicas

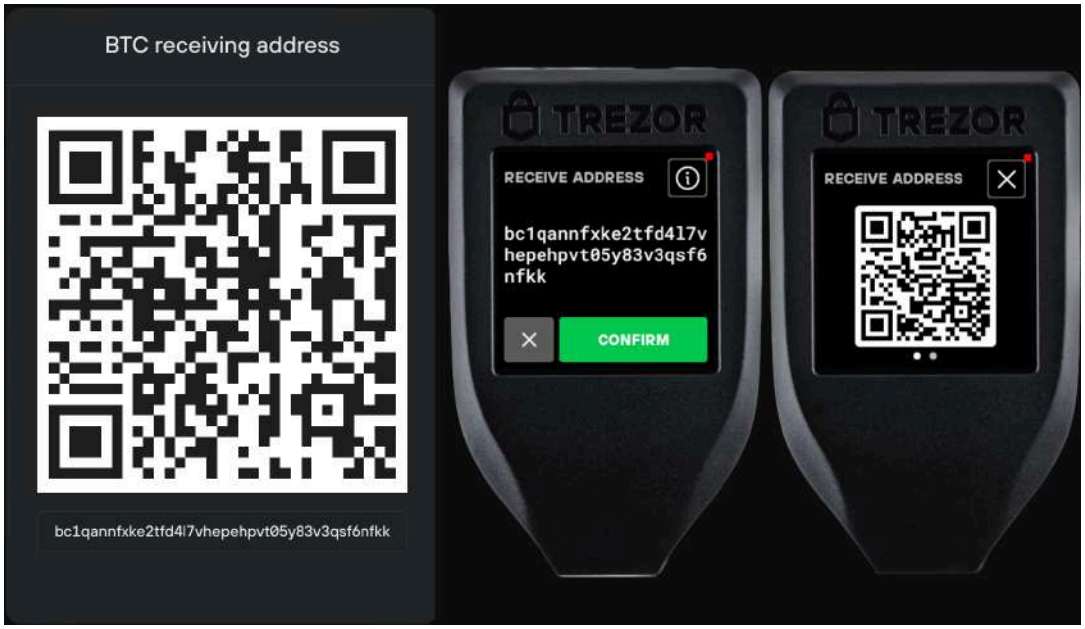
COMO USAR MÉTODOS AIR-GAPPED?

Para usar métodos air-gapped com a carteira Jade, comece exportando a chave pública estendida (xpub) da sua carteira. No Jade, vá ao menu de configurações, selecione "Exportar xpub" e exiba o código QR. Abra o Sparrow Wallet em um computador online, crie uma nova carteira, escolha a opção "Somente Visualização" (*Watch-Only*) e escaneie o código QR do Jade. Isso permite que o Sparrow visualize saldos e crie transações sem acessar as chaves privadas.

Para enviar Bitcoin, insira o endereço do destinatário e o valor no Sparrow e clique em "Criar Transação Não Assinada". Exiba o código QR gerado. No Jade, escaneie esse código QR, assine a transação offline e gere um novo código QR. Escaneie-o de volta no Sparrow e clique em "Transmitir" para enviá-lo à rede Bitcoin. Isso mantém as chaves privadas completamente offline.

BTC Sessions: Jade Plus + Sparrow

Crypto Guide: SeedSigner/Krux + Sparrow/Electrum



Transação air-gapped. Fonte: Ledger

BACKUPS EM PLACAS DE METAL

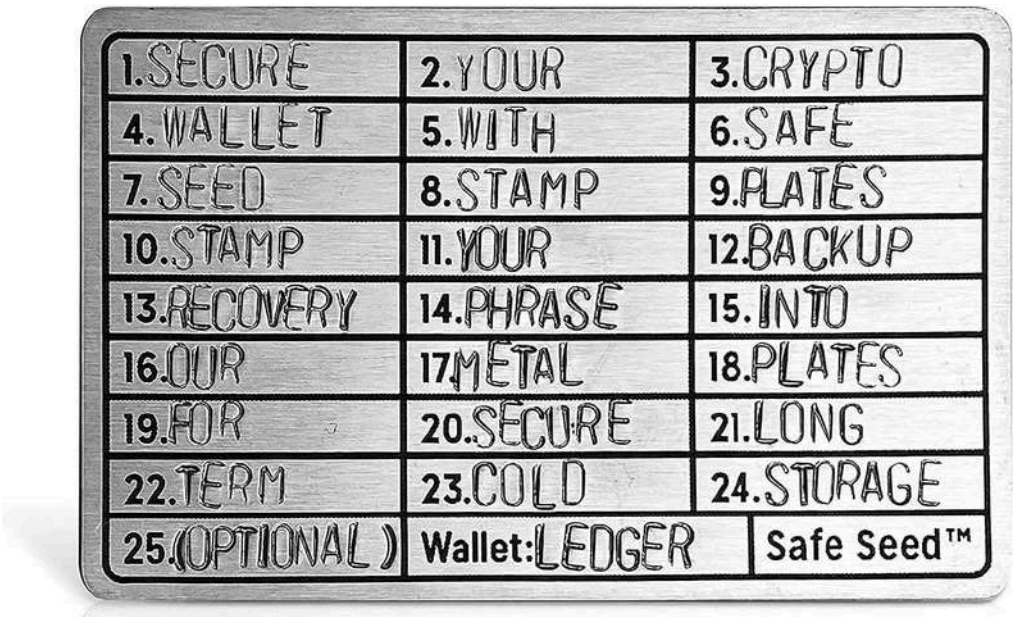
[redacted]

