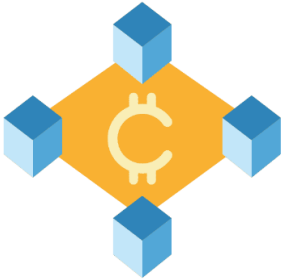


Cryptocurrencies: BITCOIN

Fundamentos da Blockchain

Juliana Mascarenhas

Tech Education Specialist DIO / Owner @Simplificandoredes e @SimplificandoProgramação

Mestre em modelagem computacional | Cientista de dados

@in/juliana-mascarenhas-ds/

Objetivo Geral

Explorar as características da plataforma pioneira no uso confiável da Blockchain. Iremos entender suas características e funcionamento.

Percurso

Etapa 1	Por que a Blockchain surgiu com Nakamoto?
Etapa 2	Whitepaper de Satoshi Nakamoto
Etapa 3	Entendendo como funciona o Bitcoin
Etapa 4	Por que utilizamos o termo mineração?

Percurso

Etapa 5	Adaptação da rede: dificuldade de mineração
Etapa 6	Bifurcações e Forks no Bitcoin
Etapa 7	Analisando as transações do Bitcoin

Etapa 1

Por que a Blockchain "surgiu" com Satoshi Nakamoto?

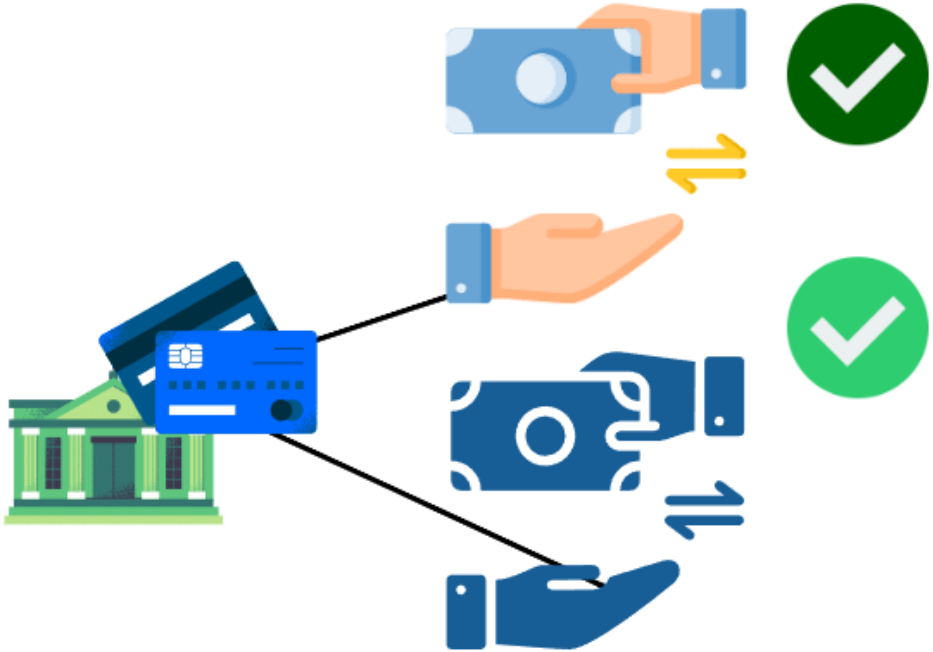
//Fundamentos da Blockchain/Cryptocurrencies: Bitcoin

Satoshi Nakamoto

- Mecanismo de consenso PoW
- Double spending & PoW
- Pioneiro - Uso confiável da Blockchain

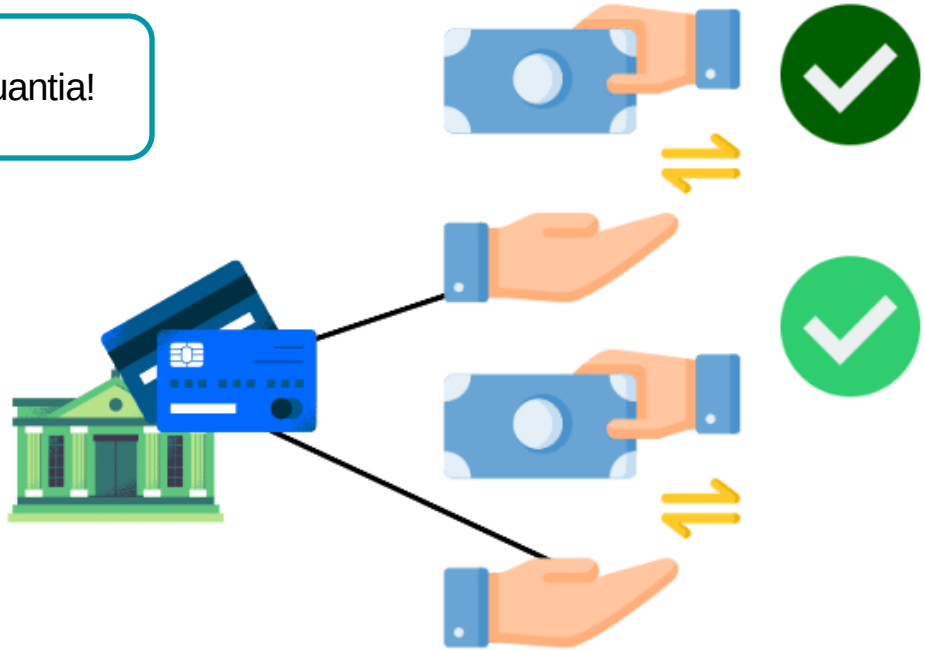
Bitcoin: A Peer-to-Peer Electronic Cash System

Mundo real – Third Trusted Party

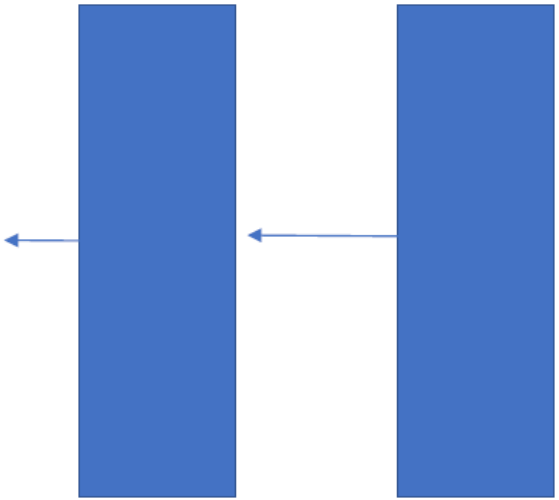


Mundo real – Third Trusted Party

Mesma quantia!



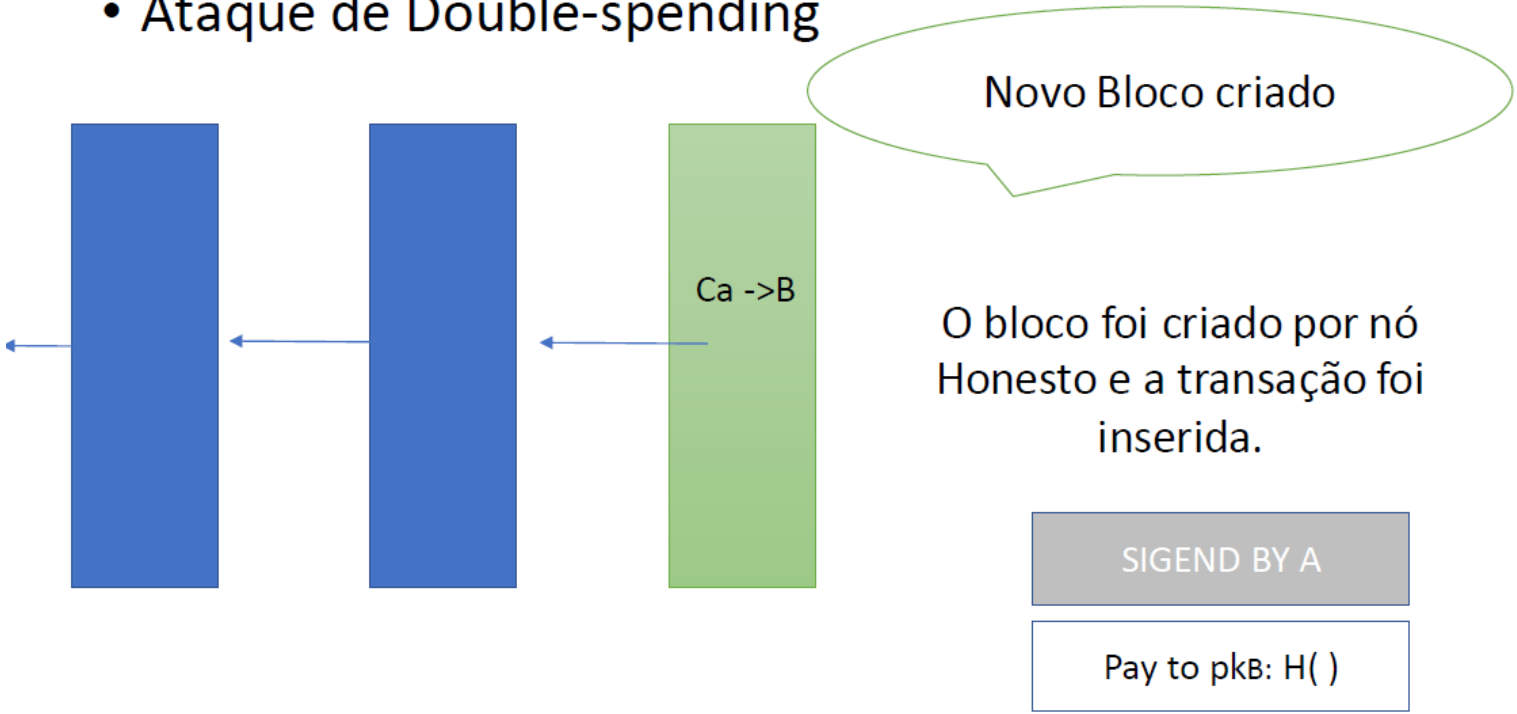
Double-Spending



Últimos Blocos
inseridos no Blockchain

Double-Spending

- Ataque de Double-spending

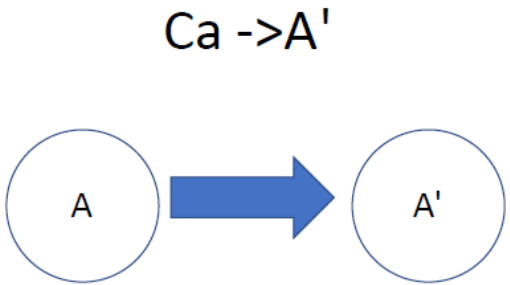


Double-Spending

- Bob recebeu a Transação de Alice
- Bob libera à Alice o produto
- Produto: Download do Software

