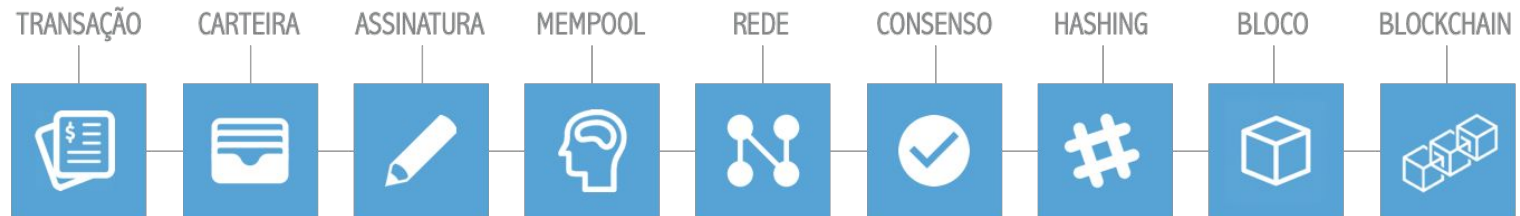


IMD0913

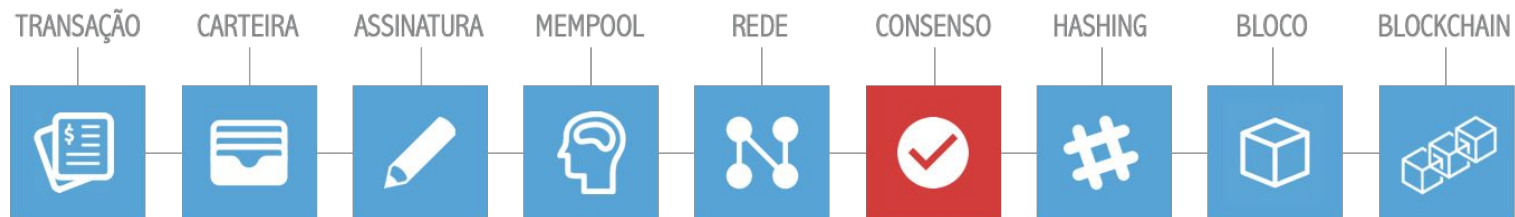
ARQUITETURA DE UM BLOCKCHAIN

CONSENSO: PROOF-OF-WORK

ARQUITETURA DE UM **BLOCKCHAIN**



