



Insper

Ativos Digitais e Blockchain

Ricardo Rocha
Raul Ikeda

Relembrando

- Blockchain: cadeia de blocos ligadas por HASH
- HASH é uma função que recebe qualquer coisa e atribui um número muito grande (usualmente 256 bits ou até $2^{256}=1,158.10^{77}$) e não é inversível
- Um bloco é válido quando o hash(previous hash+dados+**nonce**) é semelhante a um certo padrão (n zeros à esquerda)
- Achar o nonce (número inteiro) cujo o hash de saída seja válido é chamado de mineração
- Somente 1 minerador ganha o prêmio de um bloco, quem achar o nonce primeiro
- Qualquer alteração nos dados, altera drasticamente o hash e quebra a cadeia de blocos

Objetivo

- Aprofundar um pouco mais sobre Blockchain

Blockchain by Bitcoin (18/Out)

- Atualmente 401Gb
- Cada bloco tem em média 1.22Mb
- 1 Bloco a cada 10 minutos em média
- Atualmente 19 zeros à esquerda
- Remuneração por bloco:
 - 6,25 BTC via mineração
 - 14.8 BTC via transactions fees em média
- 1800 Transações por bloco em média
- Mediana de 9 minutos para confirmar uma transação

Mais detalhes: <https://www.blockchain.com/explorer>

Preço de mercado (USD)

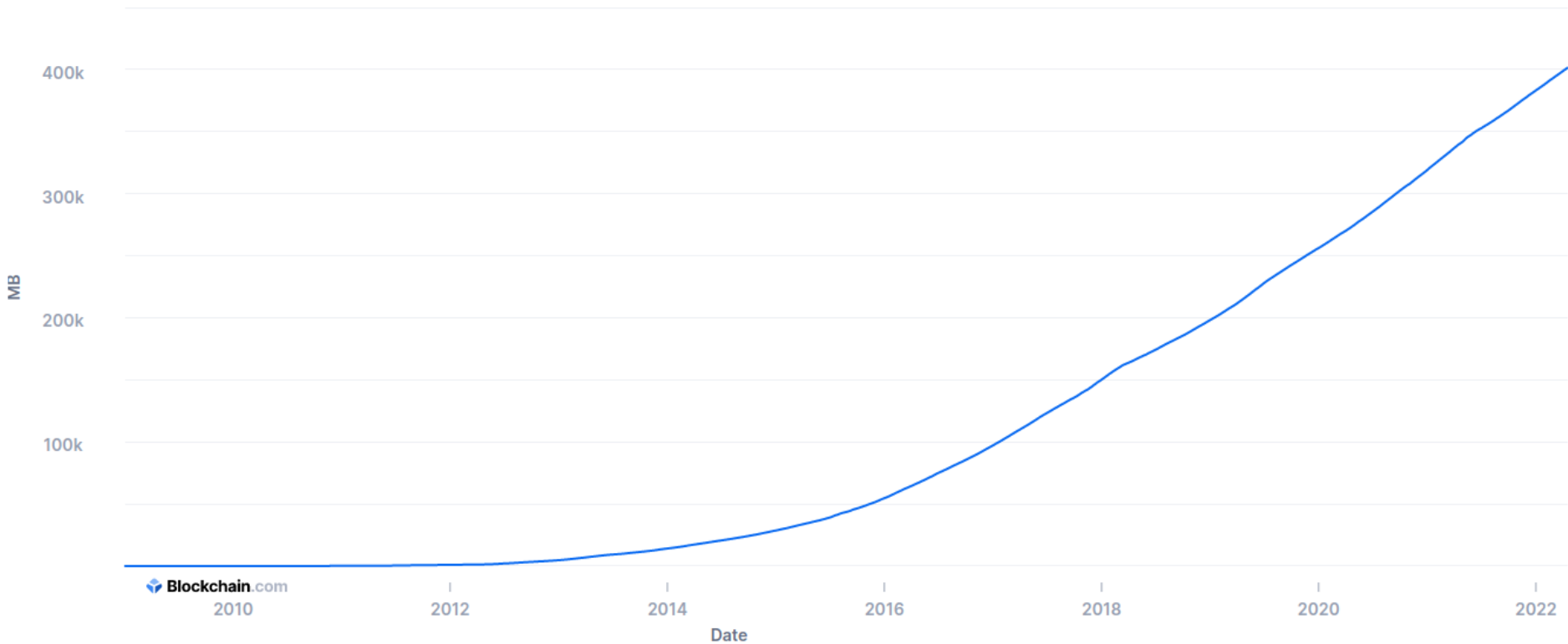
O preço médio do mercado em USD nas principais plataformas de troca de bitcoin.