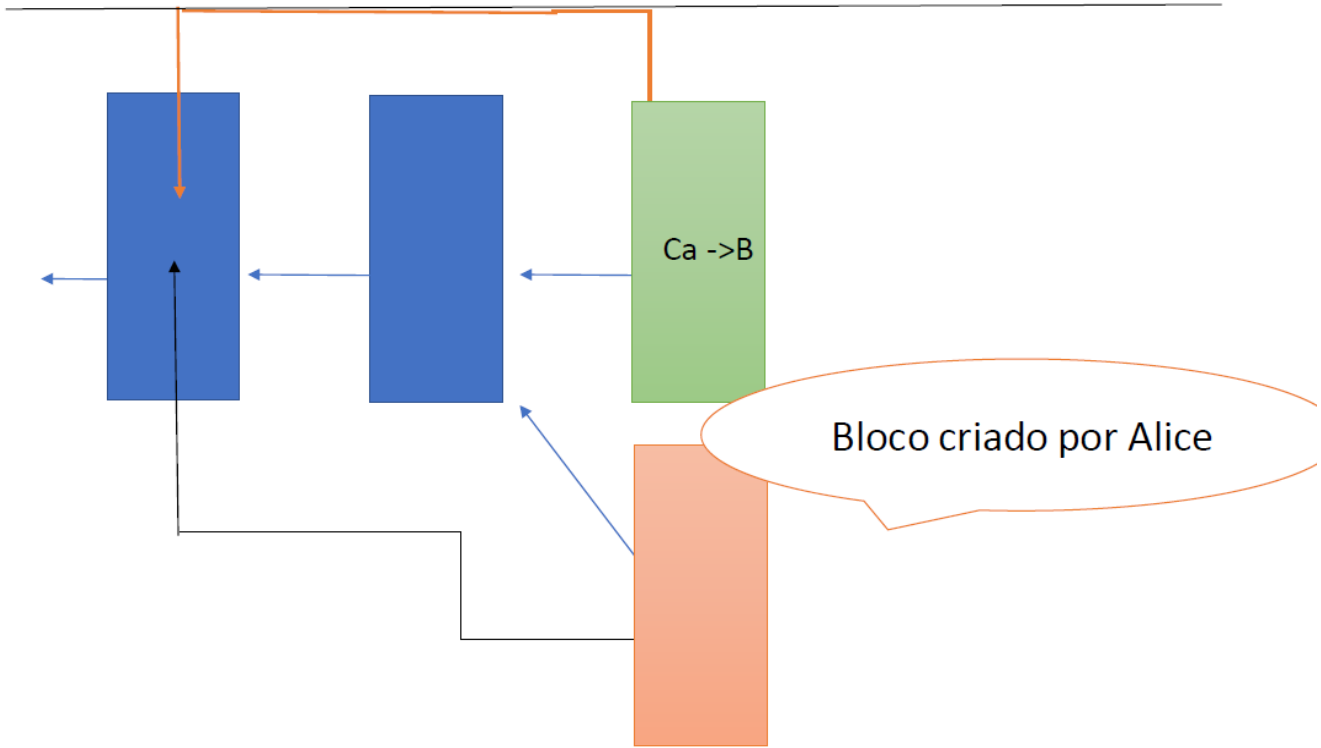
Double-Spending

- Alice realiza outra transação

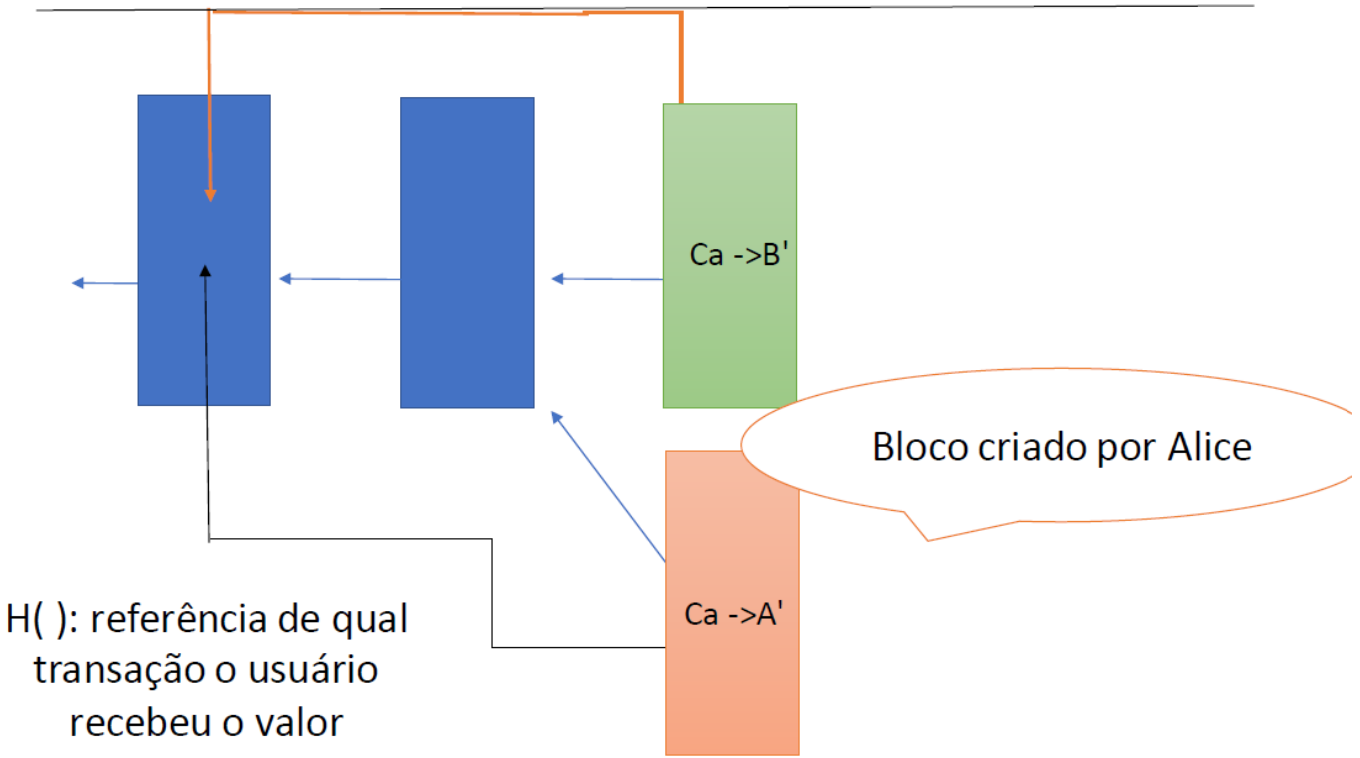


A' = conta alternativa de Alice

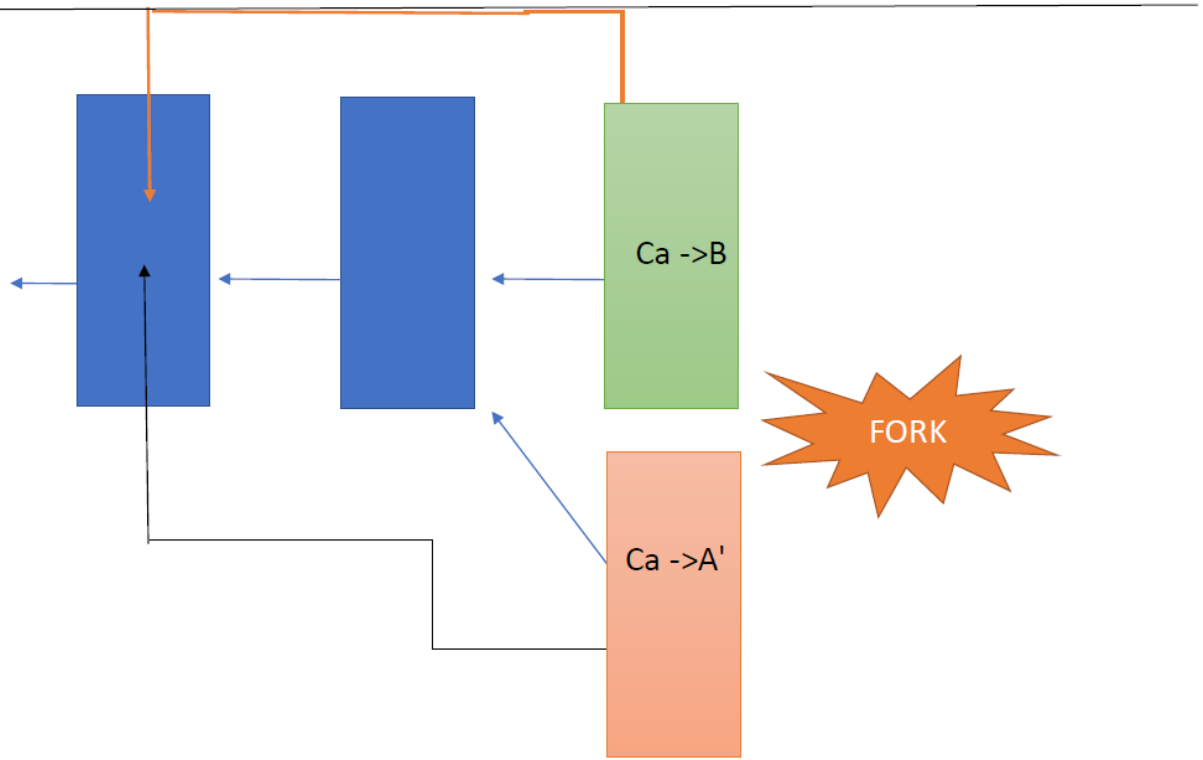
Double-Spending



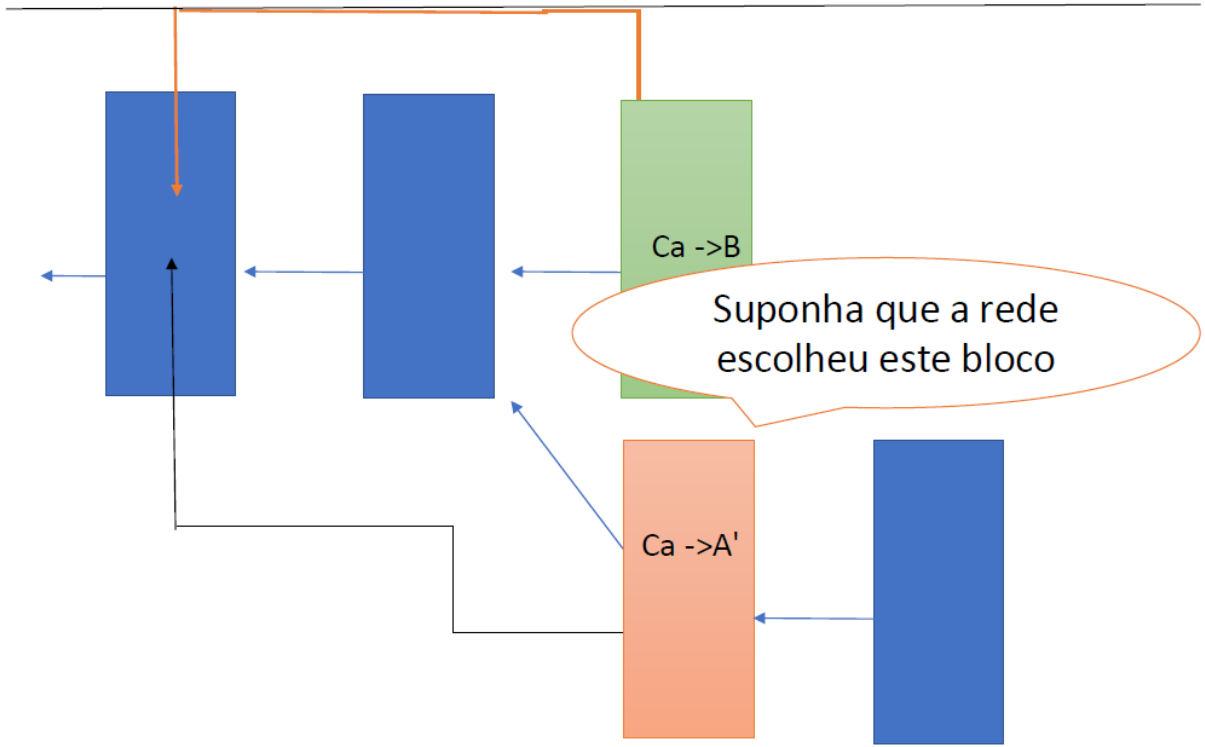
Double-Spending



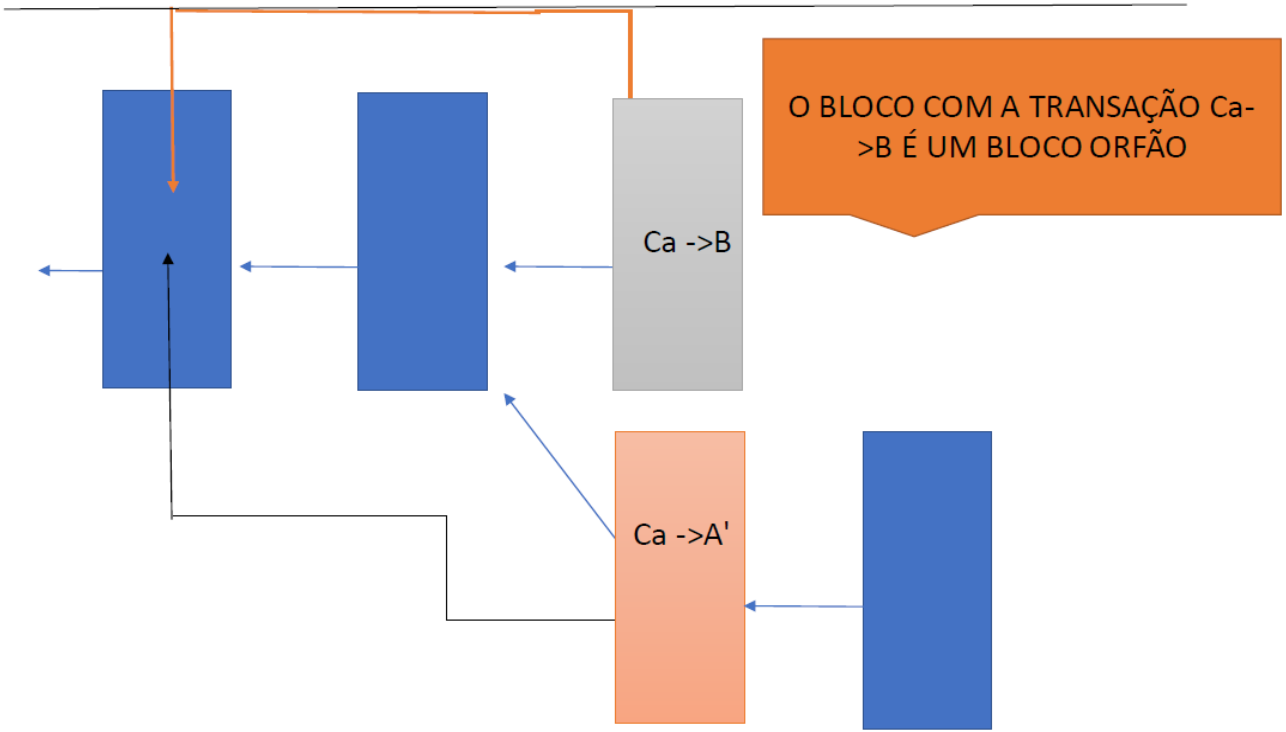
Double-Spending



Double-Spending



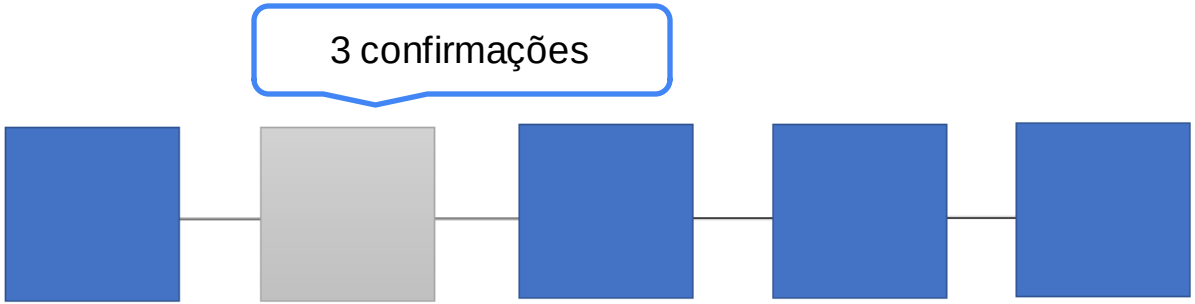
Double-Spending



Double-Spending

Solução

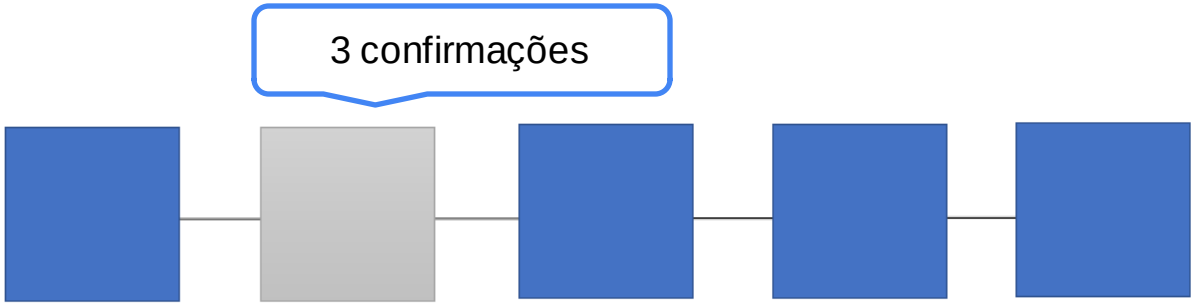
- Número de confirmações - Blocos
- N° blocos ≡ Maior confiança



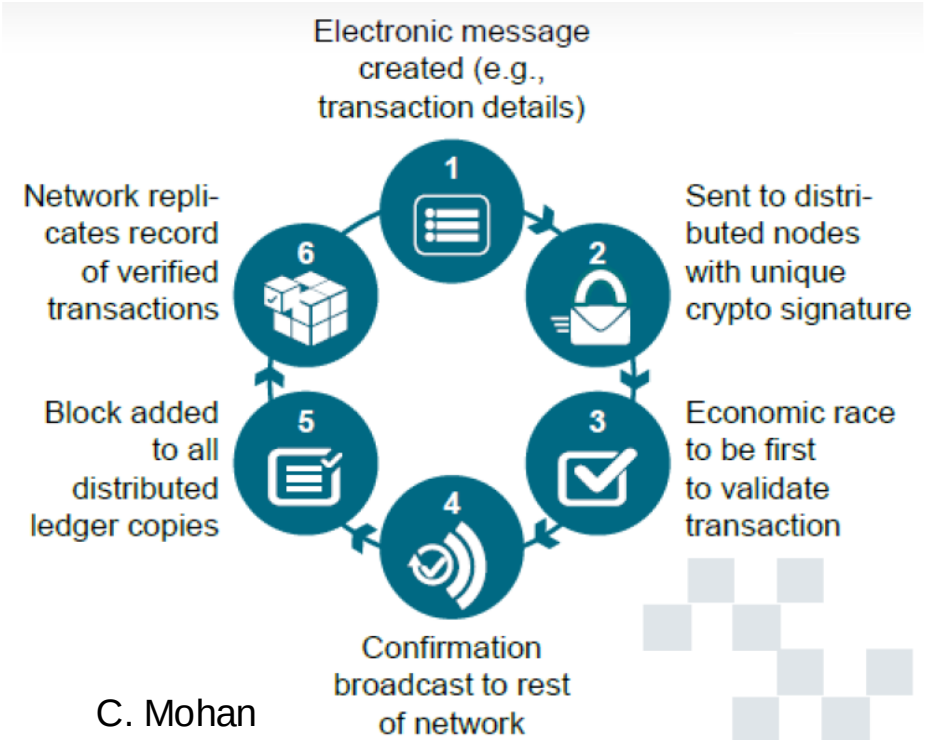
Double-Spending

Prevenção

- Estrutura da Blockchain
- Confirmações de blocos



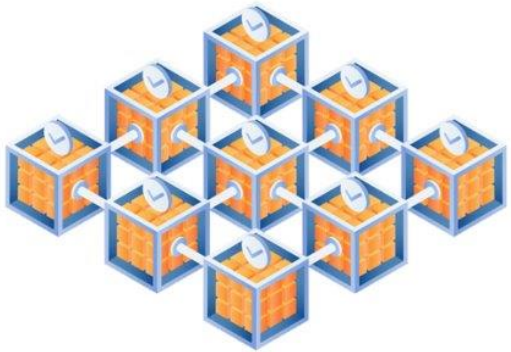
Double-Spending



C. Mohan

Versões da Blockchain

- **Versão 1.0:** Foco inicial, ambito **financeiro**, da tecnologia com Bitcoin
- **Versão 2.0**: Expansão da Blockchain com os **Smart Contracts** substituindo os papeis tradicionais
- **Versão 3.0**: **Dapps** que operam utilizando a infraestrutura da Blockchain



Etapa 2

Whitepaper de Nakamoto - Bitcoin

//Fundamentos da Blockchain/Cryptocurrencies: Bitcoin

White paper

- Satoshi Nakamoto - 2009
- Implementação original
- Double-spending
- ~~Third Trusted Party~~
- Hash + PoF

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

White paper

Força no poder computacional

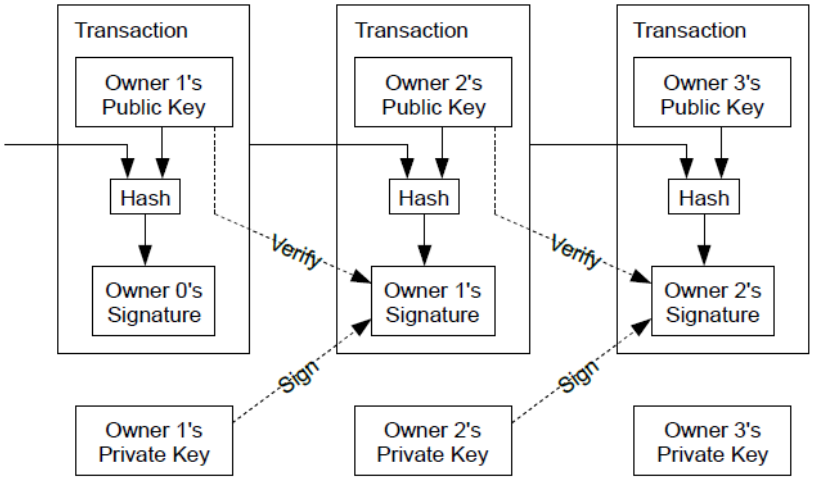
- Satoshi Nakamoto - 2009
- Implementação original
- Double-spending
- ~~Third Trusted Party~~
- Hash + PoF

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Broadcast mesages

White paper



Estrutura das transações

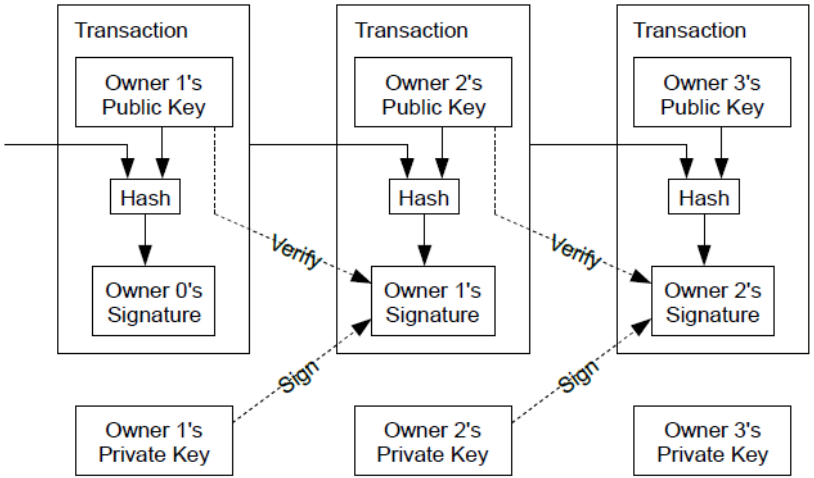
Hash

Assinaturas digitais

2. Transactions

Bitcoin: A Peer-to-Peer Electronic Cash System

White paper



E o double-spending?