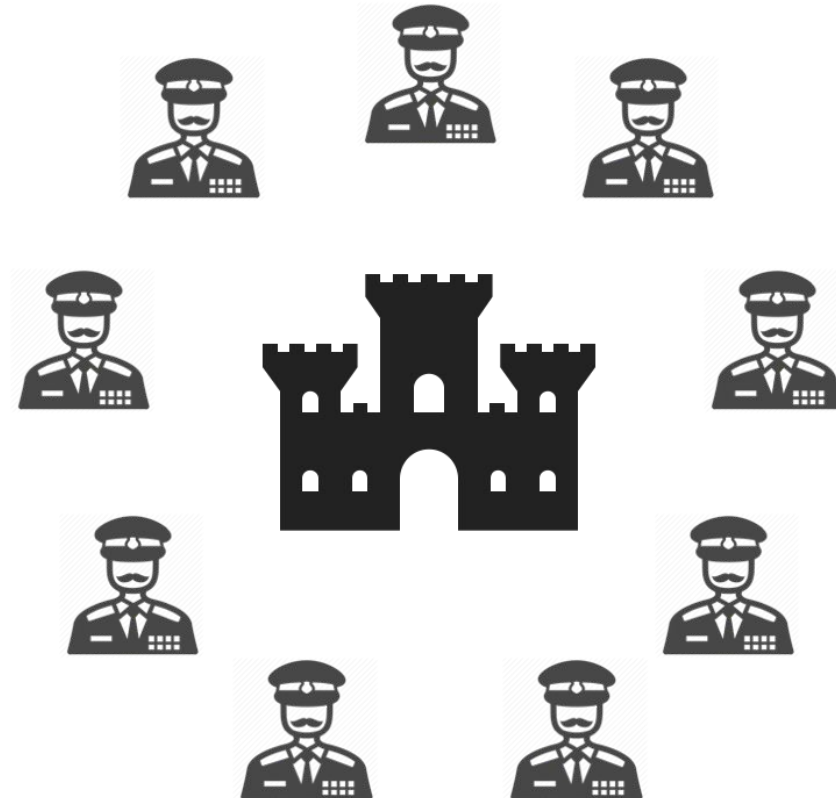
ARQUITETURA DE UM **BLOCKCHAIN**



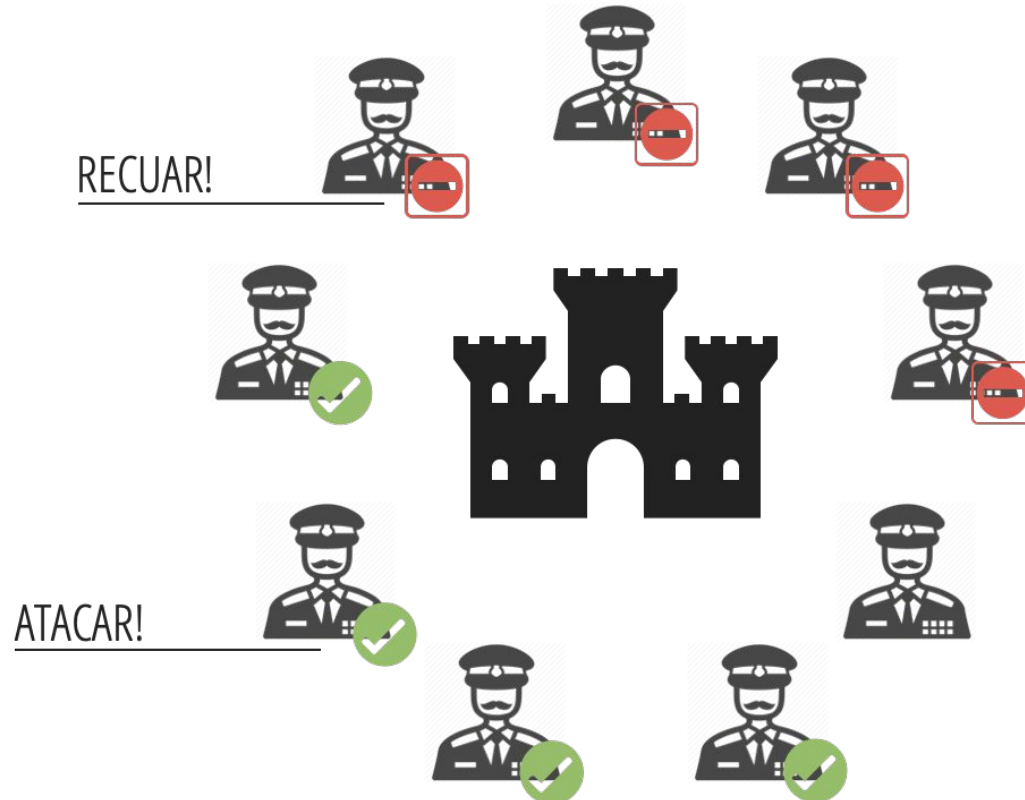
Consenso

Como a rede concorda sobre quais transações são confiáveis.

