MÓDULO 3

CRIPTOATIVOS NA PRÁTICA

por Alexandre Senra

I OPERANDO EM EXCHANGES

(1) Saindo do sistema bancário: transferência em reais (BRL), de um Banco Comercial para uma Exchange Nacional.

- Segurança do login na Exchange Nacional (MFA, 2FA) ≠ chaves privadas.
- Política de anti-money laundering (AML): Know your client (KYC).

(2) Na Exchange Nacional: troca de BRL por bitcoins (BTC). E envio de BTC para uma Exchange Estrangeira.

- Livro de ofertas:

a) ordens de compra, de venda e spread;

b) espessura do livro de ofertas;

c) ordem a mercado e ordem limite.

(3) Na Exchange Estrangeira: possibilidade de troca dos BTC por muitos outros ativos, inclusive por stablecoins, como o theter do dólar americano (USDT).

- Segurança do login (MFA, 2FA).
- KYC → vale mesmo a pena como política AML?

Algumas notícias:

https://webitcoin.com.br/hacker-prova-que-roubou-dados-de-procedimentos-kyc-de-exchanges-jan-24/

https://cointelegraph.com.br/news/crypto-exchange-digitex-removes-kyc-to-protect-user-data

https://saude.estadao.com.br/noticias/geral,nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes,70003536340

- Maior variedade de ativos disponíveis.
- Book mais espesso.
- Falta de padronização: KYC a depender do País onde sediada a exchange. Além da existência de exchanges descentralizadas (https://idex.io/).
- Muita atenção ao remeter criptoativos para qualquer outro endereço público. Errar a espécie de criptoativo ou um dígito sequer resultará na perda do saldo.

II CRIANDO UMA CARTEIRA DE PAPEL

(1) O jeito errado de se fazer.

- Dispensar a aleatoriedade.
- Gerá-la online.
- Gerá-la offline e depois reconectar o computador.
- Gerá-la a partir de sites “suspeitos”.

Exemplos de sites onde se pode gerá-la:

- https://walletgenerator.net/;
- https://www.bitaddress.org/.

Não recomendamos **nenhum** site para a geração de carteiras de papel.

III LIDANDO COM OUTRAS CARTEIRAS (HARDWARE WALLET, DESKTOP WALLET, MOBILE WALLET E WEB WALLET)

https://bitcoin.org/en/choose-your-wallet?step=1

- A Fundação Bitcoin.org não recomenda nenhum site para a geração de carteiras de papel nem que se faça uso de web wallets;
- Não confundir senha e seed words com chave privada, chave pública e endereço público. Senha e seed words são próprios das aplicações (carteiras que criptografam as chaves privadas). Chave privada, chave pública e endereço público são próprios da blockchain.

A parábola...

- Chave privada → chave da porta da sua casa.
- Chave pública → endereço da sua casa.
- Endereço público → endereço para receber encomendas.

Características da chave privada: você pode mudar a plástico que vem em cima dela, mas ela é insubstituível, necessária para entrar na sua casa, e vem com o endereço da sua casa escrito nela.

É muito perigoso eu ficar com essa chave da porta por aí. Não quero ficar com essa chave e não quero que ninguém tenha acesso a ela. Recorro a uma pessoa que instala fechaduras eletrônicas. Mas ela me faz uma advertência muito importante: ela não guarda a senha das fechaduras que instala. Você terá a senha para entrar na sua casa e uma senha de reinicialização, caso a fechadura dê qualquer problema. Se você perder as 02, nunca mais entra na sua casa.

Pronto. Agora eu tenho acesso à minha casa digitando a senha na fechadura eletrônica. E se quebra essa fechadura ou eu me esquecer da senha? Tenho a senha de reinicialização. E se eu me esquecer das 02? Já era.

- Chave privada → chave pública → endereço público.
- À exceção da paper wallet, as demais aplicações armazenam chaves privadas de maneira criptografada. Elas não aparecem ao usuário, que, em vez disso, tem acesso aos fundos da carteira de 02 formas diversas: senha (+ arquivo wallet.dat, armazenado na aplicação) ou seed words (= palavras sementes; = sementes).

IV EXAMINANDO A BLOCKCHAIN DO BTC

(1) Bloco: dados disponíveis.

(2) Endereço público: dados disponíveis.

- Entradas (inputs) e saídas (outputs). Divisibilidade e agrupabilidade do bitcoin.

Mais de uma saída. Ex.1: taxa da exchange. **Ex.2:** nota alta e troco (endereço de troco).

Mais de uma entrada. Ex.: notas pequenas em diversos compartimentos da carteira.

Cuidado com a ambiguidade do termo "carteira". Pode designar tanto o par de chaves ("paper wallet") quanto a aplicação utilizada para armazenar ou transacionar bitcoins onde as chaves permanecem criptografadas (demais carteiras).

- Histórico do saldo? Dá pra calcular.

(3) Transaction Identification (txid; = hash da transação): dados disponíveis.

V UMA OUTRA CLASSIFICAÇÃO NECESSÁRIA DOS CRIPTOATIVOS

Token = gênero (def.): símbolo.

(1) Cointoken: símbolo = uma pretensa moeda.

(2) Utility token: símbolo é representativo de uma utilidade.

(3) Security tokens: símbolo é representativo da fração de um valor mobiliário.

(4) Non-security tokens: símbolo é representativo da fração de um ativo real (que não seja um valor mobiliário).

- Vascotoken (Lei 6.385/76, art. 2º; Ofício nº 15/2020/CVM/SER, de 02/10/2020).
- CHZ → utility tokens → vote! https://www.socios.com/ **Obs.:** Chiliz é uma moeda com aplicação específica.