Programando Soberania

Criptografia e o Protocolo Bitcoin

Felipe Selva

Desvendando o Bitcoin

Seu Guia Essencial para a Soberania Digital

Bem-vindo ao universo do Bitcoin, uma tecnologia que está redefinindo o conceito de dinheiro e finanças. Este guia foi criado para ser sua porta de entrada, explicando de maneira simples e direta os pilares do Bitcoin e as ferramentas que podem fortalecer sua privacidade e segurança nesta jornada.

01

O coração do Bitcoin

A BlockChain

O Livro-Caixa Incorruptível

Imagine um livro-caixa digital, compartilhado por milhares de computadores ao redor do mundo. Cada transação é registrada em uma página, chamada de "bloco". Uma vez que um bloco é preenchido e adicionado à corrente (daí o nome "blockchain"), ele não pode mais ser alterado. Essa é a essência da blockchain do Bitcoin.

- **Descentralização:** Não existe um banco central ou uma única empresa controlando a blockchain. Ela é mantida por uma rede de participantes voluntários, o que a torna resistente à censura e ao controle de qualquer entidade.
- **Transparência e Pseudonimato:** Todas as transações são públicas e podem ser verificadas por qualquer pessoa. No entanto, as transações são ligadas a "endereços" de Bitcoin, que são sequências de letras e números, e não diretamente à sua identidade real.

02

Ferramentas auxiliares para as sua privacidade e segurança

TOR e VPN:

Seus Guardiões na Internet

Sua atividade na internet pode revelar muito sobre você, incluindo seu interesse em Bitcoin. Seu Provedor de Internet (ISP) sabe quais sites você visita. Ferramentas como o TOR e as VPNs são essenciais para ofuscar sua pegada digital.

- **VPN (Virtual Private Network):** Uma VPN cria um "túnel" criptografado entre seu dispositivo e um servidor da empresa de VPN. Todo o seu tráfego passa por esse túnel.
    - **Ideal para:** Uso diário, proteção em redes Wi-Fi públicas (aeroportos, cafés) e para mascarar sua localização geográfica. Por exemplo, ao comprar Bitcoin em uma exchange, usar uma VPN impede que seu provedor de internet saiba que você está se conectando àquela corretora específica.
- **TOR (The Onion Router):** O TOR oferece um nível de anonimato ainda maior. Ele direciona seu tráfego através de uma série de três servidores voluntários ao redor do mundo, criptografando os dados em camadas (como uma cebola). Cada servidor só conhece o passo anterior e o próximo, mas nenhum conhece o caminho completo.
    - **Ideal para:** Situações que exigem máxima privacidade, como transmitir suas transações de Bitcoin sem revelar seu endereço de IP de origem. Ao usar uma carteira de Bitcoin conectada através da rede TOR, você dificulta enormemente que alguém associe suas transações à sua localização real.

03

Seu próprio node

A Soberania Financeira

Seja Seu Próprio Banco

Quando você usa uma carteira de Bitcoin em seu celular ou computador, geralmente confia nos servidores ("nós") de uma empresa para lhe dizer seu saldo e para transmitir suas transações para o resto da rede. Isso é conveniente, mas abre mão da privacidade, pois a empresa pode registrar seus endereços e seu histórico de transações. Rodar seu próprio nó completo do Bitcoin elimina essa dependência.

- **Por que isso importa?**
    1. **Privacidade Absoluta:** Ao conectar sua carteira ao seu nó, suas consultas de saldo e transações não são enviadas para servidores de terceiros. Você consulta sua própria cópia da blockchain. Ninguém além de você sabe quais endereços lhe pertencem.
    2. **Segurança Máxima:** Você não confia em ninguém para validar as transações. Seu nó verifica de forma independente se cada transação recebida segue as regras do Bitcoin. Você se protege contra transações falsas e garante que as regras do sistema (como o limite de 21 milhões de moedas) estão sendo cumpridas.
    3. **Fortalecimento da Rede:** Cada nó completo é um pilar que sustenta a descentralização do Bitcoin, tornando a rede mais resiliente e robusta contra ataques.

Rodar um nó hoje é mais fácil do que nunca, com soluções "plug-and-play" que usam computadores de baixo custo como o Raspberry Pi, permitindo que você tenha seu próprio "banco" rodando 24/7 em sua casa.

04

Tails

O Sistema Operacional

Um Santuário para Suas Criptomoedas

Para situações que exigem o mais alto grau de segurança, como criar uma carteira "fria" (cold storage) ou assinar uma transação importante, o Tails é a ferramenta definitiva. Trata-se de um sistema operacional completo que pode ser iniciado a partir de um simples pen drive.

- **Como Funciona?** Você insere o pen drive com Tails em um computador e o inicia a partir dele. O sistema operacional roda inteiramente na memória RAM, sem tocar no disco rígido do computador.
    - **Amnésia Digital:** Por não gravar nada no disco rígido, ele é "amnésico". Assim que você desliga o computador, toda a sua atividade, incluindo senhas digitadas, arquivos abertos e sites visitados, desaparece sem deixar rastros. Isso o torna imune a malwares ou spywares que possam estar instalados no sistema operacional principal do computador.
    - **Segurança em Camadas:** O Tails força toda a sua conexão à internet a passar pela rede TOR, garantindo anonimato. Ele já vem com uma carteira Electrum (uma popular carteira de Bitcoin) e outras ferramentas de criptografia, criando um ambiente hermeticamente fechado e seguro.

Caso de Uso: Você pode usar o Tails para gerar uma nova carteira de Bitcoin offline. As chaves privadas nunca tocarão em um computador conectado à internet, oferecendo o padrão-ouro de segurança para guardar seus fundos a longo prazo.