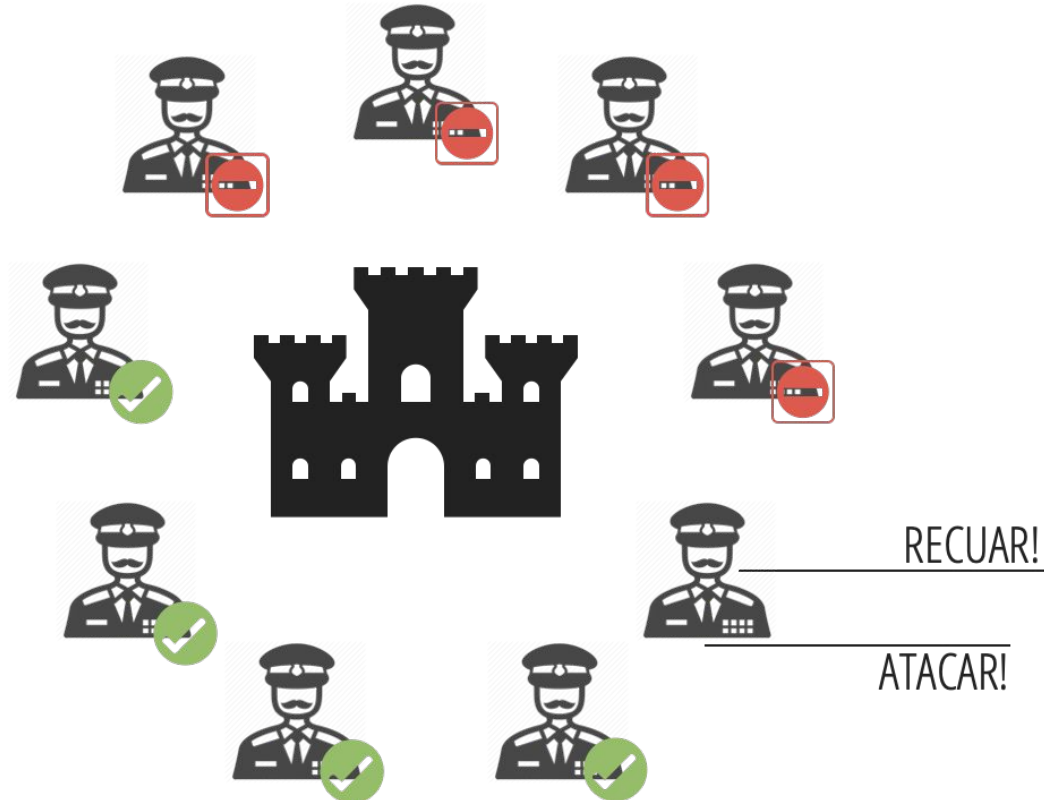
Problema dos Generais Bizantinos



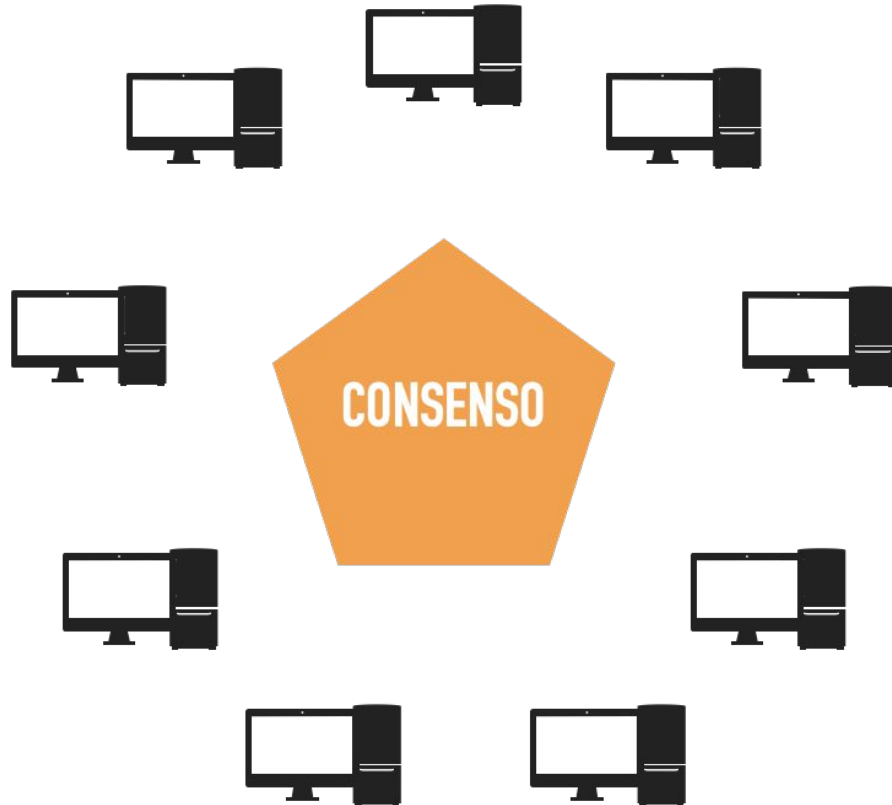
Problema dos Generais Bizantinos



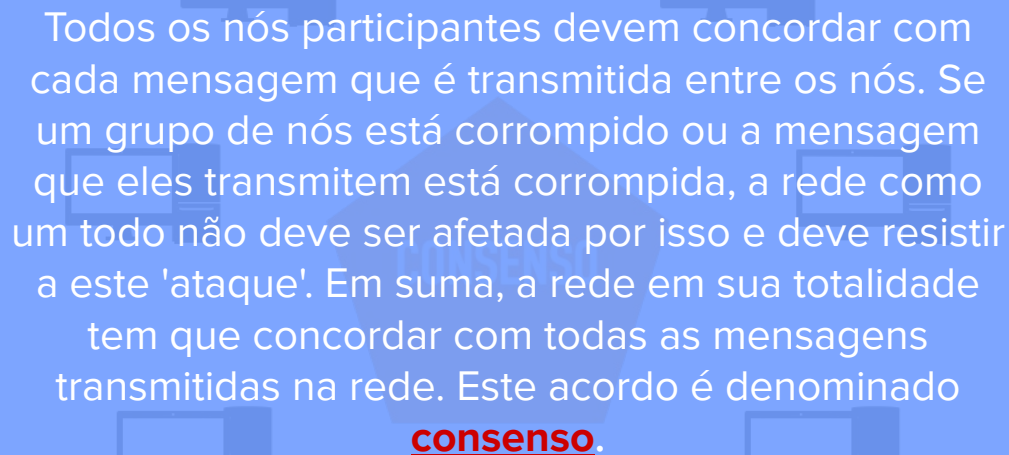
Problema dos Generais Bizantinos



Problema dos Generais Bizantinos



Problema dos Generais Bizantinos

A diagram illustrating a network of nodes. At the top, there are three computer icons. In the center, a large blue rectangular box contains text. At the bottom, there are two computer icons. The text inside the box describes the Byzantine Generals problem and the concept of consensus.