Blockchain.com

Tamanho do blockchain (MB)

O tamanho total do blockchain menos os índices da base de dados em megabytes.



Dificuldade de Mineração

- Bitcoin possui um mecanismo que ajusta a dificuldade de mineração (zeros à esquerda) conforme o potencial dos mineradores
- Se há mais poder computacional, adiciona-se zeros, senão remove-se.
- O objetivo é manter uma média de 10 minutos entre blocos

Dificuldade

Dificuldade de rede

Uma medida relativa de quão difícil é minar um novo bloco para o blockchain.



Mais sobre este gráfico

Explicação

A dificuldade é uma medida de como é difícil extrair um bloco Bitcoin ou, em termos mais técnicos, encontrar um hash abaixo de um determinado alvo. Uma dificuldade elevada significa que será necessário mais poder computacional para extrair o mesmo número de blocos, tornando a rede mais segura contra ataques. O ajuste da dificuldade está diretamente relacionado com a potência de mineração total prevista estimada no gráfico Taxa de hash total (TH/s).

Notas

A dificuldade é ajustada a cada 2016 blocos (a cada 2 semanas aproximadamente) de modo a que o tempo médio entre cada bloco permaneça 10 minutos.

Metodologia

A dificuldade provém diretamente dos dados de blocos confirmados na rede Bitcoin.




Halving

- A remuneração inicial (coinbase) era de 50 BTC (< \$1 na época)
- A cada 210 mil blocos, a remuneração cai pela metade
- O primeiro halving ocorreu em 28/Nov/2012 (1 BTC = \$12)
- O segundo em 09/Jul/2016 e o terceiro em 11/Mai/2020
- O próximo é estimado em 757 dias (aprox 2 anos)
- Estima-se que em 2140 o coinbase esteja zerado. Haverá 32 cortes
- No total serão 21 milhões de bitcoins criados, hoje há 18,8 milhões já em circulação

Mais detalhes: <https://coinmarketcap.com/halving/bitcoin/>

Transactions

- Chave pública como endereço
- Chave privada para assinar a transação
- Pode transferir para mais de uma conta:

Fee	0.00033600 BTC (150.673 sat/B - 37.668 sat/WU - 223 bytes)	0.00349450 BTC	1 Confirmations
Hash	8e8979b3b85d1bba12388f555d323304b0c35ae5ce233559223353224...	2021-10-18 12:31	
	1NyWn38eFKbXLaiRv6sfzmwSfCcSmWhgXL	0.00383050 BTC 	3GcYa9jTkoqzdAF9db9Fowzt8VjPGEK7mG
			1NGmeZk1mgs7tuSkojMKKNxbaj7cgGQS
			0.00133282 BTC 
			0.00216168 BTC 

- Pode transferir de mais de uma conta:

Fee	0.00043688 BTC (59.847 sat/B - 26.802 sat/WU - 730 bytes) (107.078 sat/vByte - 408 virtual bytes)	0.04682224 BTC	1 Confirmations
Hash	a1a3b03e1fc67b6ee7f81315d0862e043baa924a73927f2f6d6d1614f9ca...	2021-10-18 12:30	
	3QLvkXsL3TTn35PxTZpUatuW7h6j3UmGEx	0.00989340 BTC 	15JxvoRTY9ppqLtdtzbSa53pR12hK27Nxeb
	3PMJrjU3H5xSnShgsZYn2PxBxN3SbFocu	0.00500000 BTC 	
	3Ft3jJKNbmA5vVs8DexRyojt8z1X4cAr27	0.02823125 BTC 	
	32DzQBn52gzhJp2uG1TrR7VFEvc6S5BiE	0.00413447 BTC 	
			0.04682224 BTC 

