

## Tipos de endereços Bitcoin



Bitcoin pode ser considerado selvagem se não houver entendimento. Muito se fala nos últimos dias sobre o risco de ter seus Bitcoins dentro de corretoras. E na hora de mover para uma carteira começa a aparecer uma sopa de letrinhas e com isto o medo de perder seus investimentos.

Então vamos lá destrinçar os tipos de endereços:

## Endereços Legados (Pay-to-Pubkey Hash)

Quando o Bitcoin foi lançado havia uma carteira que foi feita para atender as necessidade que eram importantes na época que vamos chamar de “Endereço Legado”, mas não se assuste estes endereços não deixaram de funcionar, algumas plataformas (carteiras ou exchanges) possuem compatibilidade com este endereço.

A identificação desse tipo de endereço pode ser reconhecida pelo início da sua carteira com o número “1”.

Esse endereço não suporta a atualização SegWit e não pode se comunicar com os endereços mais modernos (transações serão rejeitadas). Este tipo de endereço possui transações que tendem a ser mais caras.

E sobre a atualização SegWit vamos falar melhor sobre ela no tipo de endereço abaixo.

## Endereços Segwit (BECH 32)

O Bitcoin passou por várias atualizações elas estão documentadas publicamente no repositório <https://github.com/bitcoin/bips>. A BIP 141 define uma nova estrutura de “testemunha” que é responsável por validar os blocos separadamente. Essa estrutura contém dados necessários para verificar a validade da transação. Isso melhorou a capacidade máxima do bloco, deu compatibilidade a soluções como a Light Network.

Este tipo de endereço pode ser identificado pelo início “bc1”.

## Endereços P2SH

Esse tipo de endereço permite mais funcionalidade comparado aos endereços legados, como por exemplo carteiras multi assinadas, onde mais de uma chave privada é necessárias para mover os fundos. Ela também consegue fazer uma ligação entre os endereço Legados e Segwit, muito utilizados por corretoras e entidades financeiras

Você pode identificar esse endereço pelo seu início com o número “3”.

## Atualização Taproot (Segwit v1)

Essa atualização trouxe muitas melhorias dentre elas a “Assinaturas Schnorr”. Traduzindo, esta atualização uma maior privacidade para os usuários (Tem a prerrogativa dos contratos inteligentes na rede BTC... Mas isso é papo para outro artigo)

Muito parecido com o formato Segwit, os endereços do tipo Taproot também começam com “bc1”

Nada aqui é uma recomendação de investimento, não importa o qual louco eu esteja.