Estrutura das transações

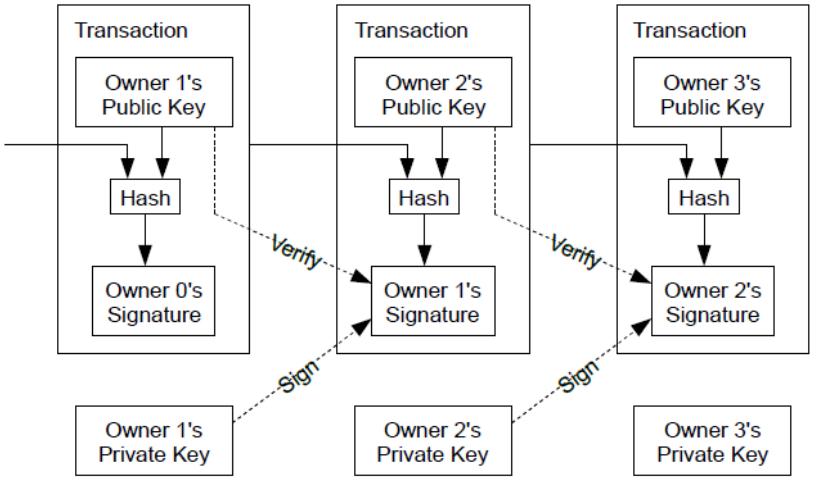
Hash

Assinaturas digitais

2. Transactions

Bitcoin: A Peer-to-Peer Electronic Cash System

White paper



E o double-spending?

Estrutura das transações

Hash

Assinaturas digitais

Saber de todas as transações

2. Transactions

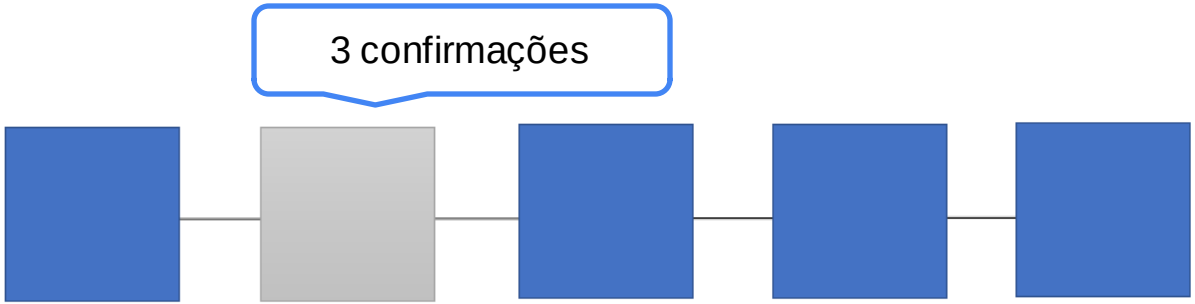
Bitcoin: A Peer-to-Peer Electronic Cash System

Double-Spending

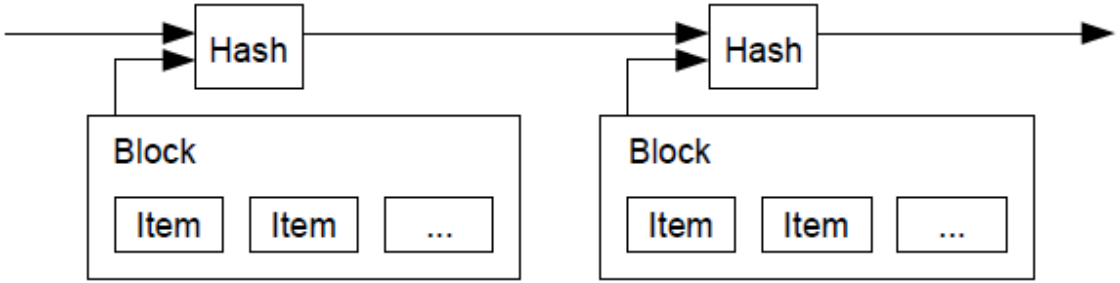
Transações Públicas

Solução

- Número de confirmações - Blocos
- N° blocos ≡ Maior confiança



White paper



Timestamp das transações

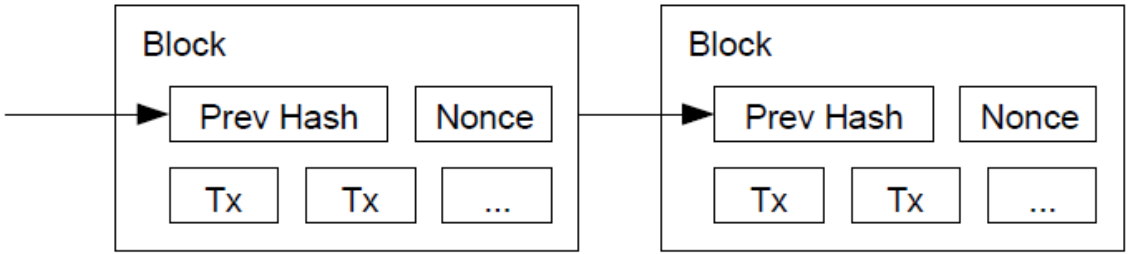
Hash

Assinaturas digitais

3. Timestamp Server

Bitcoin: A Peer-to-Peer Electronic Cash System

White paper



PoW

Mineração

Poder computacinal

4. Proof-of-Work

Bitcoin: A Peer-to-Peer Electronic Cash System

White paper

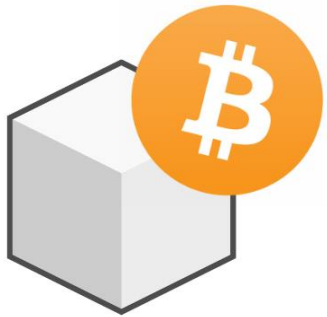
- Transações broadcasted para rede
- Cada nó adiciona as transações em um bloco
- Achou o PoW – broadcast o bloco
- Bloco aceito: transações são válidas
- Sinal de aceitação pela construção do próximo bloco

5. Network

Bitcoin: A Peer-to-Peer Electronic Cash System

White paper

- Incentivo para dar suporte a rede
- Gasto de energia e tempo CPU
- Transação especial



6. Incentive

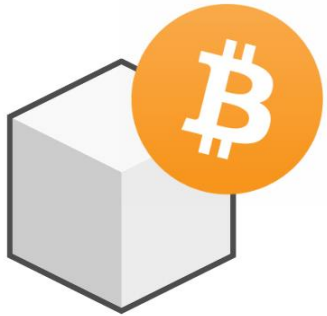
Bitcoin: A Peer-to-Peer Electronic Cash System

[32]

White paper

- Incentivo para dar suporte a rede
- Gasto de energia e tempo CPU
- Transação especial

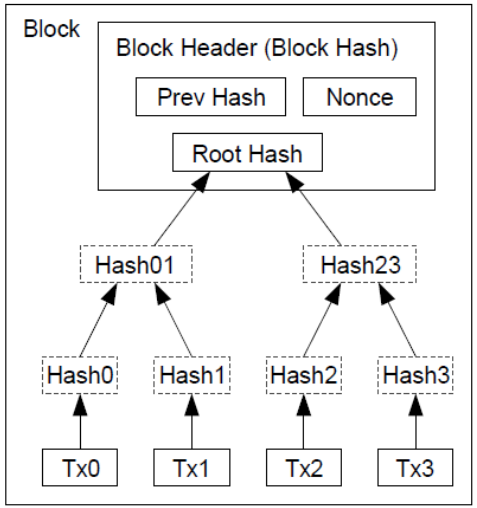
Manter honestidade



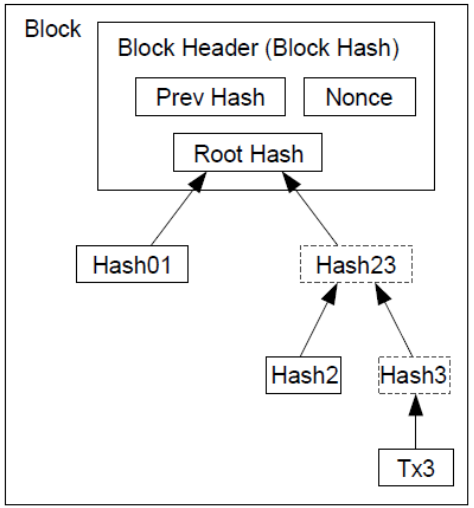
6. Incentive

Bitcoin: A Peer-to-Peer Electronic Cash System

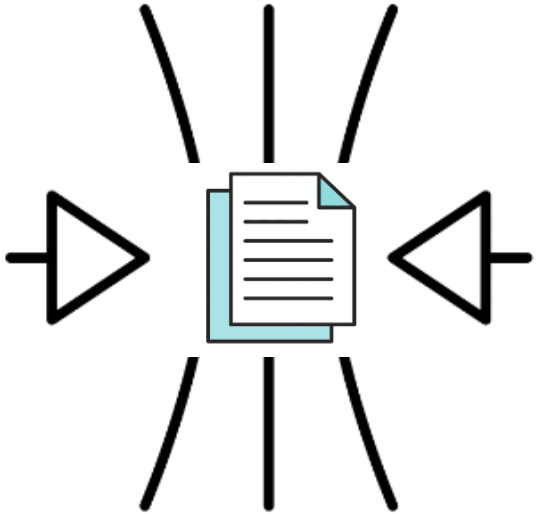
White paper



Transactions Hashed in a Merkle Tree

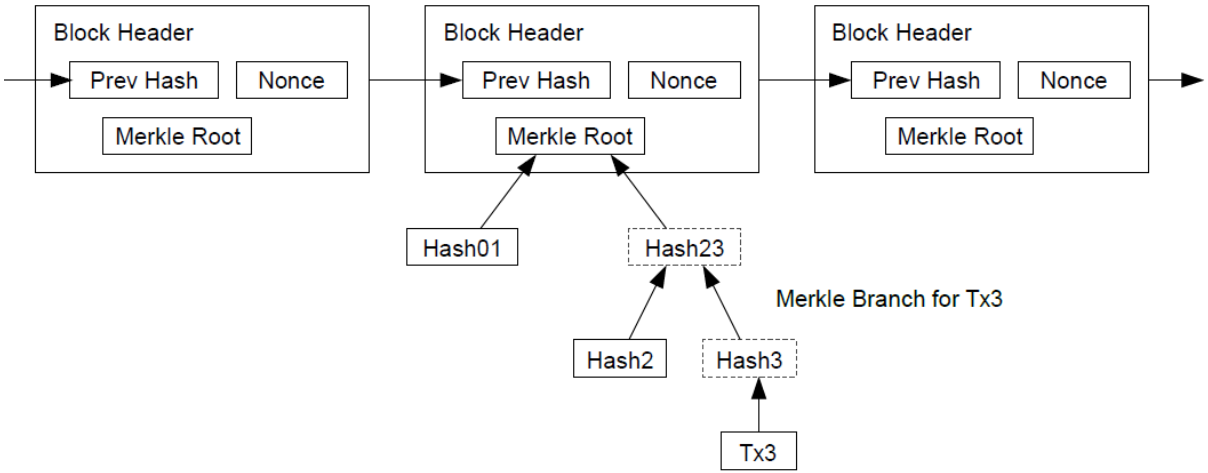


After Pruning Tx0-2 from the Block



7. Reclaiming Disk Space **Bitcoin: A Peer-to-Peer Electronic Cash System**

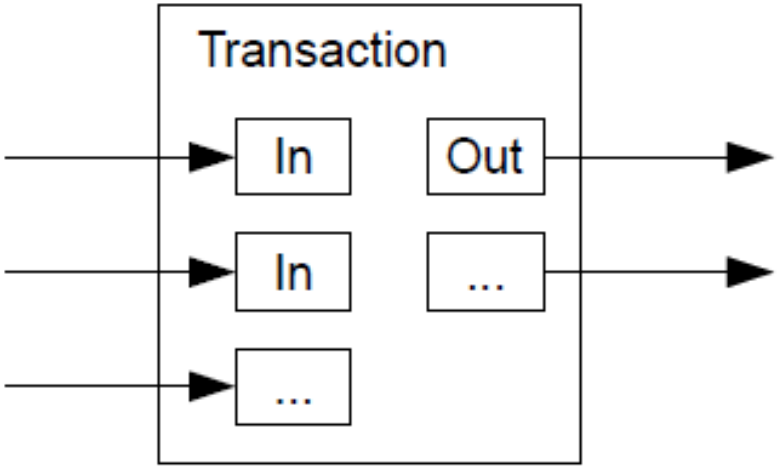
White paper



8. Simplified Payment Verification

Bitcoin: A Peer-to-Peer Electronic Cash System

White paper

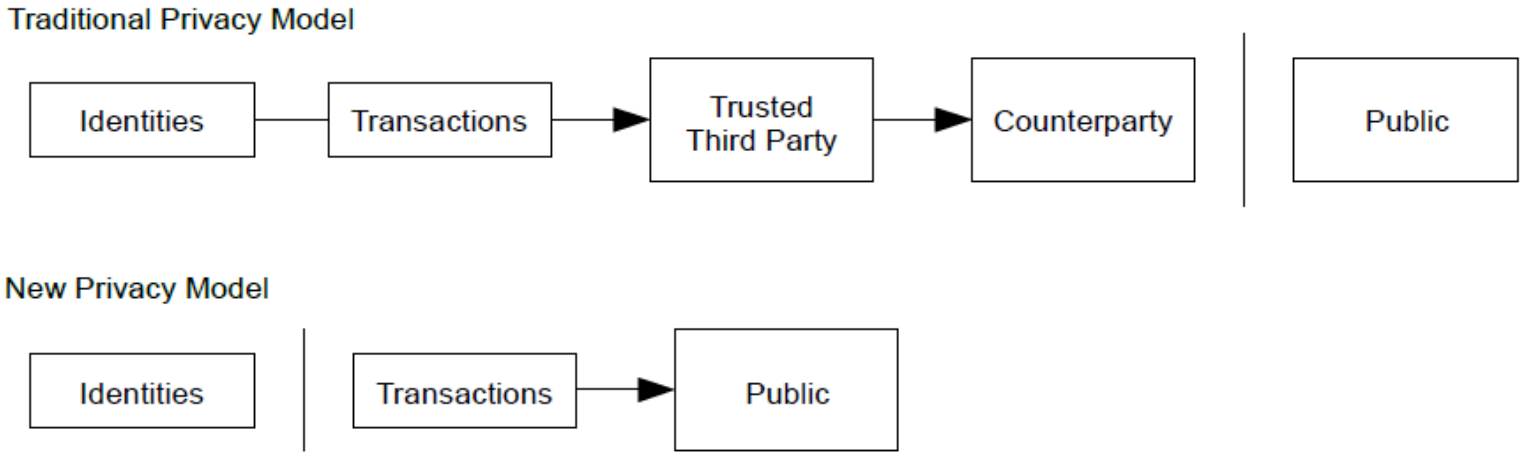


9. Combining and Splitting Value

Bitcoin: A Peer-to-Peer Electronic Cash System

[36]

White paper



10. Privacy

Bitcoin: A Peer-to-Peer Electronic Cash System

White paper

- Bloco alterado não é aceito pela rede
- Resta tentar rollback da transação
- **Race**: binominal radon walk

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

11. Calculations

Bitcoin: A Peer-to-Peer Electronic Cash System

White paper

- Bloco alterado não é aceito pela rede
- Resta tentar rollback da transação
- **Race**: binominal radon walk

11. Calculations

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

White paper

Rede P2P para realizações de transações com diretivas para previnir o double-speding de valores. Além disso Satoshi apresentou o mecismo de prova de trabalho para manter a chain imutável.