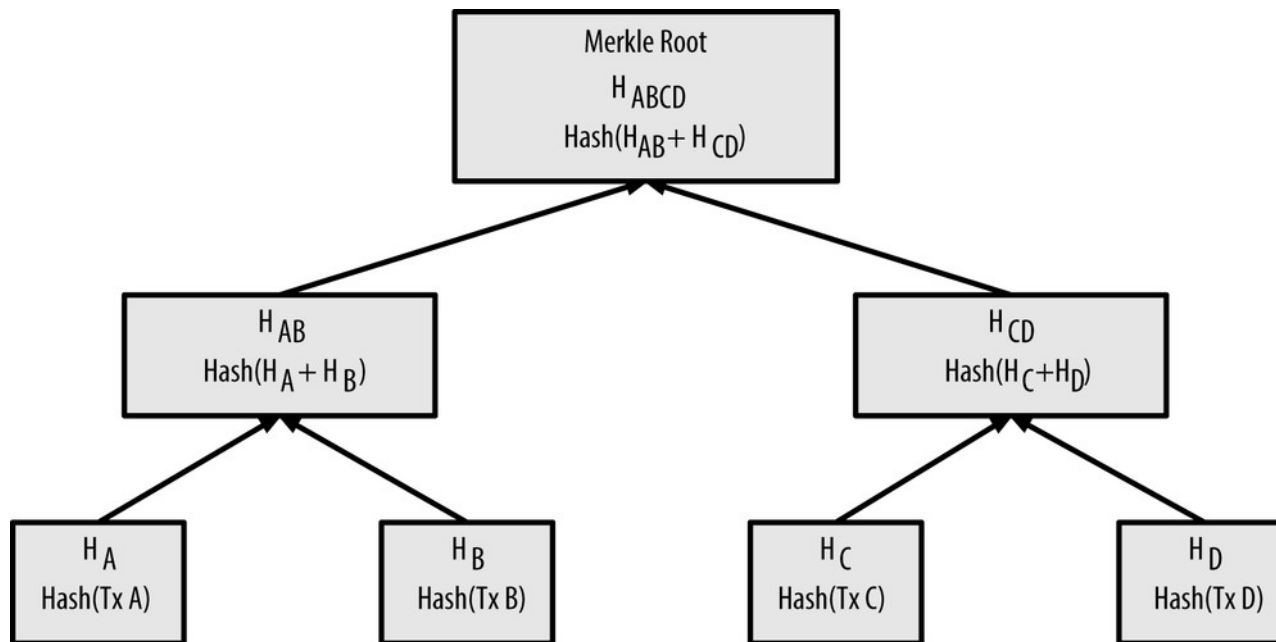
Ledger (Livro caixa)

The image shows a yellow accounting ledger form. At the top, it has a header section with 'ACCOUNTING LEDGER' on the left and 'SHEET NUMBER: _____' on the right. Below this is a table with the following columns: SN, DATE, ACCOUNT, DEBIT, CREDIT, MEMO, and BALANCE. The table has 30 rows, numbered 1 to 30 in the 'SN' column. A large yellow rectangular box with the text 'ACCOUNTING LEDGER' is overlaid on the middle of the table. The form is set against a black background.

- Disponível na [amazon.com](https://www.amazon.com)
- Se no bloco há apenas transações (e isso é desejável por causa do tamanho) como sabe-se o saldo das contas?

Merkle Tree

- Árvore binária de hashes. Estrutura:



fonte: Antonopoulos, A. M., 2014

- Vantagens:
 - Fácil de verificar se a árvore está correta.
 - Fornece uma raiz com código único.
 - Não é preciso possuir todas as transações para validar uma transação.