Um método fácil e seguro para criar uma placa de metal com a chave-mestra é usar um conjunto de punções de letras — pegue um kit de punções de metal e um martelo, e então grave as palavras em uma placa de aço inoxidável. Da mesma forma, um marcador de centro (punção automático) oferece um excelente resultado para quem usa os equivalentes numéricos do BIP39. É durável, resistente a fogo e água, e funciona sem equipamentos sofisticados.

Ao contrário das carteiras físicas (*hardware wallets*), as placas de metal podem ser adquiridas em marketplaces online, pois não há risco de adulteração — contanto que você, e somente você, seja responsável por inserir manualmente as palavras ou fazer os furos. Em resumo, nada de impressoras ou métodos digitais, incluindo imagens, mesmo offline.

WICKED SMART BITCOIN: Demonstração de Backup em Metal

CRYPTO GUIDE: OneKey KeyTag (TinySeed)



QUAIS SÃO AS MAIORES AMEAÇAS?

Todo caso de perda de Bitcoin — seja por hacks, roubo ou perda acidental — decorre de erro humano. As falhas mais comuns incluem não garantir um backup físico durável da chave-mestra, confiar em dispositivos ou softwares inseguros e cair em golpes de engenharia social. Até mesmo exchanges, que deveriam ter segurança robusta, frequentemente sofrem violações devido a falhas de design evitáveis. Para mitigar esses riscos, siga quatro princípios fundamentais:

- ☐ **Nunca compartilhe suas chaves privadas ou senhas — evite inseri-las em sites, aplicativos ou compartilhar códigos QR gerados pela carteira.**
- ☐ **Verifique a integridade do software — confira assinaturas digitais e hashes antes da instalação.**
- ☐ **Cuidado com ataques de phishing — nunca clique em links de e-mails, anúncios ou mensagens de redes sociais.**
- ☐ **Evite golpes — nunca envie Bitcoin para estranhos, promoções falsas ou alertas urgentes.**

RECOMENDAÇÃO

[redacted]

Fronteiras Energéticas: Mineração de Bitcoin, IA e o Futuro da Energia | AIM Summit Dubai 2024

Moderador: John D'Agostino - Head de estratégia, Coinbase institutional

https://www.youtube.com/watch?v=ZbKey5-hku8

SOBRE NÓS

A Santacroce Tech é especializada em consultoria conduzida por especialistas e soluções de software personalizadas em Bitcoin, inteligência artificial, LLMs privados, arquitetura de software e contratos inteligentes Web3. Com profunda expertise técnica, construímos soluções seguras e escaláveis em blockchain e IA.

Estamos ativamente envolvidos no desenvolvimento de código aberto de Bitcoin, contribuindo para projetos como Stratum V2 e Drivechain. Nossa equipe possui décadas de experiência e fortes conexões na indústria.

Nosso trabalho inclui iniciativas como o Bitcoin Center NY, a primeira stablecoin do Brasil, BRZ, e a Alkimiya, que foca na tokenização de fluxos financeiros na mineração de criptomoedas. Essas experiências nos tornam um parceiro estratégico, pronto para aconselhar equipes executivas em decisões tecnológicas cruciais.

CONTATO

Conte com a Santacroce Tech para mantê-lo informado sobre ativos digitais, inteligência artificial e a indústria Web3. Inscreva-se agora para receber insights de especialistas que importam. Para consultas comerciais ou perguntas gerais, entre em contato conosco em info@santacroce.xyz

=-=-=-=-=-= bloco 886,490 =-=-=-=-=-=