12. Conclusion

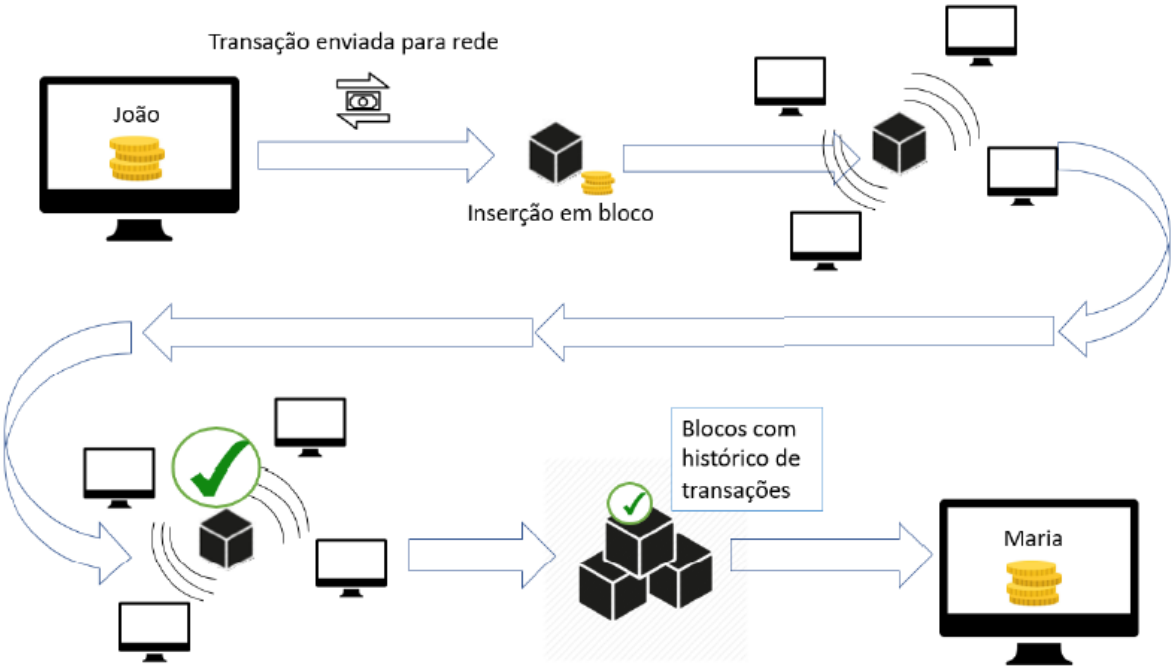
Bitcoin: A Peer-to-Peer Electronic Cash System

Etapa 3

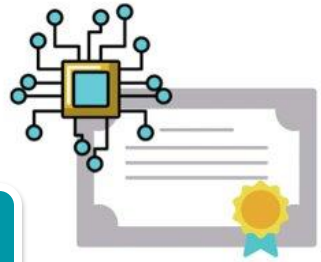
Entendendo como funciona o Bitcoin

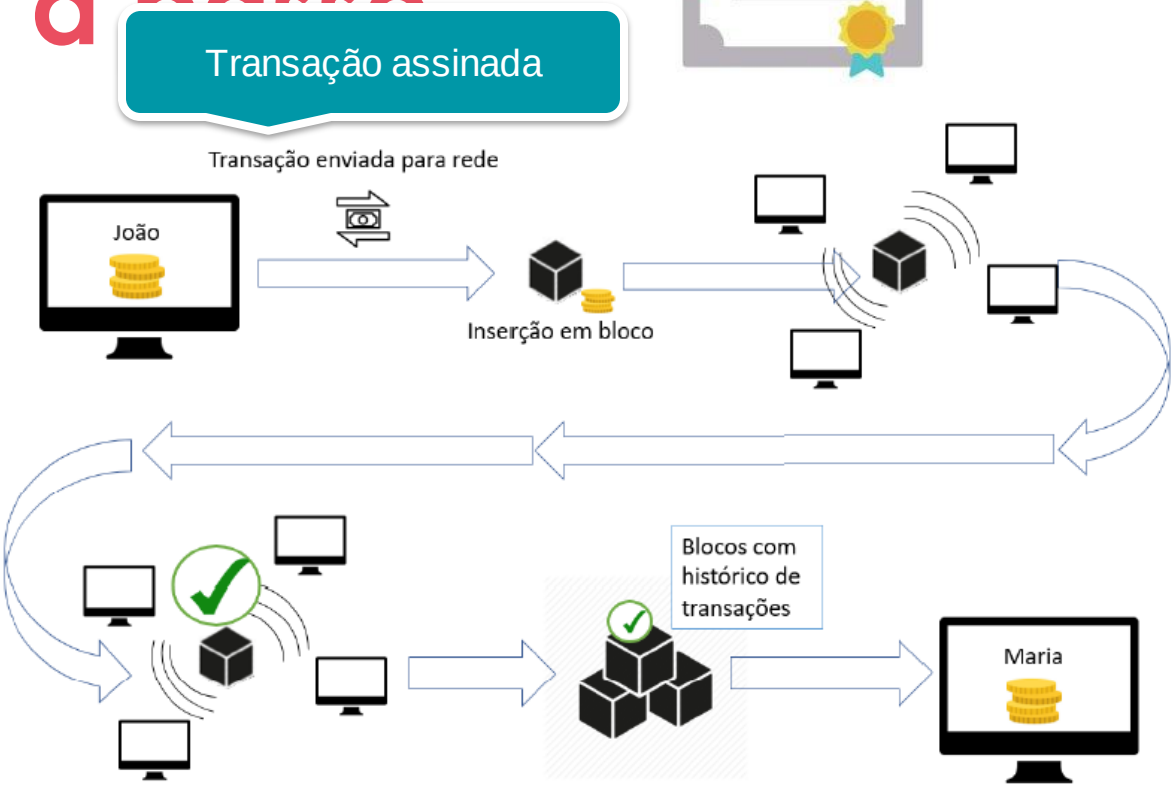
//Fundamentos da Blockchain/Cryptocurrencies: Bitcoin

