

Carteiras criptográficas



PUC Minas

Aplicações Descentralizadas e Blockchain

Prof. Carlos Leonardo dos S. Mendes

O que são carteiras criptográficas

- ▶ Uma **carteira criptográfica** (ou *crypto wallet*) é uma ferramenta para transacionar ativos utilizando a tecnologia de criptografia.
- ▶ Nas plataformas de blockchain, elas são usadas para interagir com as redes e são **necessárias para enviar e receber criptomoedas** (ou tokens).
- ▶ As **wallets** também são usadas para gerar **novos endereços de blockchain**. Esses **endereços representam as partes** em uma transação de blockchain, como por exemplo o envio de criptomoeda para pagamento de um produto ou serviço.
- ▶ Existem *wallets* que são usadas com **outras tecnologias de e-commerce**.
 - ❖ Exemplos: PayPal, PagSeguro, MercadoPago, Google Wallet, etc.

O que são carteiras criptográficas

- ▶ As **wallets** de blockchain **não armazenam os ativos**.
- ▶ Os ativos (criptomoedas ou tokens) são parte de um sistema de blockchain (dados na rede) e as **wallets** servem como **meio para acessá-los**.
- ▶ Ao serem criadas, as **wallets** de blockchain geram um ou mais pares de **chaves criptográficas assimétricas** (chave pública e privada).
- ▶ As **chaves públicas** são usadas para gerar **endereços na blockchain**. Os endereços são necessários, por exemplo, para receber pagamentos.
- ▶ As **chaves privadas** são usadas para **criar assinaturas digitais** nas transações e **não devem jamais ser compartilhadas**.

Tipos de carteiras criptográficas

Tipos de carteiras criptográficas

► Software wallets

- **Web wallet:** são carteiras que usam uma **interface web** para manuseio. Geralmente as chaves privadas são armazenadas em servidores de terceiros.
- **Desktop wallet:** são carteiras cujo software é baixado e **executado localmente**. São mais seguras porque as chaves privadas são armazenadas localmente e gerenciadas pelo detentor.
- **Mobile wallet:** semelhante às *desktop wallets*, mas desenvolvidas para **dispositivos móveis** (smartphones). Geralmente usam QR codes para enviar e receber transações.
- Exemplos de *software wallets*:
 - ❖ Metamask, MyEtherWallet (MEW), Parity, Jaxx

Tipos de carteiras criptográficas

- ▶ **Hardware wallets.** São dispositivos físicos desenvolvidos especificamente para gerar e armazenar as chaves sem qualquer conexão com a Internet.
- ▶ Embora tenham acessibilidade e integração mais restrita, são consideradas uma das alternativas mais seguras para geração, armazenamento e gerenciamento de chaves.
- ▶ Exemplos de *hardware wallets*:
 - ❖ Ledger Nano S, Trezor One, Safepal S1



Tipos de carteiras criptográficas

- ▶ **Paper wallets.** Consiste de um pedaço de papel com um endereço blockchain e a chave privada correspondente.
- ▶ As chaves são geralmente impressas no formato alfa-numérico (uma longa cadeia de caracteres) junto com um *QR code* para ser escaneado e executar transações.





PUC Minas