Todos os nós participantes devem concordar com cada mensagem que é transmitida entre os nós. Se um grupo de nós está corrompido ou a mensagem que eles transmitem está corrompida, a rede como um todo não deve ser afetada por isso e deve resistir a este 'ataque'. Em suma, a rede em sua totalidade tem que concordar com todas as mensagens transmitidas na rede. Este acordo é denominado **consenso**.

Proof-of-Work (PoW)

Sistema em que a informação deve ser custosa para ser produzida, mas fácil de ser verificada.

Mineração

Minerar é o processo de adicionar transações (organizado em um bloco) no blockchain.

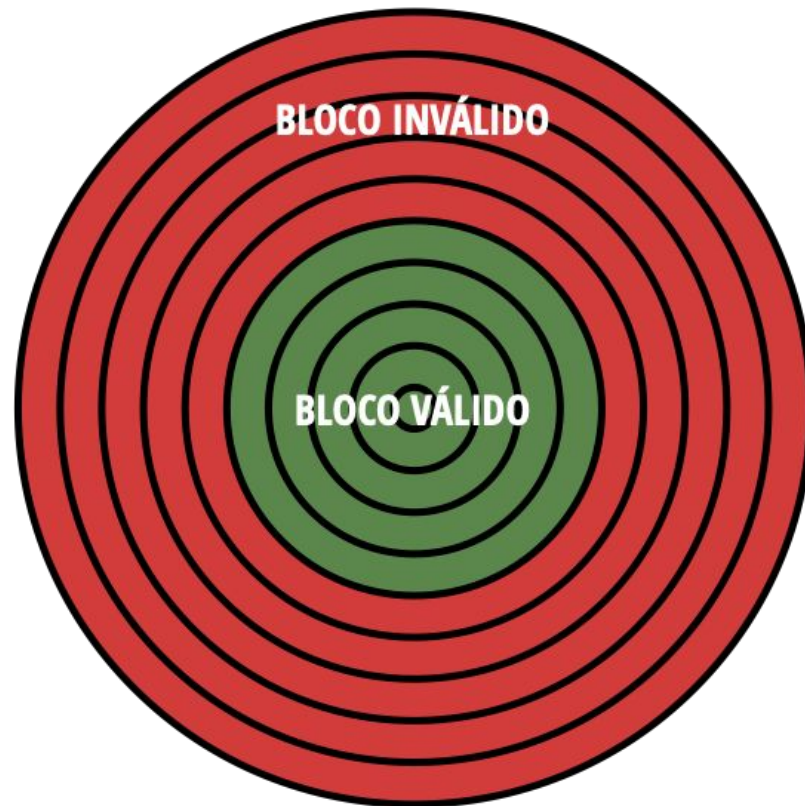
Proof-of-Work

Minerar é como jogar dardos em um alvo com os olhos vendados:

Probabilidade igual de atingir qualquer parte do alvo;