Passo a passo

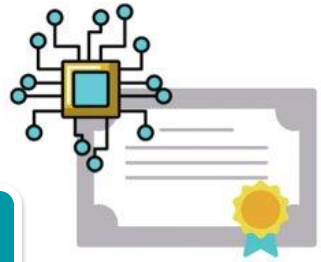


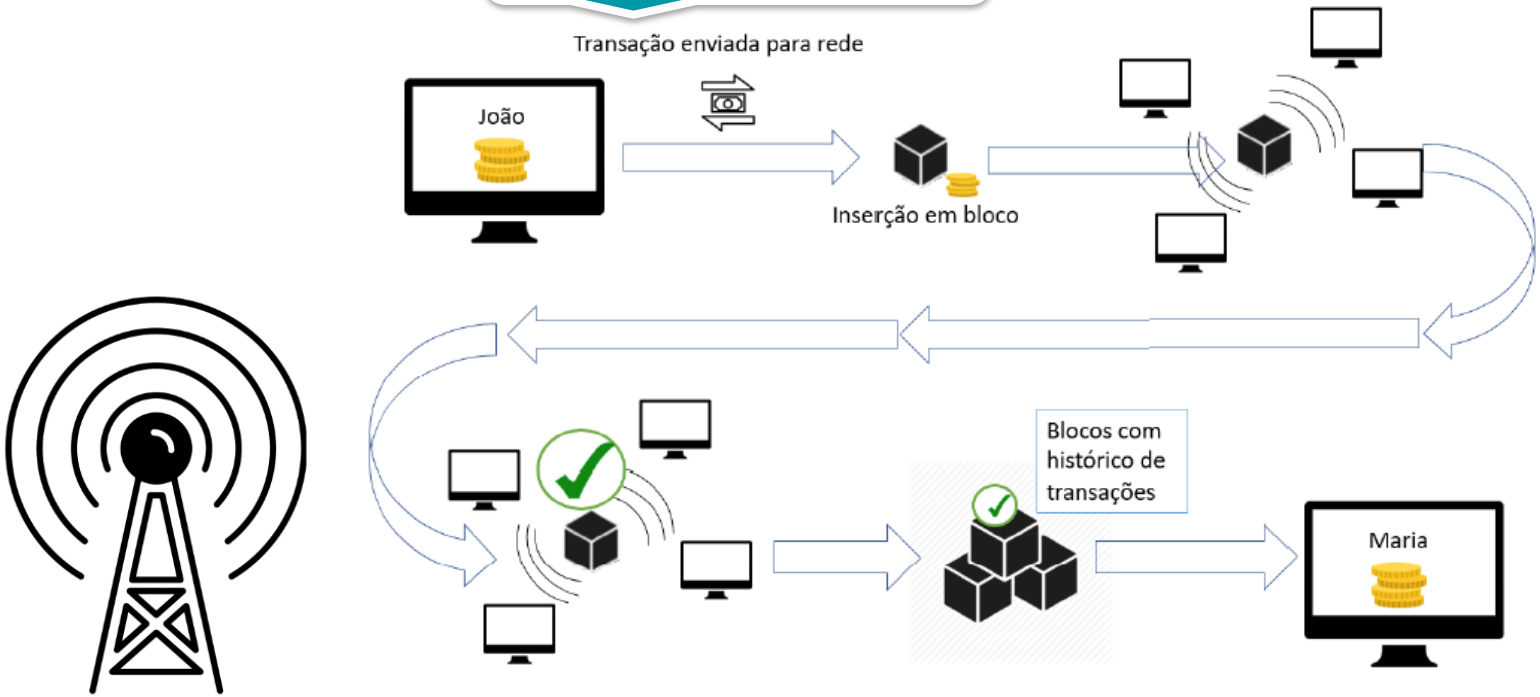
Passo a passo





Passo a passo

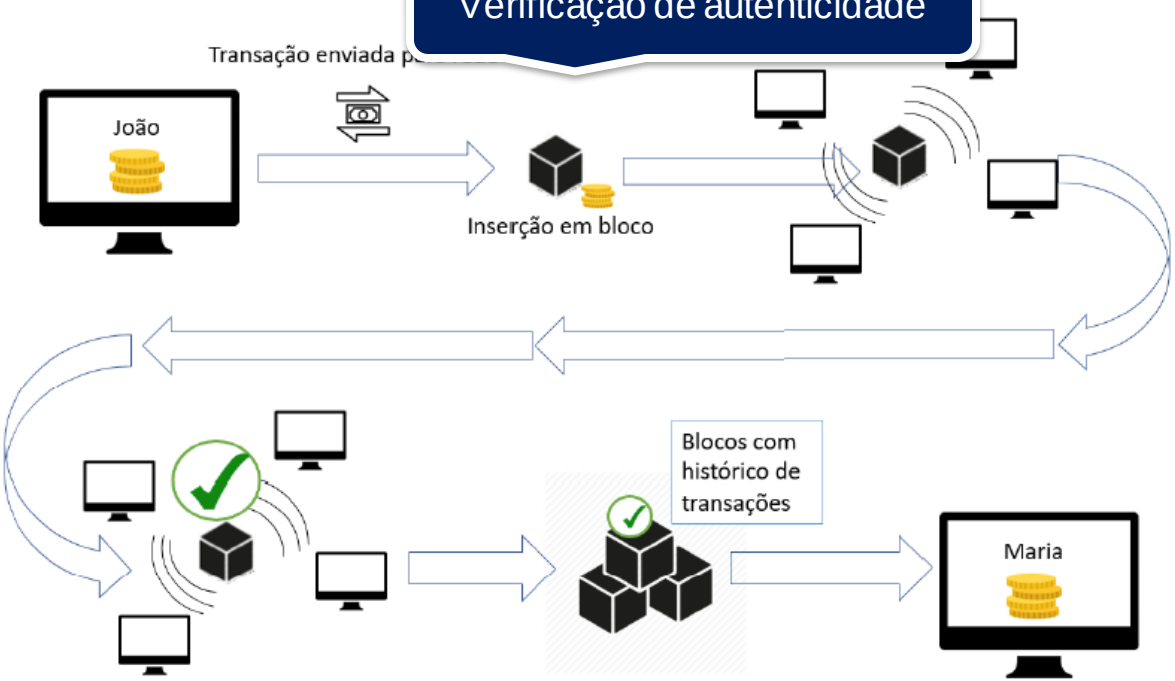




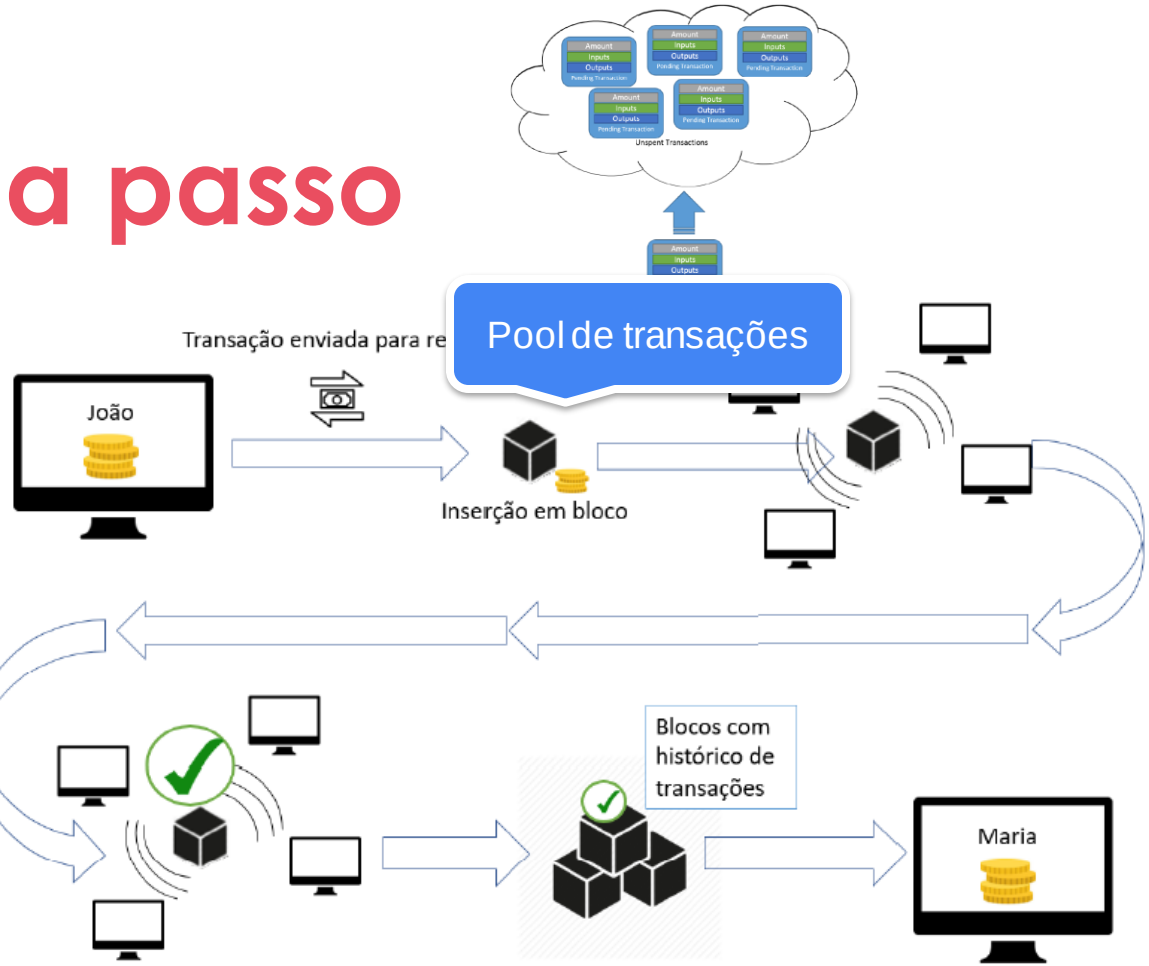
Passo a passo

Double-speding

Verificação de autenticidade



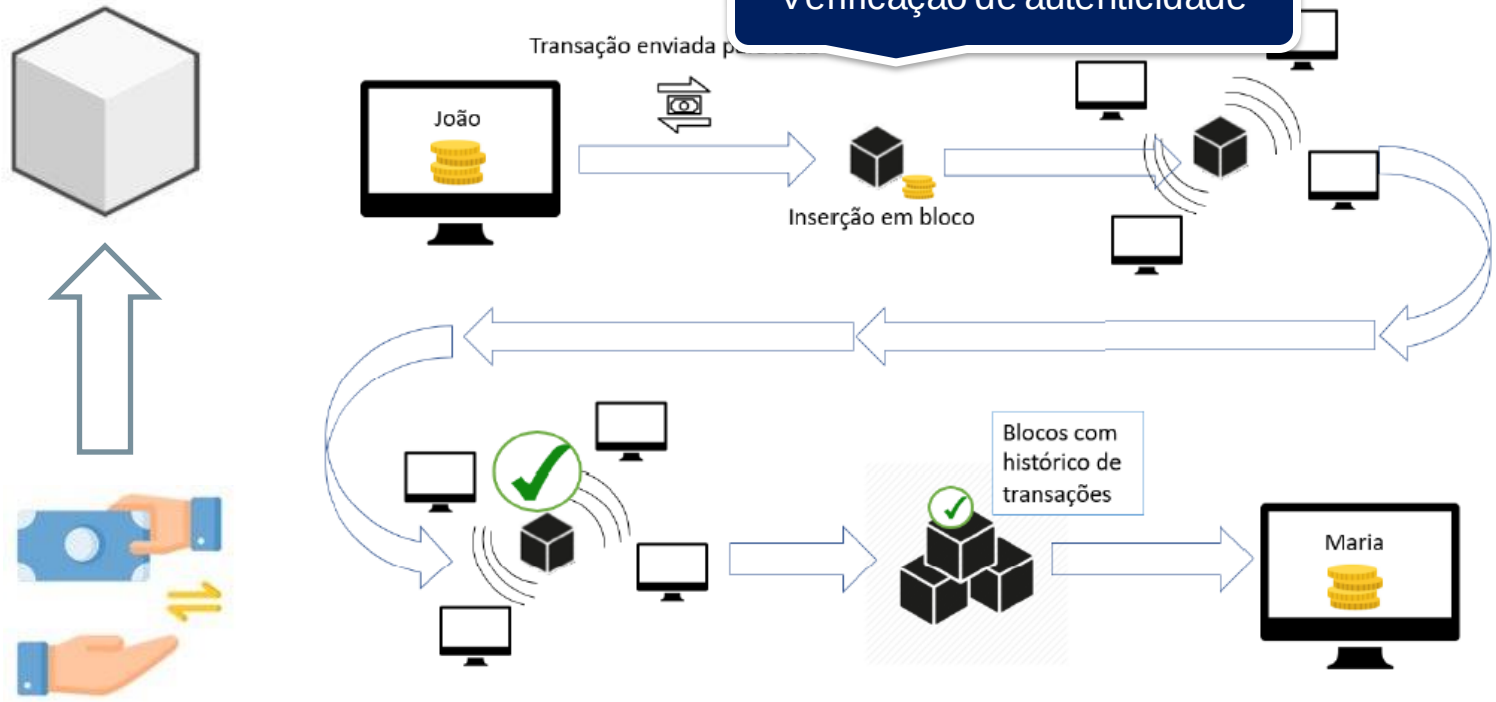
Passo a passo



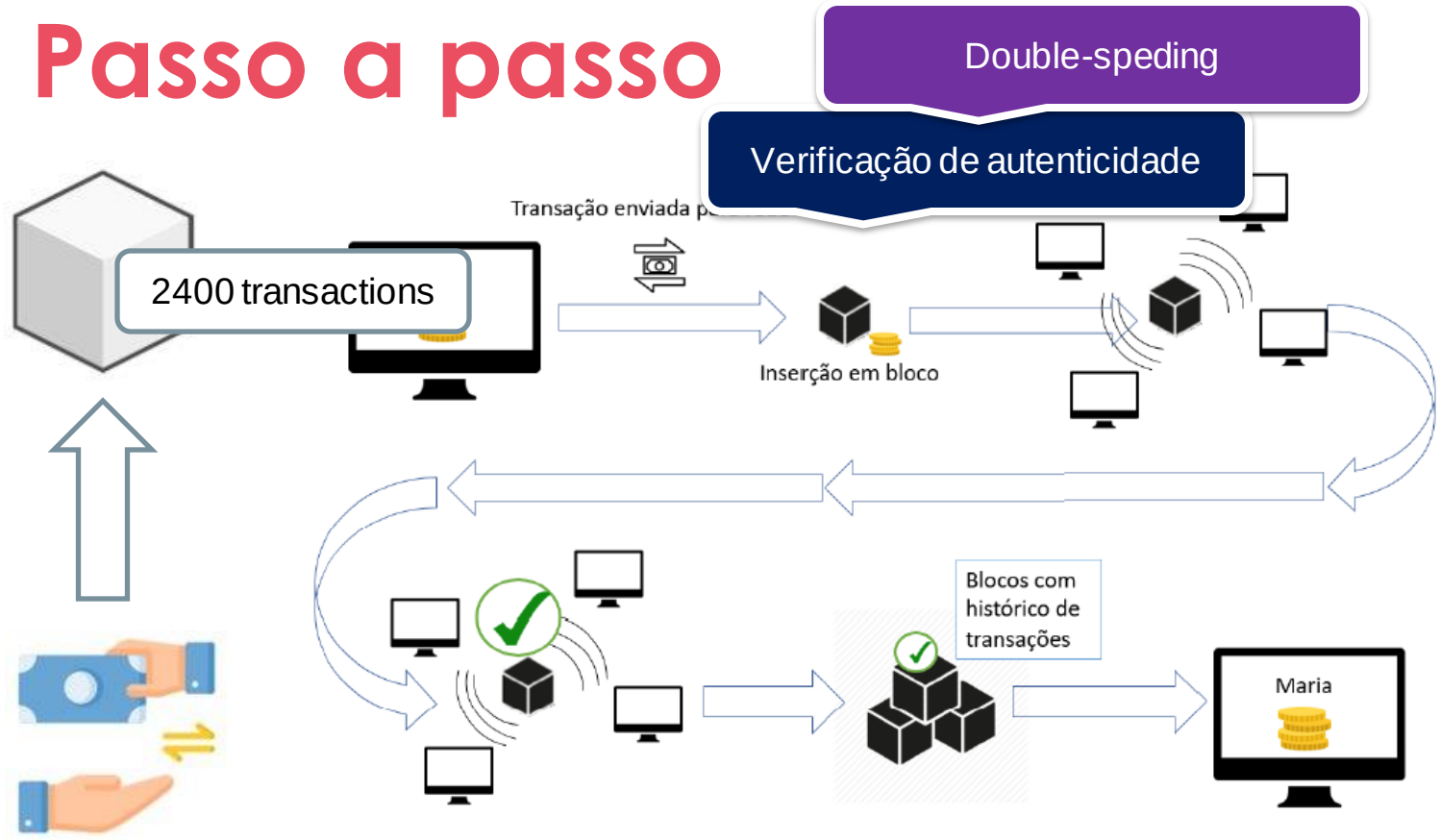
Passo a passo

Double-speding

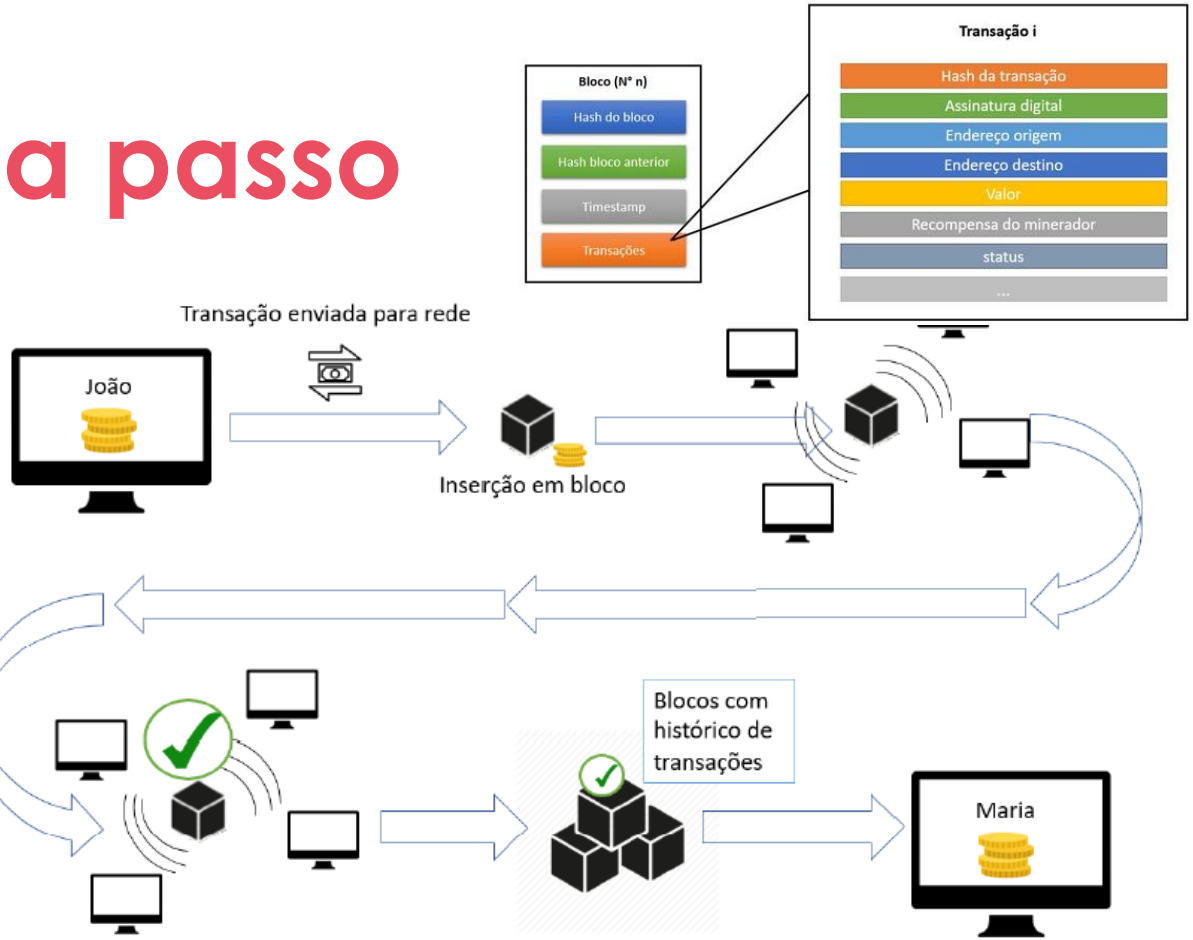
Verificação de autenticidade



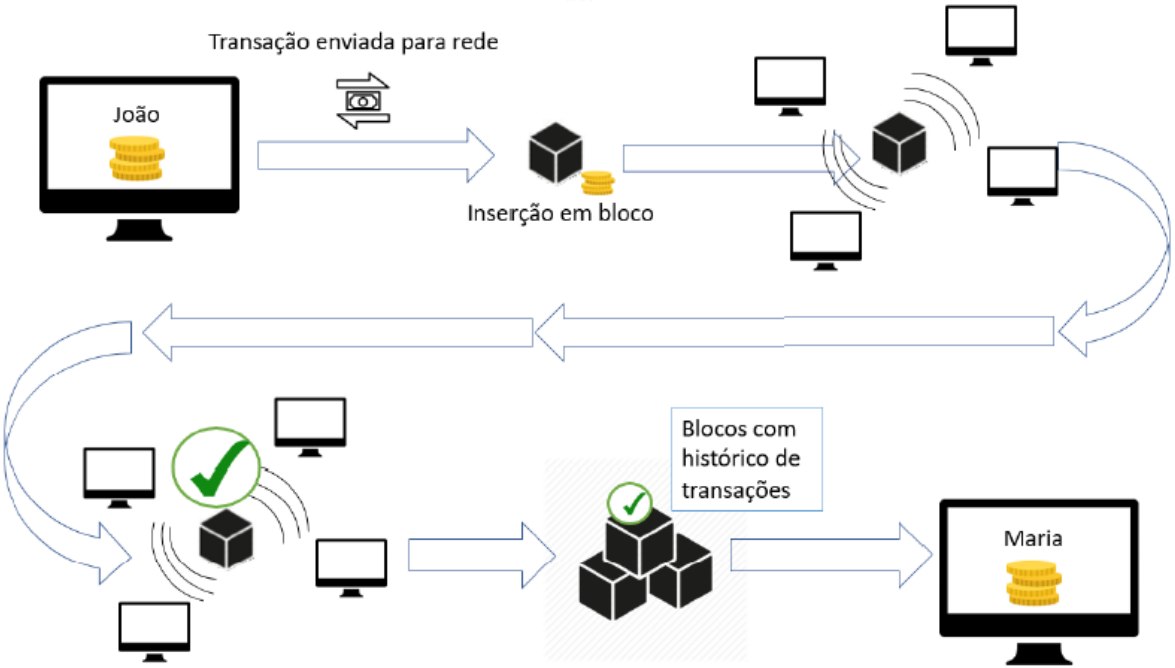
Passo a passo



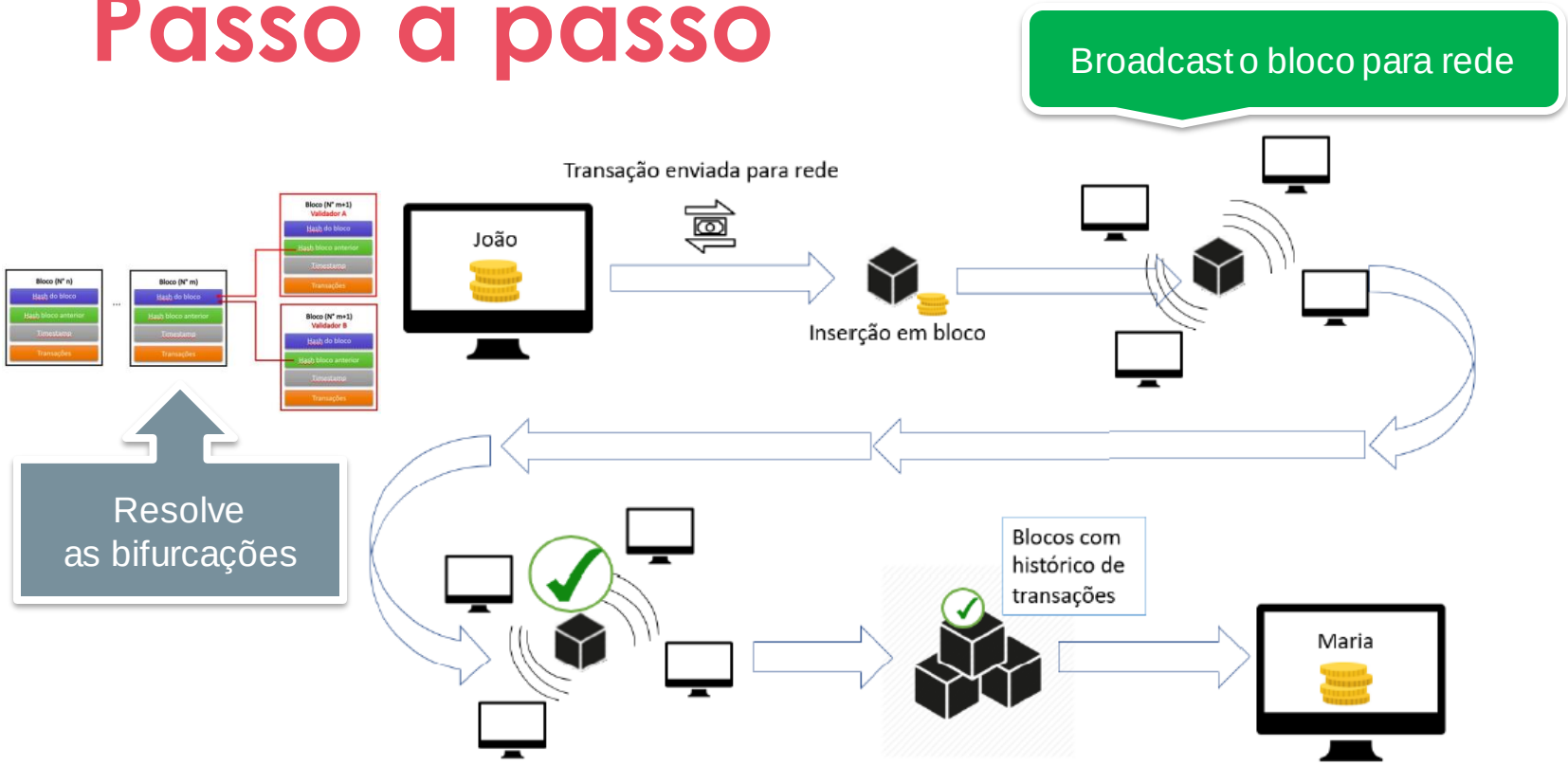