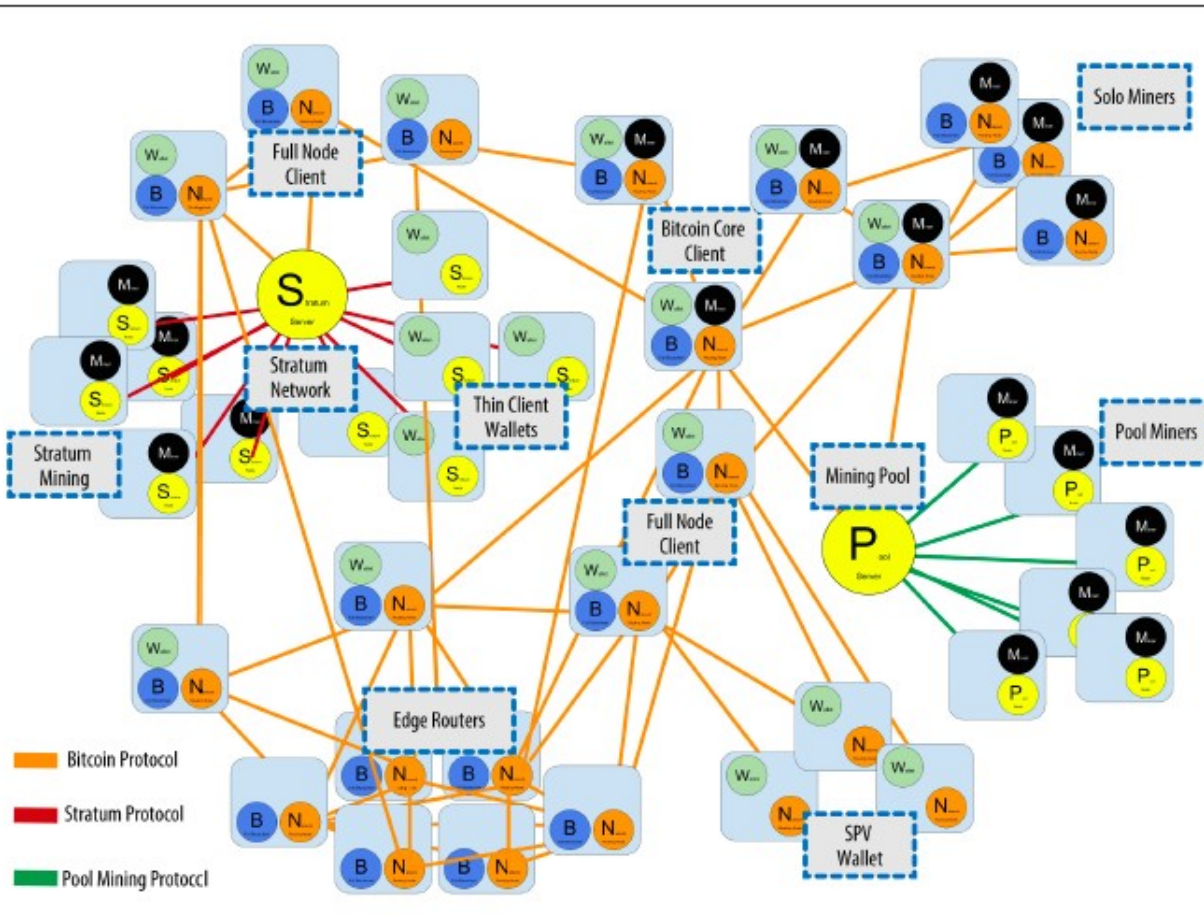
Wallets

- A base blockchain é apenas um livro-caixa.
- Todas as transações são listadas porém não estão consolidadas.
- Qualquer um que tenha uma cópia das transações consegue validar e consolidar o saldo de um endereço.
- O termo wallet é designado para representar uma carteira que contém as chaves privadas de um determinado endereço. Não contém moedas realmente.
- Pode ser implementada em hardware ou software.
- Existem empresas que administram carteiras.
- Você pode comprar e vender bitcoins diretamente na rede ou nas corretoras.

Exchanges (Corretoras)

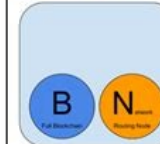
- Uma corretora permite transacionar moedas entre carteiras
- Funciona analogamente à uma bolsa de valores, mas de cryptomoedas
- Fornece preço de compra e venda (com spread, claro)
- **NÃO** necessariamente está transacionando na rede global (?!?)
- Custa em média 0.0005 BTC (R\$ 150,00) para realizar uma transação na rede principal
- Caso Mt. Gox: <https://coinsutra.com/biggest-bitcoin-hacks/>
- Outro caso: <https://gizmodo.com/crypto-exchange-says-it-cant-repay-190-million-to-clie-1832309454>
- Fresquinho: <https://livecoins.com.br/ceo-thodex-desaparece-prejuizo-2-bilhoes/amp>

Exemplo de Rede



Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



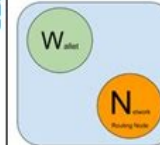
Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



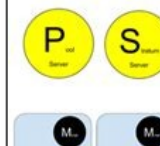
Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.



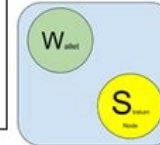
Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.



Mining Nodes

Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.



