

Bitcoin

Ivan Sendin

Exercício

Aulas passadas

Blockchain

Endereços

Transações

Pizza

Transações e Endereços

Ivan Sendin

FACOM - Universidade Federal de Uberlândia
ivansendin@yahoo.com, sendin@ufu.br

7 de agosto de 2024

Exercicios Avaliativos

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Teste de Mineração Egoista
- “Em processo de correção”
- Testes Multiplos
P-Hacking

Aulas Passadas

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Mineração e Consenso Distribuído
- Merkle Tree

Bitcoin

Ivan Sendin

Exercício

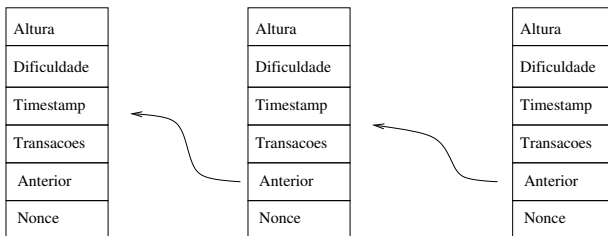
Aulas passadas

Blockchain

Endereços

Transações

Pizza



Endereços

Bitcoin

Ivan Sendin

Exercício

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Os usuários do Bitcoin são endereços
- Chave Pública
- A SK correspondente assina autorizando a gastar o dinheiro
- Codificado em Base58

Endereços

Bitcoin

Ivan Sendin

Exercício

Aulas passadas

Blockchain

Endereços

Transações

Pizza

```
from bitcoinlib.wallets import Wallet
from bitcoinlib.mnemonic import Mnemonic

passphrase = Mnemonic().generate()
print("A sua passphrase é:", passphrase)
#A sua passphrase é: glimpse flavor enroll peanut enough
under final reason squirrel twenty sport slender
w = Wallet.create('SBSEG2024', keys=passphrase, network='bitcoin')

print(w.get_key().address)
#12yPhuv7yJCfepq7kZQm5ej93Fes5do64n

print(w.get_key().wif)
# xprvA3n4M5SJLFo41eHbv6mMud26vNRKewz6jVFizSHiyKoHySciXABJhBYceudbk1K
# imGnLw7YcRwG8qLx3BW6tbbmtjXmMLTwAT8wpM819pH9
```

Prefixo	Tipo	Descrição
1	Pay-to-Public-Key-Hash (P2PKH)	Utiliza assinaturas digitais para validar as transações
3	Pay-to-Script-Hash (P2SH)	O resultado da execução do script valida ou não uma transação
bc1	Segregated Witness (SegWit)	Modifica a forma como os dados são armazenados na blockchain.
bc1p	Taproot (P2TR)	Utiliza assinaturas de Schnorr amplia o uso smart contract no Bitcoin

Tabela: Tipos de endereços Bitcoin

Paper Wallets

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- `walletgenerator.net`
- `bitaddress.org`
- Vários endereços, outras moedas, QR Code,...

Bitcoin

Ivan Sendin

Exercicio

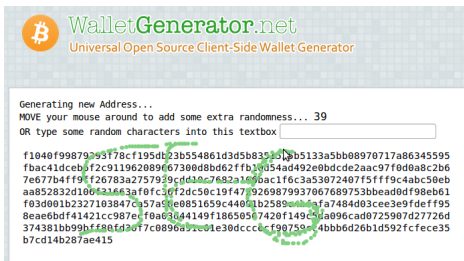
Aulas passadas

Blockchain

Endereços

Transações

Pizza



The screenshot shows the WalletGenerator.net website. At the top, there is a Bitcoin logo and the text "WalletGenerator.net" in green, followed by "Universal Open Source Client-Side Wallet Generator" in orange. Below this, a message says "Generating new Address..." and "MOVE your mouse around to add some extra randomness... 39". A text input field is present with the prompt "OR type some random characters into this textbox". Below the input field, a long Bitcoin address is displayed: f1040f99879253f78cf195d23b554861d3d5b8351b3b5133a5bb08970717a86345595fbac41dceb5f2c911962089067300d8bd62ffb10054ad492e0bdcde2aac97f0d0a8c2b67e677b4ff9cf26783a2757939cdd10c7682a1656ac1f6c3a53072407f5fff9c4abc50ebaa852832d100f21663af0fc30f2dc50c19f47f9269879937067689753bbeat0df98eb61f03d001b2327103847ca57a50e0851659c44001b2589c1b5afa7484d03cee3e9fdeff958eae6bdf41421cc987ecf0a03044149f18650507420f149c0a096cad0725907d27726d374381bb99bfff0fd20f7c0896a3ec01e30dccc0cf90759c4bbb6d26bd592fcefce35b7cd14b287ae415. A green dashed circle highlights the address.