Passo a passo



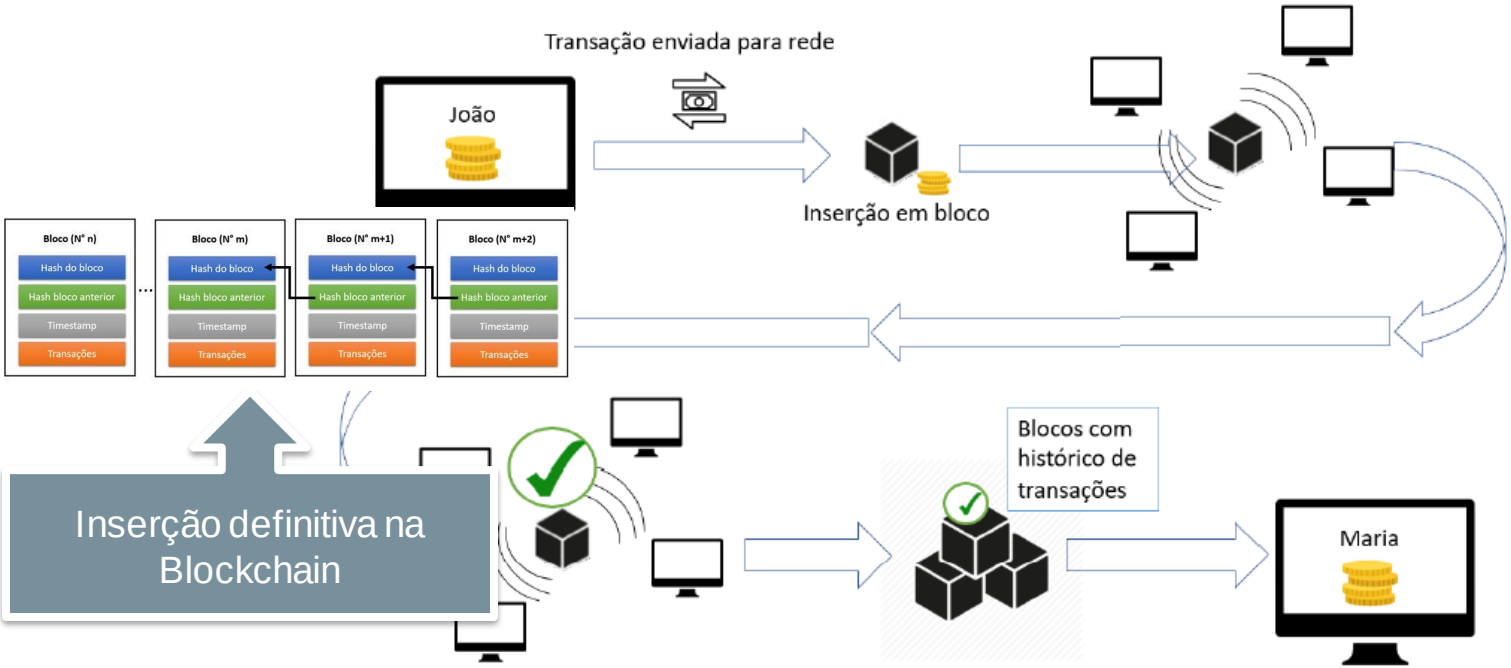
Passo a passo



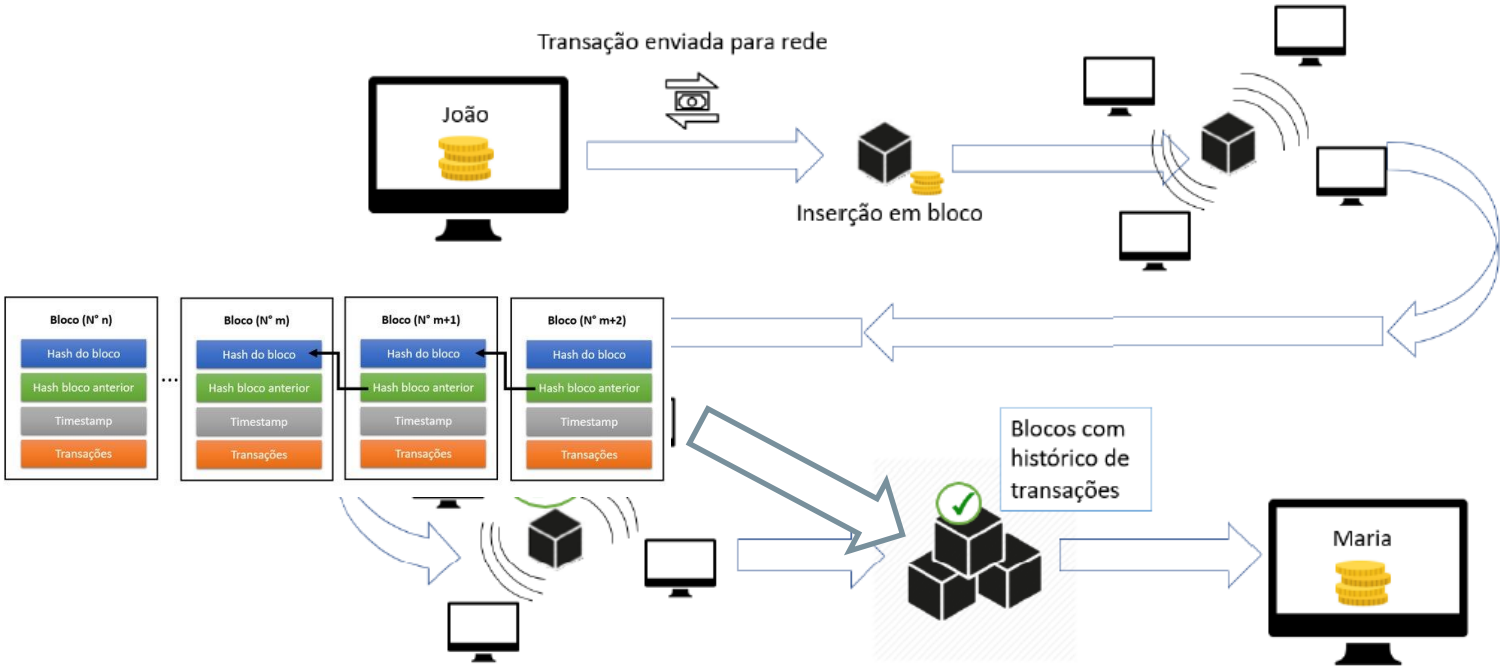
Passo a passo



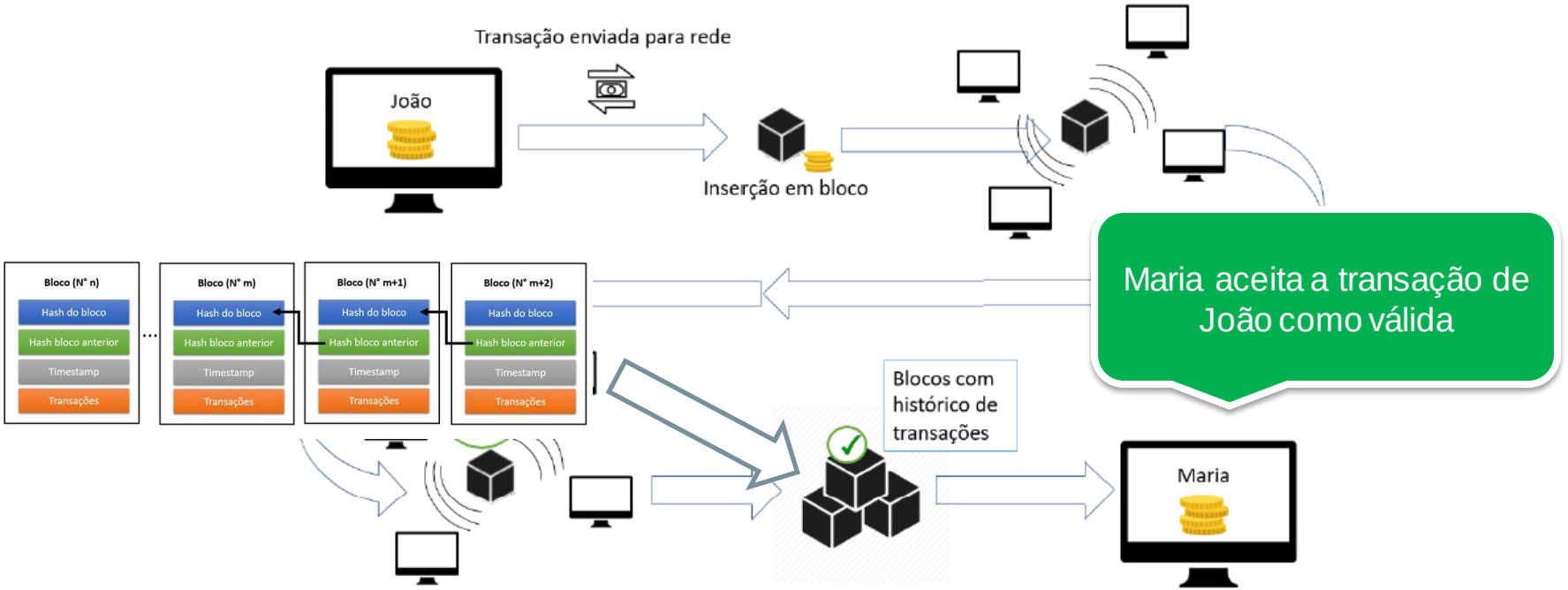
Passo a passo



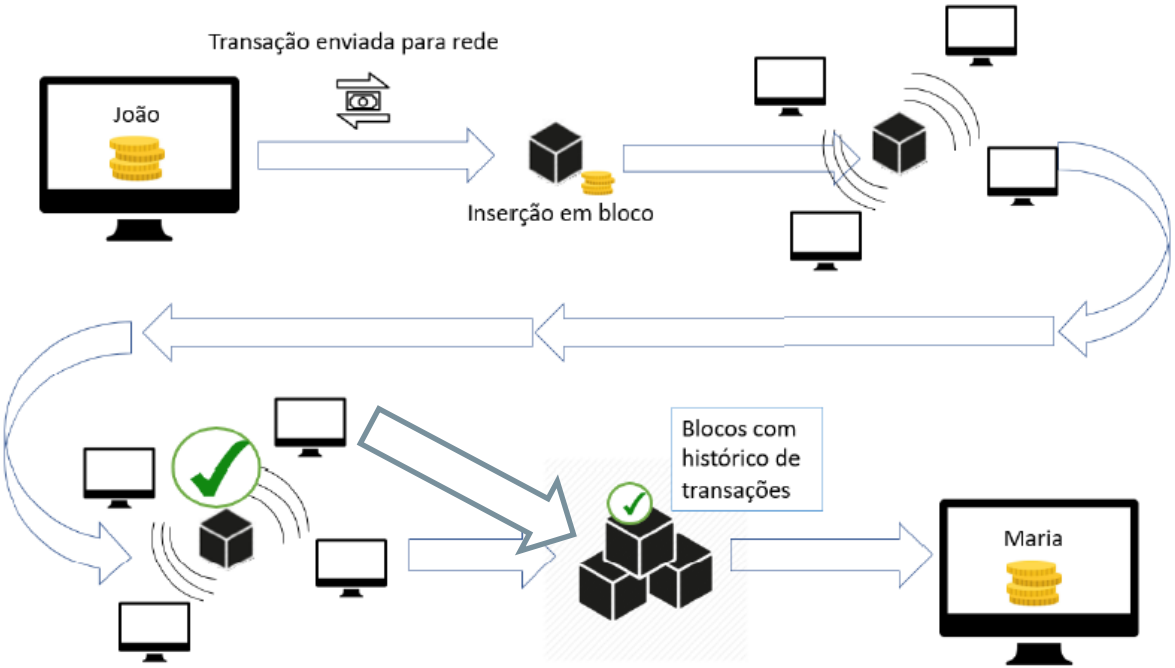
Passo a passo



Passo a passo



Operação das Criptos



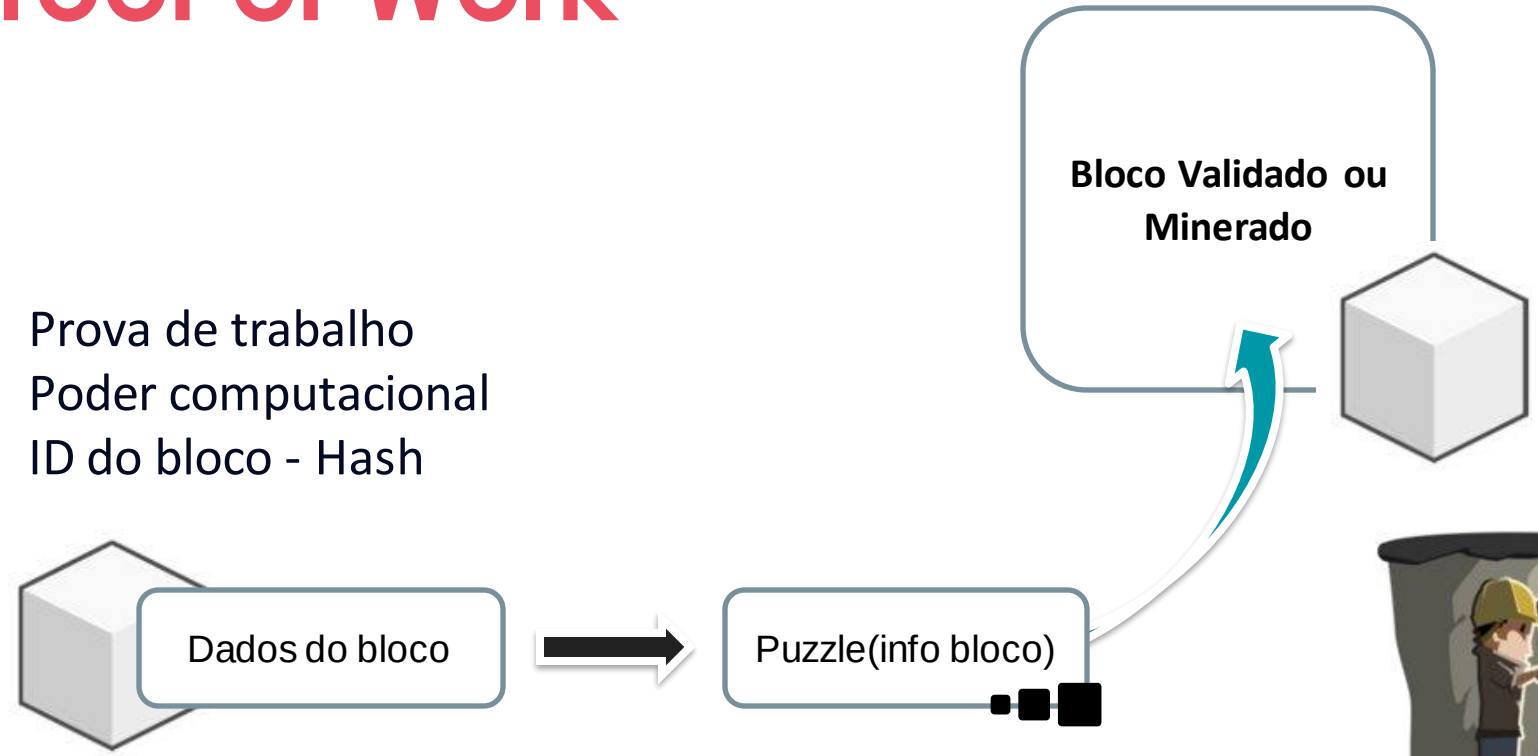
Etapa 4

Por que utilizamos o termo Mineração?

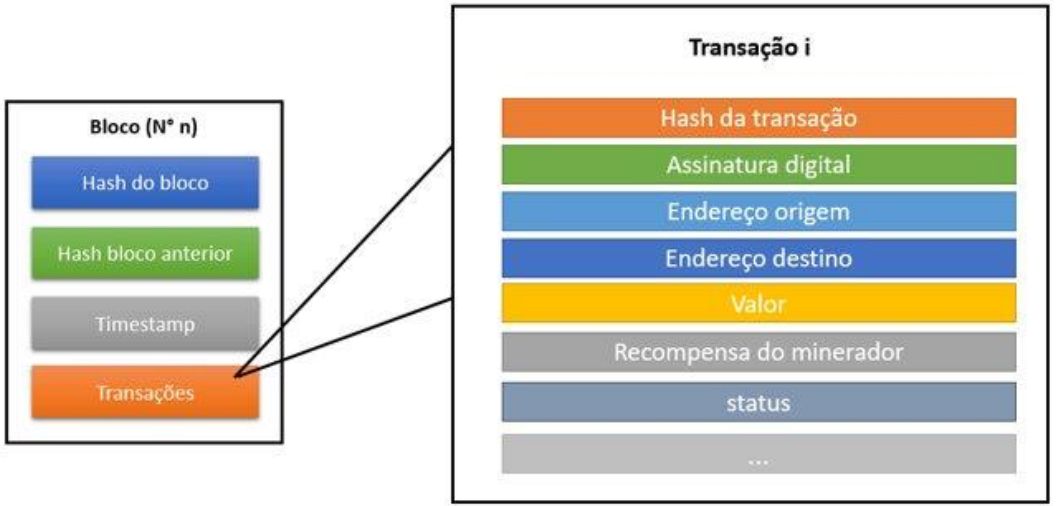
//Fundamentos da Blockchain/Cryptocurrencies: Bitcoin

Proof of Work

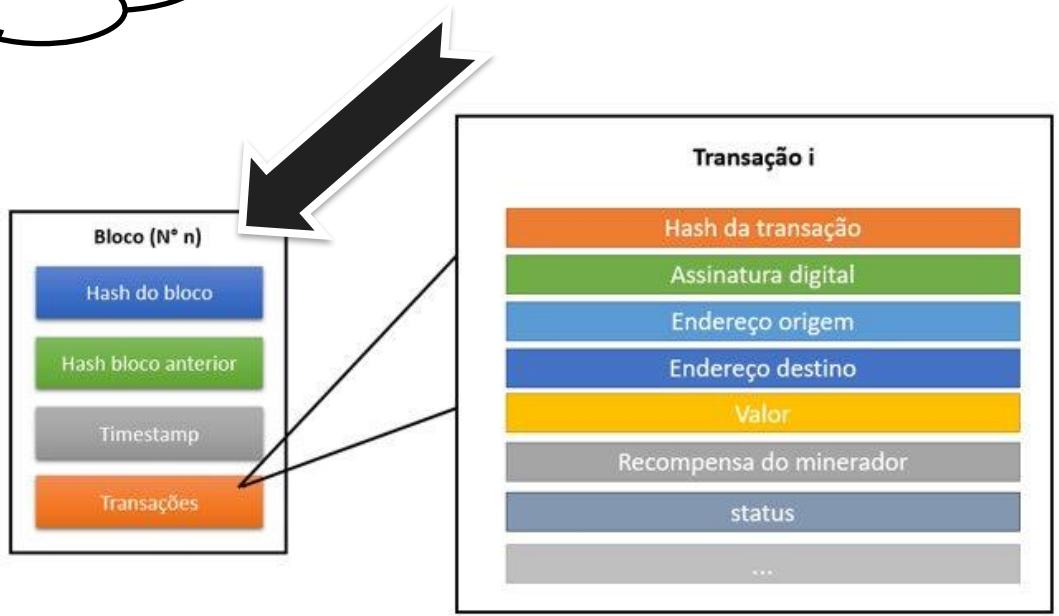
- Prova de trabalho
- Poder computacional
- ID do bloco - Hash



