MÓDULO 2

BITCOIN, BLOCKCHAIN E OUTROS CRIPTOATIVOS

por Alexandre Senra

I O QUE É O BITCOIN?

Def. (inicial): É um sistema de pagamento global e descentralizado.

- **Hardware.**

É uma rede de computadores distribuída (P2P), sem uma autoridade central.

- **Software.**

  É um software de que fazem parte:

  - um gerador de chaves aleatórias;
  - livro-razão público e distribuído (= blockchain; = ledger público).

- **Criptomoeda.**

  É um criptoativo, que surge como pagamento do software para o hardware e assume a função de moeda dentro de um sistema de pagamento.

II CARCTERÍSTICAS DO BITCOIN

- **Hardware:**
  - Descentralizado.
  - Validadores + mineradores (ASIC).

- **Blockchain:**
  - Distribuído.
  - Público.
  - Pseudônimo.

- 0% confiança e 100% verificabilidade (a solução do problema do gasto duplo).
- Consensualidade (e o ataque da maioria).
- Assimetria entre os custos de se resolver a prova de trabalho (**PoW**) e de verificabilidade.
- Sepultamento progressivo (= consenso exponencialmente consolidado).
- Transações on-chain e off-chain (ex. exchanges).

- **BTC:**
  - Escassez.
  - Inflexibilidade da oferta.
  - Volatilidade.
  - Divisibilidade/agrupabilidade.
  - Transportabilidade.
  - (Não) deteriorabilidade.

III MINERAÇÃO DE BTC

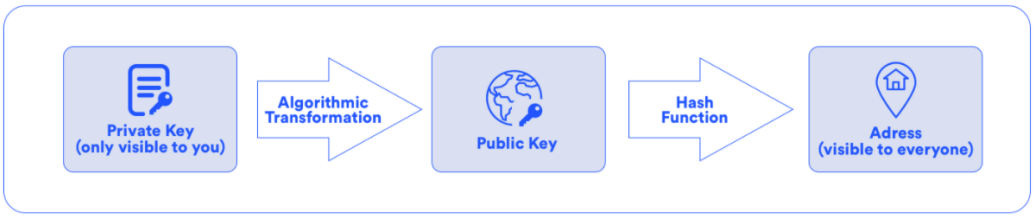
- Recompensa e halving.

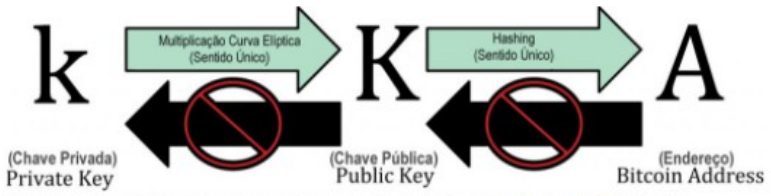
- Taxa de transação da rede (≠ taxa de transação de exchanges).

  Obs.: Depende do tamanho da transação em bytes e não do valor transferido.

  (https://www.blockchain.com/btc/tx/d486aeb0e59181fd1addb4aa69ce04d638188fc1125c424899267e8ed6a8af24)

IV CHAVE PRIVADA, CHAVE PÚBLICA E ENDEREÇO BITCOIN





Gerando uma Chave Pública e um endereço a partir de uma chave privada. Fonte: Mastering Bitcoin (adaptado)

- **Composições.**
  - **A chave privada.**

    Um número aleatório de 78 dígitos. Ou uma sequência alfanumérica de 51 caracteres. Ex.:

    - 22253723355774722335514752419334321201576740247621632658033392892734079982402;
    - 5JjwSXrkyidrvgvuJumSq8wdkW7hrbYzp9iN9zh6zbCKrhFEh5D (mesma chave, com outra codificação; WIFA).
  - **A chave pública.**
    - Mesmo formato da chave privada. Compõe um par.
  - **O endereço público.**
    - Sequência alfanumérica de 34 caracteres (podendo, excepcionalmente, ter 26).

- **Funções criptográficas unidirecionais** (= praticamente irreversíveis).

- **Unicidade do par de chaves** (= praticamente impossível gerar 2x a mesma chave).

  - Praticamente quanto?
    - A chance de se gerar o mesmo par de chaves é de 1 em 10^{77}.
    - 10^{23} = número de grãos de areia na Terra.

V ARMAZENANDO BITCOINS (TIPOS DE CARTEIRA)

- **De acordo com a plataforma:**
  - Desktop wallet.
  - Mobile wallet.
  - Web wallet.
  - Hardware wallet.
  - Paper wallet.

- De acordo com o grau de autonomia e à forma como interagem com a rede:
  - Fullnode client.
  - Lightweight client.