Bitcoin

WalletGenerator.net

Universal Open Source Client-Side Wallet Generator

Generating new Address...

MOVE your mouse around to add some extra randomness... 39

OR type some random characters into this textbox

f1040f99879253f78cf195d23b554861d3d5b8351b3b5133a5bb08970717a86345595fbac41dceb5f2c911962089067300d8bd62ffb10054ad492e0bdcde2aac97f0d0a8c2b67e677b4ff9cf26783a2757939cdd10c7682a1656ac1f6c3a53072407f5fff9c4abc50ebaa852832d100f21663af0fc30f2dc50c19f47f9269879937067689753bbeat0df98eb61f03d001b2327103847ca57a50e0851659c44001b2589c1b5afa7484d03cee3e9fdeff958eae6bdf41421cc987ecf0a03044149f18650507420f149c0a096cad0725907d27726d374381bb99bfff0fd20f7c0896a3ec01e30dccc0cf90759c4bbb6d26bd592fcefce35b7cd14b287ae415

Paper Wallets - O caso walletgenerator

Bitcoin

Ivan Sendin

Exercício

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Código do site era diferente do código do github
- Usava o conteúdo de URLs com fonte de entropia
- <https://medium.com/mycrypto/disclosure-key-generation-vulnerability-found-in-wallet-generator>

Vanity Address

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- 1NiNja1bUmhSoTXozBRBEtR8LeF9TGbZBN
- 1DETACHABLEDD7hgExqScWngMrxDGtXwcX
- Como??

Clipboard Malware

Bitcoin

Ivan Sendin

Exercício

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Um endereço BTC é uma string bem estruturada
- É fácil detectar um endereço em uma string
- Malware "de prateleira"
- Monitora a área de clipboard
- ao detectar um endereço bitcoin, troca por um outro endereço
- Ao fazer uma compra, o site mostra um endereço, copy-paste para o programa da sua carteira e já era!

Transações

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Lista de Entrada
- Lista de Saída

Transações

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Entrada
- Referência a saída não gasta de um outra transação
- *Unspent Transaction Output* UTxO

Transações

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Pagando 22 BTCs para xyz

Bitcoin

Ivan Sendin

Exercicio

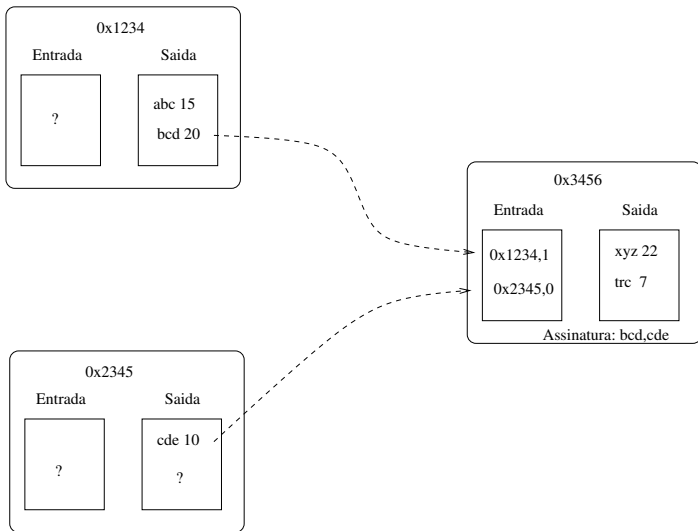
Aulas passadas

Blockchain

Endereços

Transações

Pizza



Transações

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Não tem endereço na entrada
- Endereço de troco
Não precisa ser novo...mas é bom
- Taxa
- “Sem” saldo

Transações

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Coinbase
- Primeira transação de cada bloco
- SEM ENTRADA!!

Pizza

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- primeira compra feita com Bitcoin

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

Utilizando a API do blockchain.info desenvolva um script para:

Bitcoin

Ivan Sendin

Exercicio

Aulas passadas

Blockchain

Endereços

Transações

Pizza

- Pegar o último bloco da blockchain
- Encontrar a transação de Coinbase
- Lista os endereços que estão recebendo os Bitcoins