Proof of Work



Proof of Work



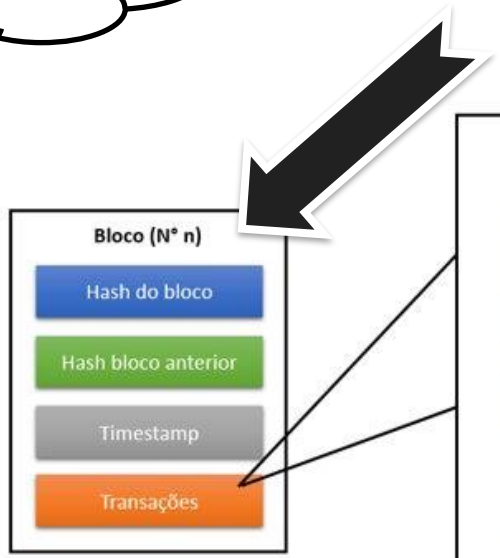
Proof of Work

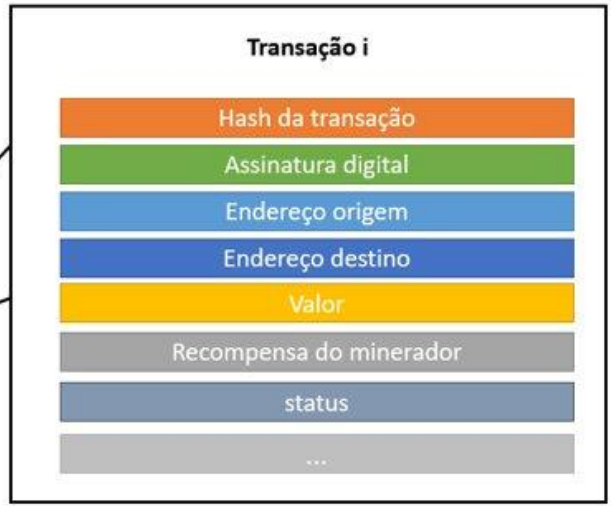
Cabeçalho

Hash das transações

Hash do bloco anterior

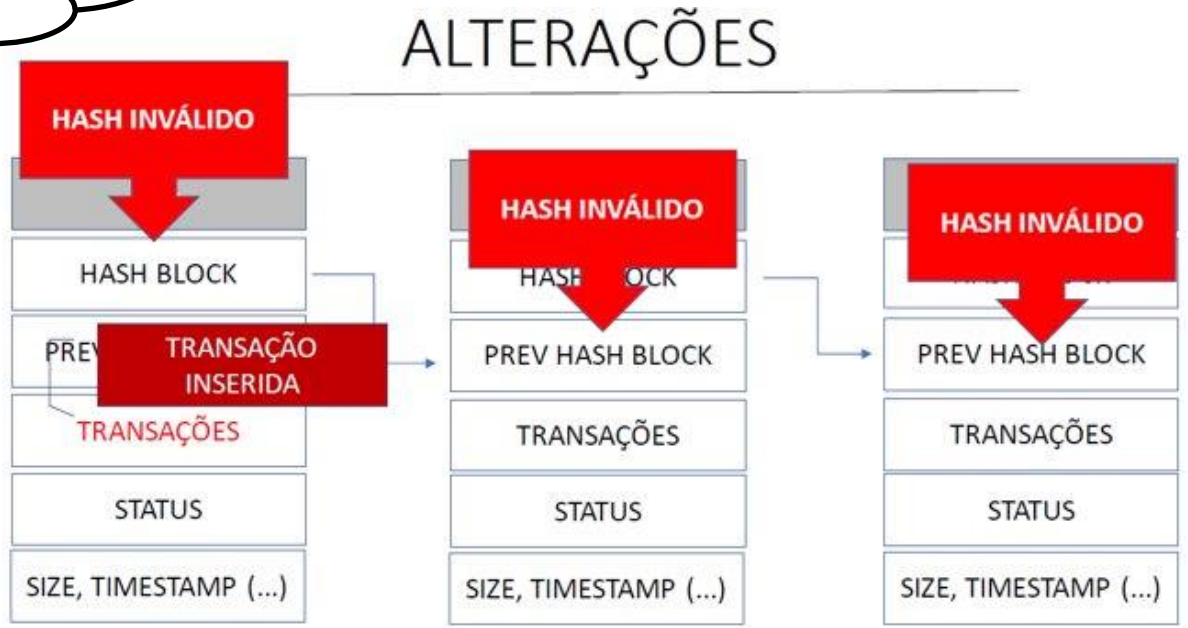
...





Proof of Work

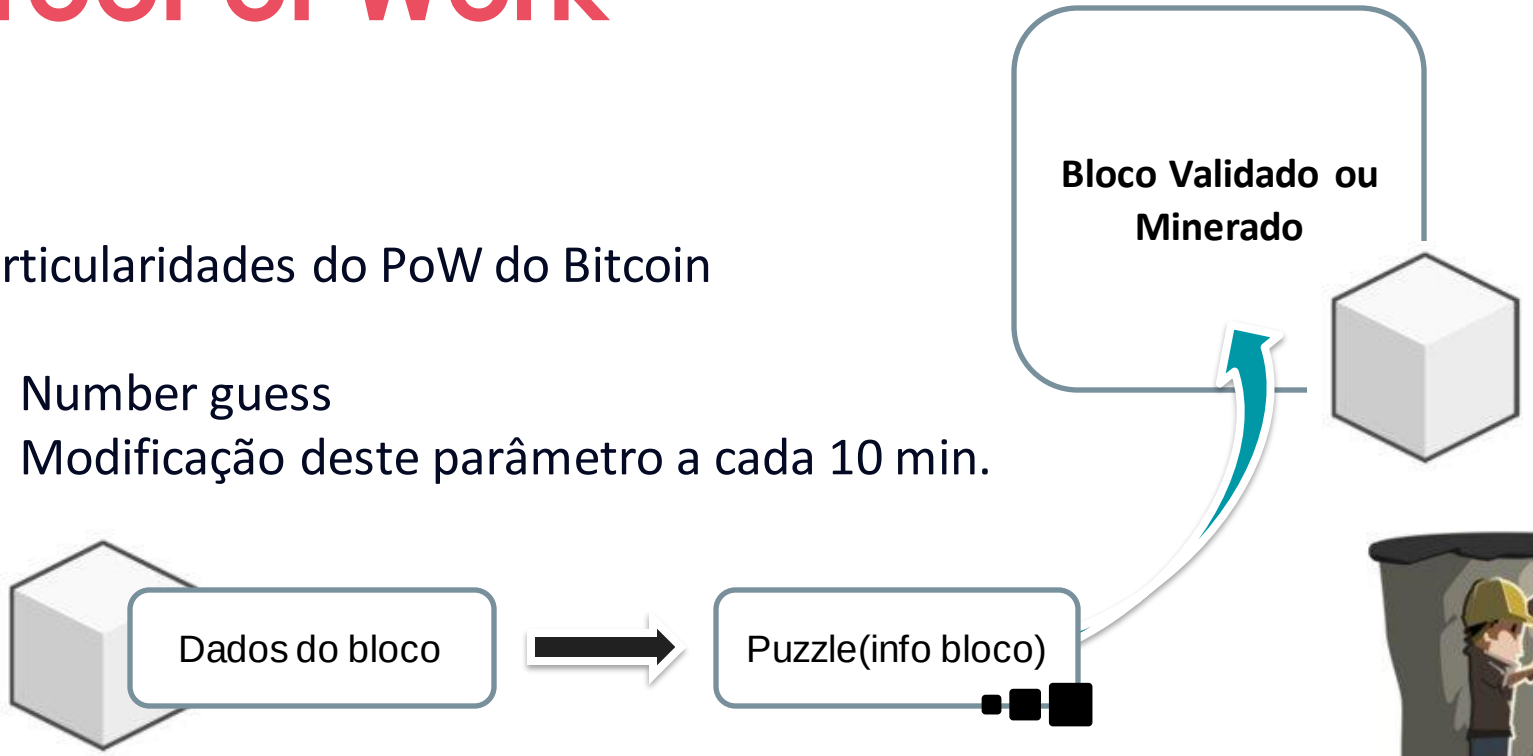
Rede Rejeita



Proof of Work

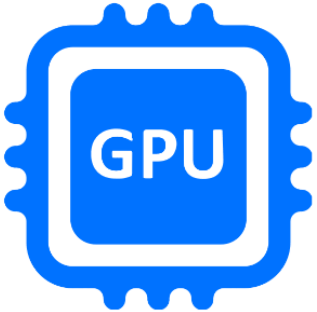
Particularidades do PoW do Bitcoin

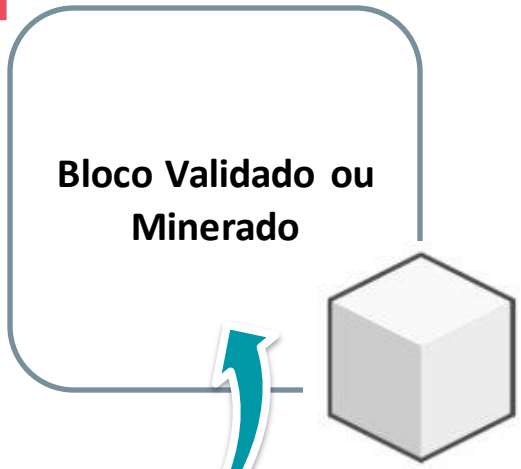
- Number guess
- Modificação deste parâmetro a cada 10 min.

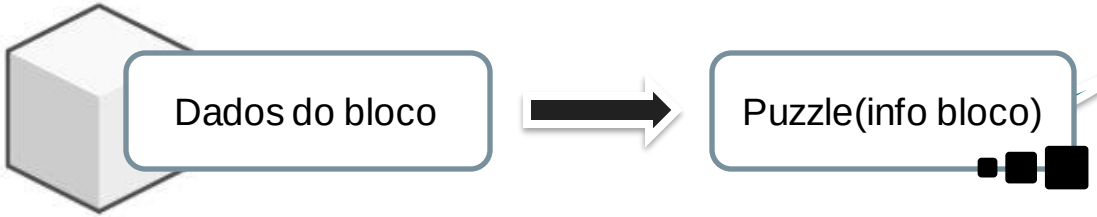


Sha256 - Criptografia

- Output – 256 bits hash
- One-way: **sem decode**
- SHA-256 (NSA)
- SHA-2: double

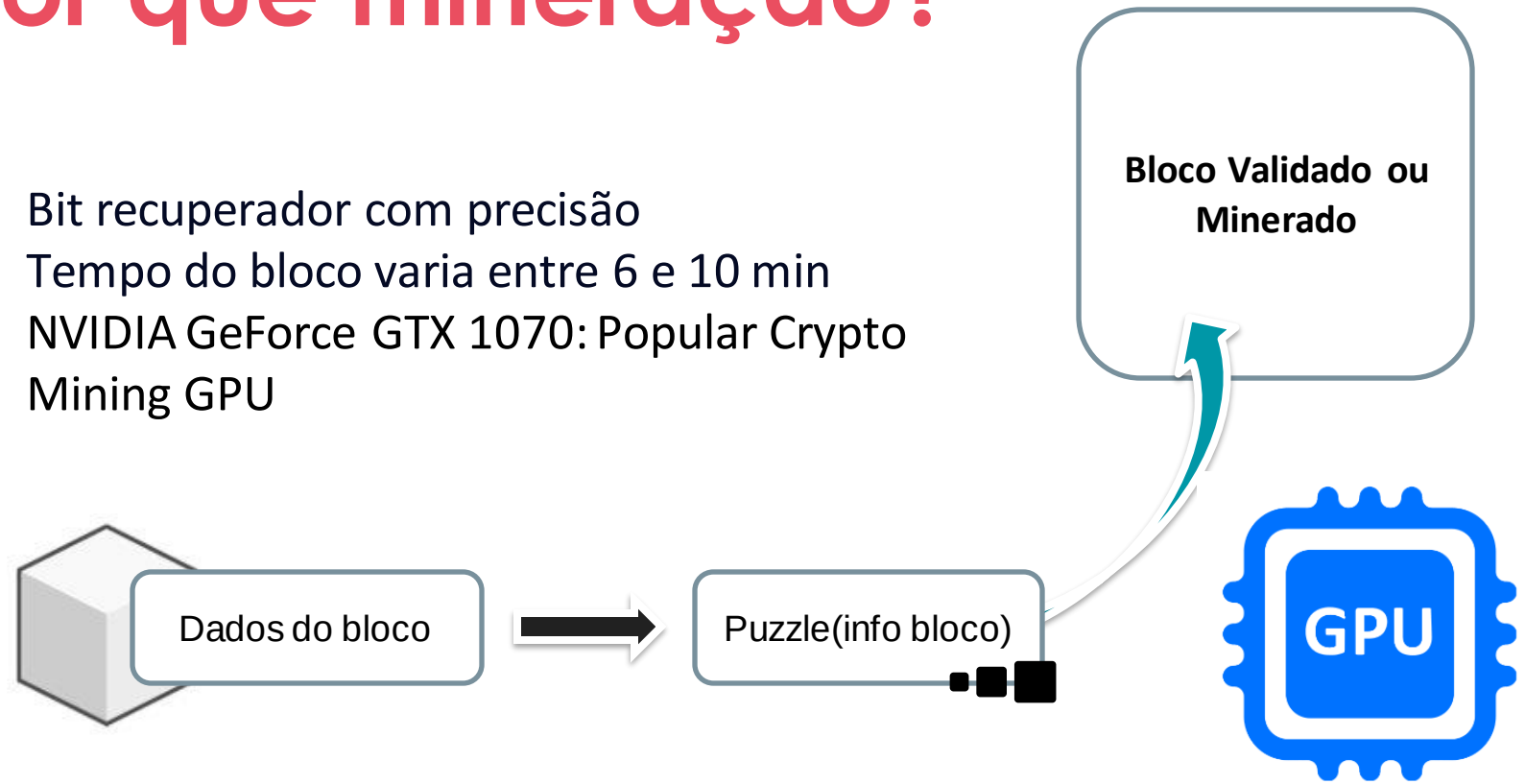






Por que mineração?

- Bit recuperador com precisão
- Tempo do bloco varia entre 6 e 10 min
- NVIDIA GeForce GTX 1070: Popular Crypto Mining GPU



Etapa 5

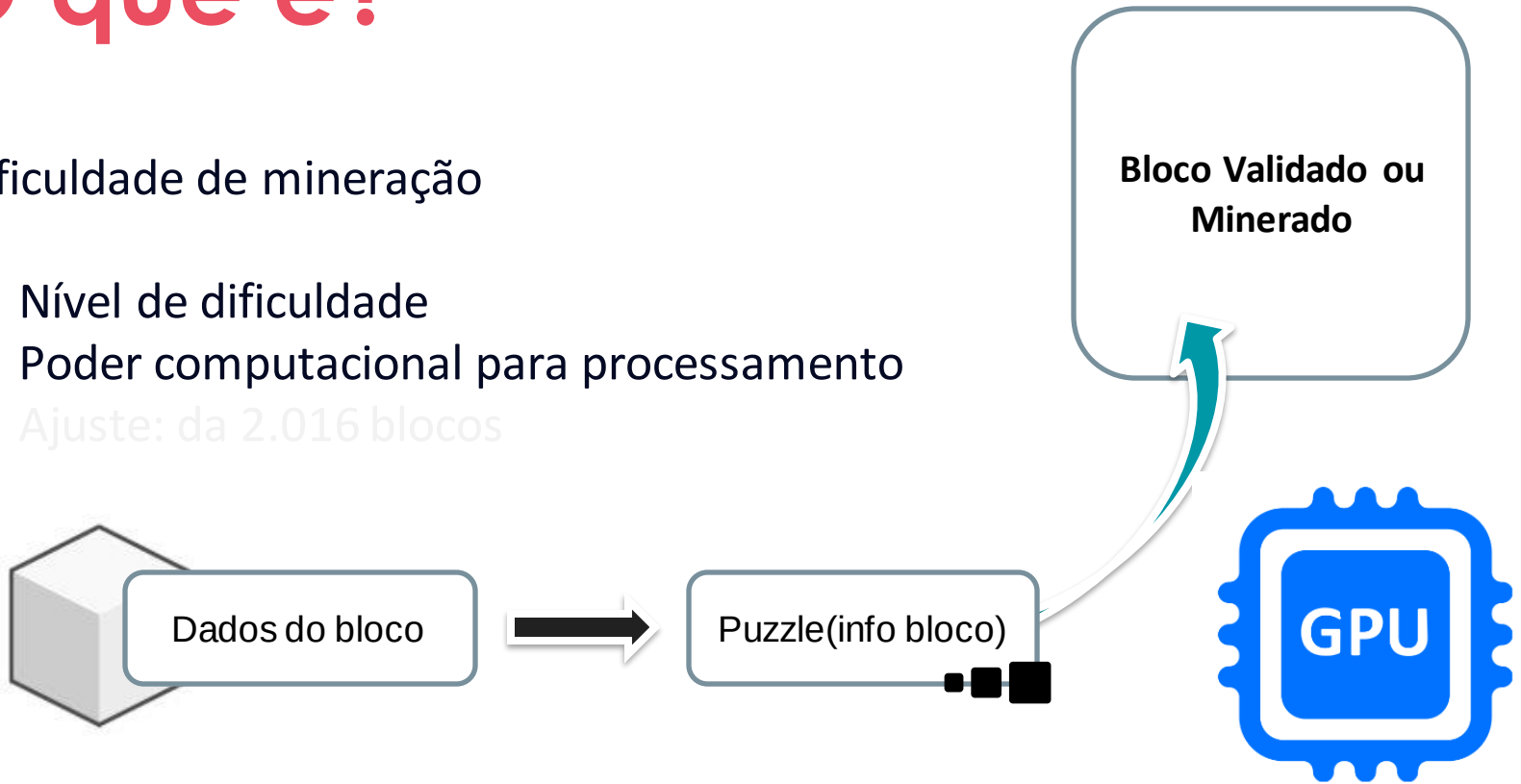
Adaptação da rede – dificuldade de Mineração

//Fundamentos da Blockchain/Cryptocurrencies: Bitcoin

O que é?