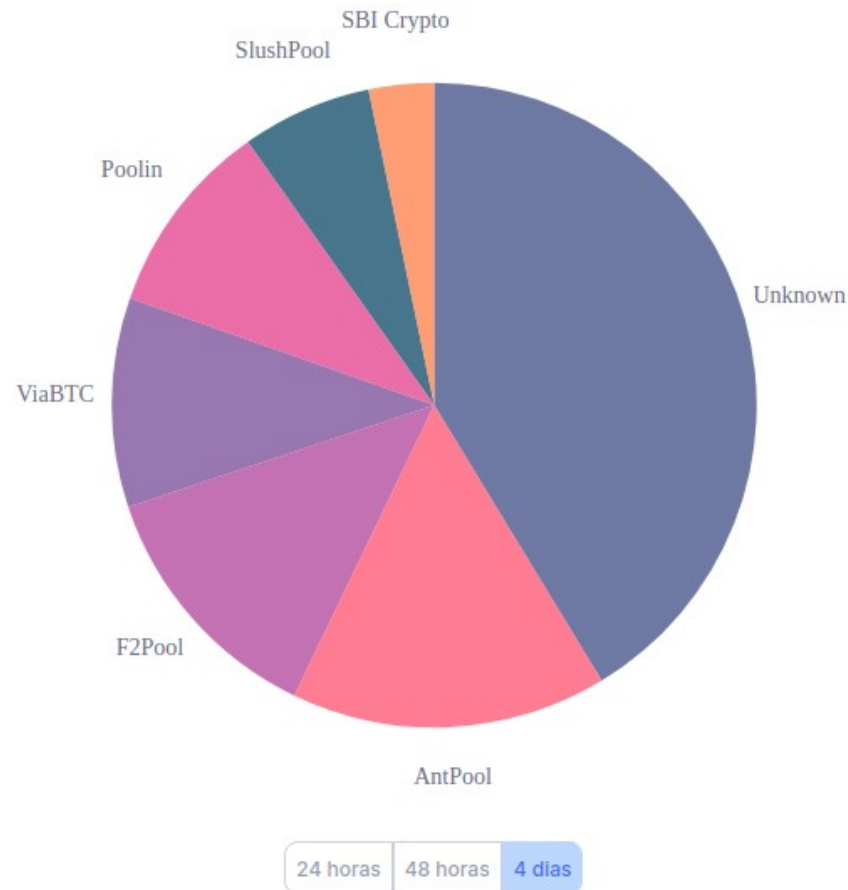
Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

Perfil dos Mineradores

Distribuição da taxa de hash

Uma estimativa da distribuição da taxa de hash entre os maiores conjuntos de mineração.



Implementação

- Bitcoin core: <https://github.com/bitcoin/bitcoin>
- Curiosidade: Bitcoin não é considerado Turing Completo

Consenso e Votação

- Para evitar fraudes, cria-se uma rede *peer-to-peer*, onde cada nó possui uma cópia do Blockchain.
- Quando um novo nó é minerado, envia-se os dados do bloco a todos os nós da rede.
- Cada nó declara se aceita ou rejeita o bloco em questão. Caso um certo número de nós aceite o bloco, ele é incorporado ao Blockchain e começa-se a minerar um novo bloco.
- Durante a análise do bloco, os nós também avaliam a validade dos dados, e no caso de transações financeiras, se haveria saldo suficiente para efetuar cada transação.
- Caso o bloco enviado seja inválido, se o minerador insistir em incorporar o bloco, ele irá divergir do resto da rede (fork).

Forking

- O que acontece se dois mineradores acharem o bloco ao mesmo tempo?
- Como em um sistema de "votação" quem obter a maioria dos nós reconhecendo o bloco, venceria o pleito. Durante a divergência, cada nó cria um fork na lista e vai empilhando. Quando o consenso é atingido, descarta-se o ramo preterido.
- No caso extremo, pode haver cisão e criar duas redes diferentes. Em alguns casos o fork é intencional (troca de configuração, divergências permanente entre nós, etc).

BTC, XBT, BCH, BCG ou BSV?

- BTC é o código usual para bitcoin core, mas de acordo com a ISO 4217, o prefixo BT é reservado ao Butão. O correto seria usar o prefixo X de commodities. É a rede com maior captação.
- BSV (Satoshi Vision) mantém-se fiel à ideia original do paper.
- BCH e BCG são hardforks do BTC que alteram detalhes técnicos (por exemplo tamanho máximo do bloco ou algoritmo PoW), que redefinem os incentivos da rede.
- Na prática não há empecilhos para a realização de um hardfork, mas qual o impacto financeiro?

Mais detalhes: <http://www.bitcoin-en.com/bitcoin-hard-forks-history.html>

Recapitulando

- Exploração dos Blocos
- Coinbase & Halving
- Transações
- Redes & Exchanges
- Forking (quando dá briga)

Próxima aula

- Ethereum e as novas possibilidades