VI NEGOCIANDO BITCOINS

- Exchanges nacionais.
  - https://bitvalor.com/

- Exchanges estrangeiras.
  - https://coinmarketcap.com/pt-br/rankings/exchanges/

- P2P.
  - https://catalogop2p.com/

VII ASPECTOS LEGAIS DO BITCOIN

- **RFB** (https://receita.economia.gov.br/publicacoes/ebooks/paginas/perguntao-irpf2020)
    - São um ativo financeiro, declarável na aba “outros bens”.

MOEDA VIRTUAL - COMO DECLARAR

445 — As moedas virtuais devem ser declaradas?

Sim. As moedas virtuais (bitcoins, por exemplo), muito embora não sejam consideradas como moeda nos termos do marco regulatório atual, devem ser declaradas na Ficha Bens e Direitos como “outros bens”, uma vez que podem ser equiparadas a um ativo financeiro. Elas devem ser declaradas pelo valor de aquisição.

Atenção:

Como esse tipo de “moeda” não possui cotação oficial, uma vez que não há um órgão responsável pelo controle de sua emissão, não há uma regra legal de conversão dos valores para fins tributários. Entretanto, o contribuinte deverá guardar documentação que comprove a autenticidade desses valores.

    - Alienações são tributadas a título de ganho de capital.

ALIENAÇÃO DE MOEDAS VIRTUAIS

606 — Os ganhos obtidos com a alienação de moedas “virtuais” são tributados?

Os ganhos obtidos com a alienação de moedas virtuais (bitcoins, por exemplo) cujo total alienado no mês seja superior a R$ 35.000,00 são tributados, a título de ganho de capital, segundo alíquotas progressivas estabelecidas em função do lucro, e o recolhimento do imposto sobre a renda deve ser feito até o último dia útil do mês seguinte ao da transação.

O contribuinte deverá guardar documentação que comprove a autenticidade das operações.

    - Movimentações e operações devem ser informadas, em conformidade com a IN RFB 1.888/2019.

- **STJ (natureza jurídica):**

> […] INVESTIGADO QUE ATUAVA COMO TRADER DE CRIPTOMOEDA (BITCOIN), OFERECENDO RENTABILIDADE FIXA AOS INVESTIDORES. […] OPERAÇÃO QUE NÃO ESTÁ REGULADA PELO ORDENAMENTO JURÍDICO PÁTRIO. **BITCOIN QUE NÃO TEM NATUREZA DE MOEDA NEM VALOR MOBILIÁRIO**. INFORMAÇÃO DO BANCO CENTRAL DO BRASIL (BCB) E DA COMISSÃO DE VALORES MOBILIÁRIOS (CVM). INVESTIGAÇÃO QUE DEVE PROSSEGUIR, POR ORA, NA JUSTIÇA ESTADUAL, PARA APURAÇÃO DE OUTROS CRIMES, INCLUSIVE DE ESTELIONATO E CONTRA A ECONOMIA POPULAR. (STJ, CC 161.123/SP, Rel. Ministro SEBASTIÃO REIS JÚNIOR, TERCEIRA SEÇÃO, julgado em 28/11/2018, DJe 05/12/2018)

VIII OUTROS CRIPTOATIVOS E BLOCKCHAINS

- **Definindo e categorizando criptoativos.**

  Criptoativos (def.): são ativos virtuais escassos, protegidos por criptografia e baseados numa rede descentralizada.

  - Gênero, de que são espécies: (1) criptomoeda; (2) criptocommodity; (3) criptotoken.
    - Criptomoeda: tem a pretensão de se tornar uma moeda (instrumento que sirva como meio troca, reserva de valor e unidade de conta) - ex.: *bitcoin*;
    - Criptocommodity: é uma commodity digital (= um insumo digital) – ex.: capacidade de armazenamento fornecida via blockchain;
    - Criptotoken: é um bem ou serviço acabado – ex.: uma rede social ou navegador que rode em blockchain.
  - Criptografia de chave pública (= criptografia assimétrica).
  - Nenhum componente é, por si só, indispensável.

- **Alguns outros criptoativos.**

Obs.: o bitcoin tem uma dominância superior a 60% no mercado de criptoativos.

- **Monero** (XMR) e as moedas de privacidade.
- **Theter** (USDT) e as stablecoins.
- **Ethereum**: o computador mundial. (https://ethereum.org/pt-br/)
  - **Hardware:** validadores e “mineradores” (PoW → PoS Etherem 2.0).

- **Software:** é a principal blockchain[1] programável do mundo, contando com uma linguagem Turing completa. Hospeda outros criptoativos (ex.: BAT, relacionado ao navegador "Brave"), roda *smart contracts* etc.
- **Criptoativo:** ether (ETH). É uma criptomoeda. E é uma criptocommodity (forma de pagamento pelo uso desse computador).

- **BAT** e o navegador que respeita a sua privacidade (Brave).
- **MBVASCO01**, o processo de tokenização e novas diferenciações.

1 Blockchain, neste contexto, já não é mais um simples livro-razão distribuído. É uma tecnologia baseada na arquitetura P2P, onde todos são clientes e servidores.