Dificuldade de mineração

- Nível de dificuldade
- Poder computacional para processamento
- Ajuste: da 2.016 blocos

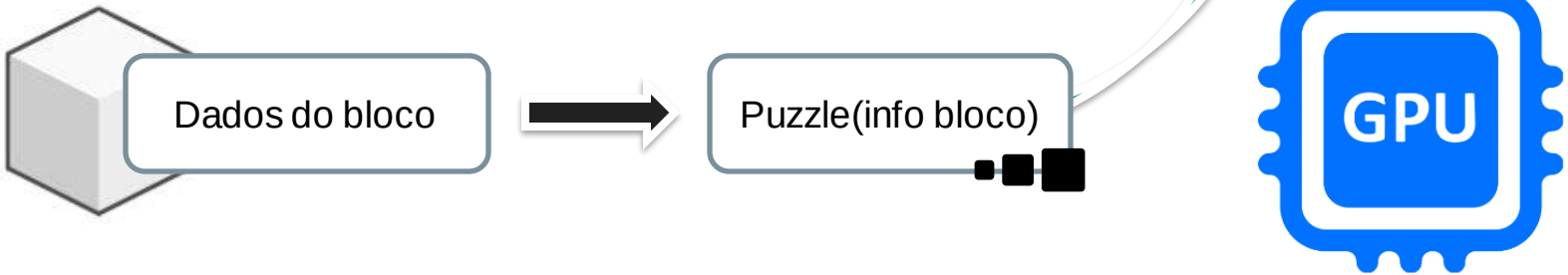


O que é?

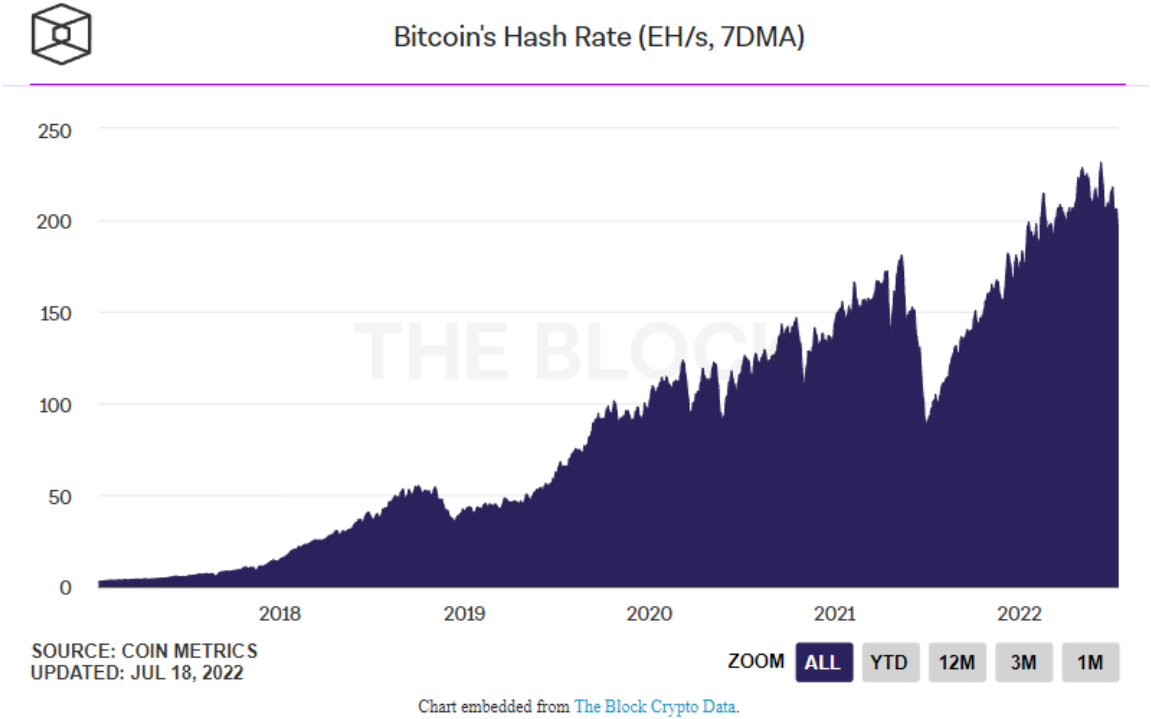
Problema matemático

Dificuldade de mineração

- Nível de dificuldade
- Poder computacional para processamento
- Ajuste: da 2.016 blocos



O que é?


Bitcoin's Hash Rate (EH/s, 7DMA)
250
200
150
100
50
0
2018
2019
2020
2021
2022
SOURCE: COIN METRICS
UPDATED: JUL 18, 2022
ZOOM
ALL
YTD
12M
3M
1M
Chart embedded from The Block Crypto Data.

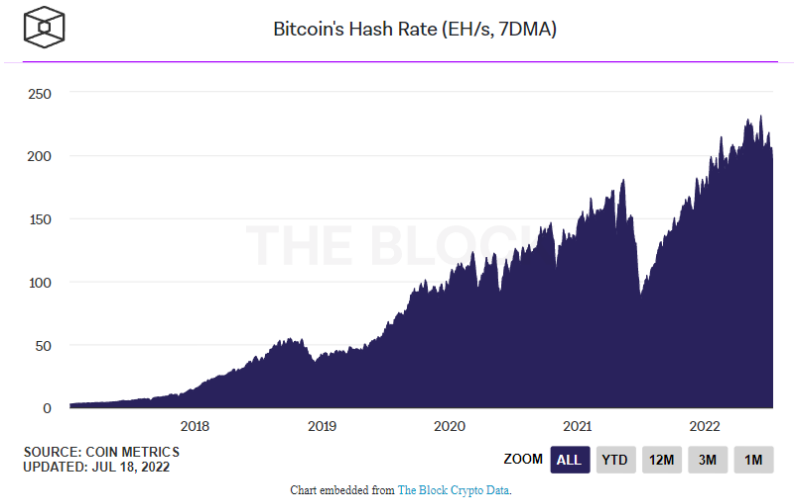
O que é?

História recente

- 25/05/20: 4.33%

Probição pela China

- 4.81% de queda



O que é?

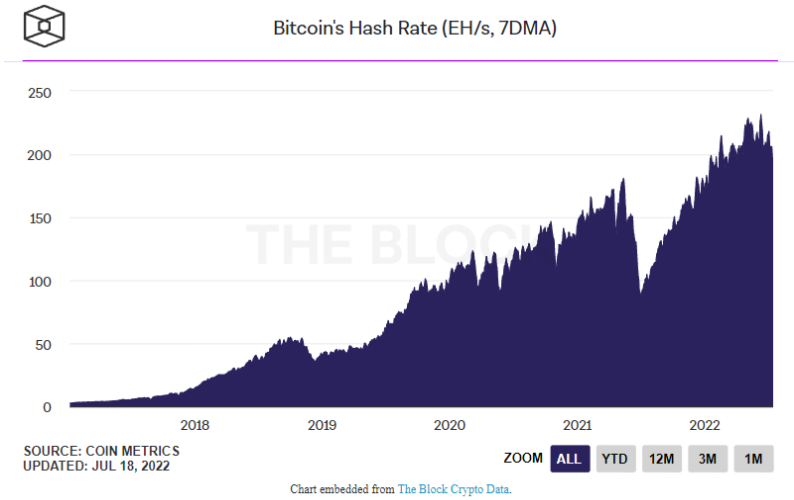
31,25 T (trilhões de hashes) ⇨ 29,90T

História recente

- 25/05/20: 4.33% ⇩

Probição pela China

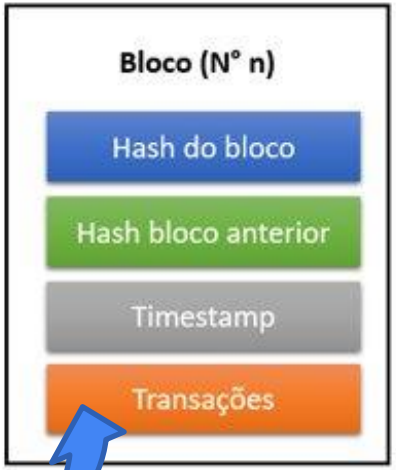
- 4.81% de queda

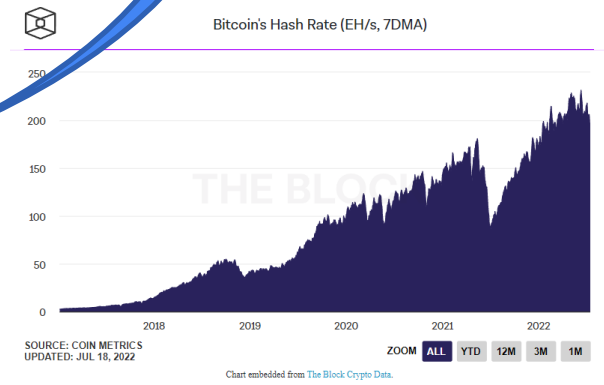


Atrelada ao Hash rate

Por que?

- Prazo para criação do bloco





https://explorer.btc.com/btc/insights-difficulty

Etapa 6

Bifurcações e Forks no Bitcoin

//Fundamentos da Blockchain/Cryptocurrencies: Bitcoin

Hard Forks

https://bitcoincash.org/

BitcoinCash

https://bitcoingold.org/

BITCOINGOLD

https://litecoin.org/

QUANTUM BLOCKCHAINS

https://www.quantumblockchains.io/

Hard Forks

https://bitcoincash.org/

HARD FORK BITCOIN CASH

- Forked at block 478558,
- Hard Fork em 2017
- 1 BTC = BCH

Alto custo (taxas) do Bitcoin

Tempo de processamento

Busca escalabilidade e baixo custo

Hard Forks

https://bitcoingold.org/

BITCOINGOLD

HARD FORK BITCOIN GOLD

- Forked at block 491407
- Hard fork em 2017/2018
- 1 BTC = 1 BTG

Poder nas mãos de poucos

Anonimato completo

Redução de tempo e tamanho de blocos

Hard Forks

https://litecoin.org/

HARD FORK LITECOIN

- Hard fork gerado em 2011
- Objetivo: + rapidez na confirmação das transações

- Mecanismo PoW - Tenebrix

Validação de transações + rápida

Quantidade em circulação

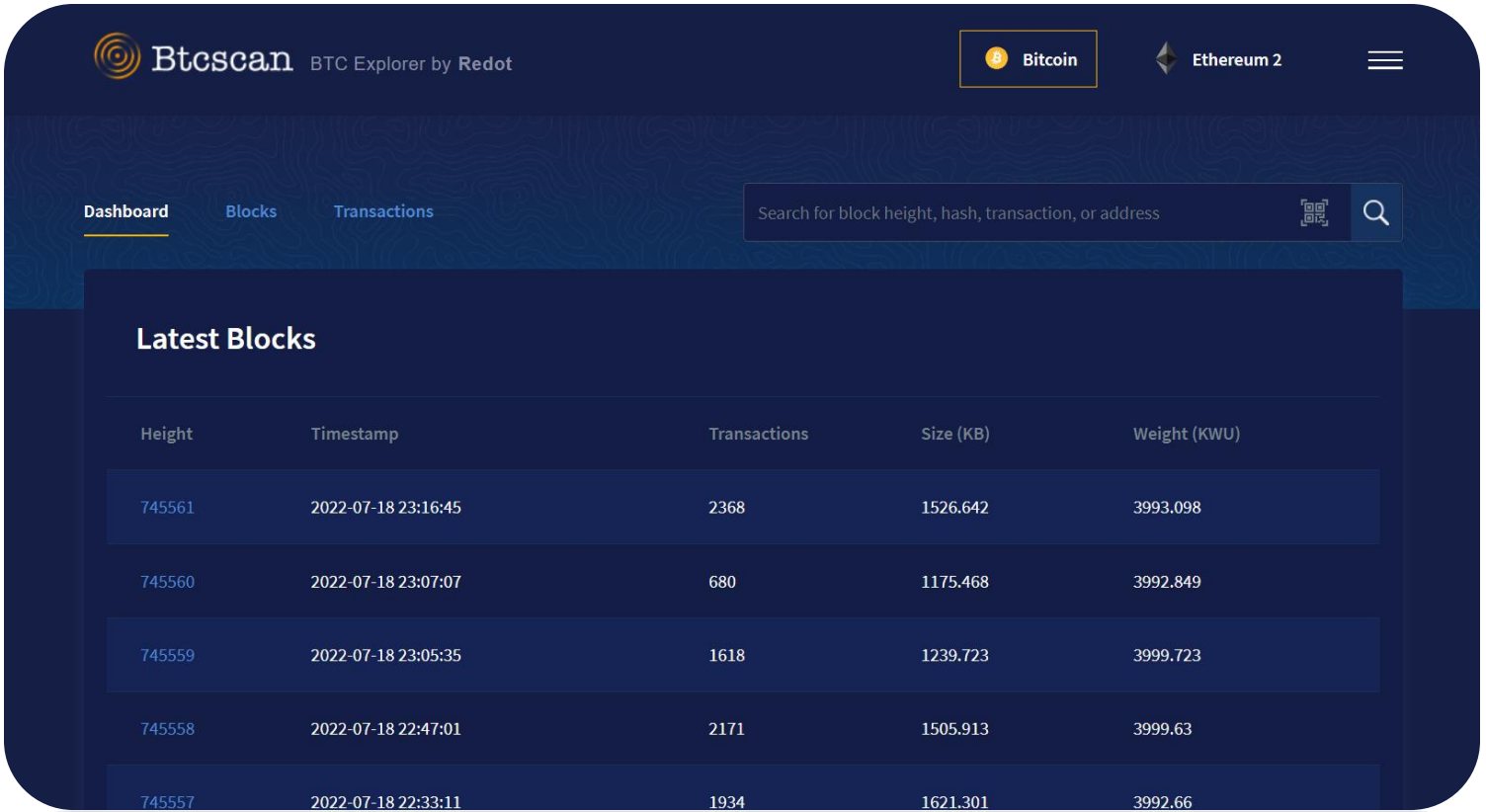
Menor taxação nas transações

Etapa 9

Analisando as Transações do Bitcoin

//Fundamentos da Blockchain/Cryptocurrencies: Bitcoin

https://btcscan.org/



Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)

Para saber mais

Bitcoin: A Peer-to-Peer Electronic Cash System

https://www.blockchain.com/charts/mempool-size

https://criptonizando.com/bitcoin-consome-mais-energia-que-um-pais-com-100-milhoes-de-pessoas/

https://www.cnnbrasil.com.br/business/conheca-o-blockchain-verde-opcao-que-reduz-uso-de-energia-e-de-emissoes-da-rede/

https://www.nasdaq.com/articles/what-to-do-if-your-bitcoin-transaction-gets-stuck-2016-12-06

Para saber mais

https://coinmarketcap.com/alexandria/article/what-is-gpu-mining

https://portaldobitcoin.uol.com.br/dificuldade-de-mineracao-do-bitcoin-tem-pior-ajuste-em-nove-meses-e-cai-43/

https://www.moneytimes.com.br/dificuldade-para-minerar-bitcoin-btc-tem-maior-queda-desde-julho-de-2021/#:~:text=O%20que%20%C3%A9%20a%20dificuldade,dificuldade%2C%20maior%20o%20poder%20computacional

https://coinext.com.br/blog/o-que-e-fork-do-bitcoin