Lançadores velozes = mais acertos/segundo

Mineradores procuram por um *hash* abaixo de um alvo decidido por um algoritmo

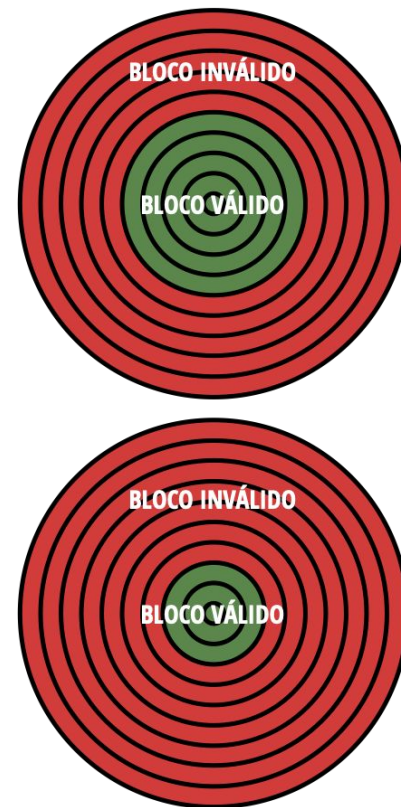


Dificuldade

Representação do número de computações esperados para achar um bloco válido

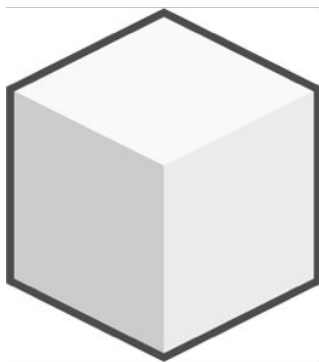
De maneira mais simples: quantidade de 0's mais significativos

Ajusta a cada 2016 blocos (~2 semanas)



Dificuldade

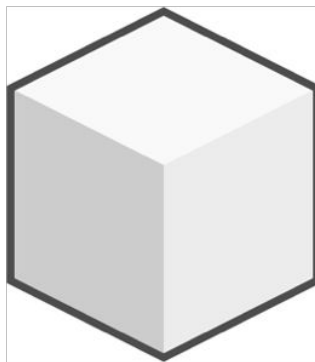
muito rápido...



0 →

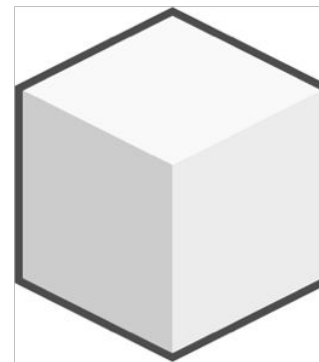
aumenta a
dificuldade

10 minutos



00

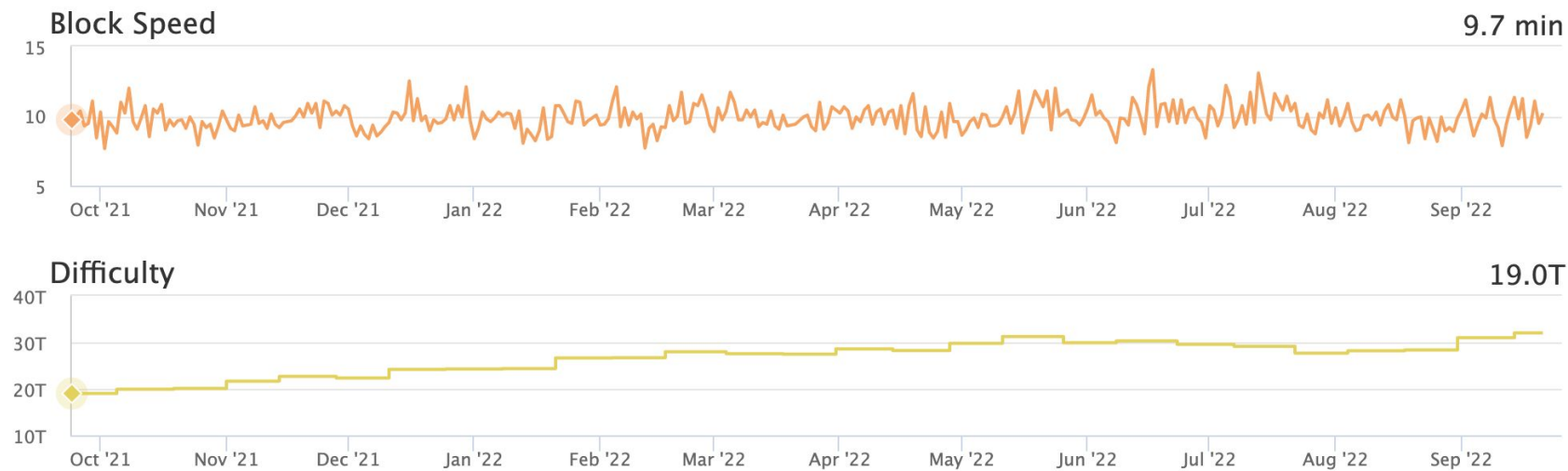
muito devagar...



← 000

diminui a
dificuldade

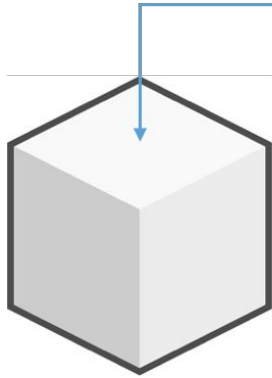
Dificuldade



Dificuldade

target bits
0x171ba3d1

Dificuldade



target bits
0x171ba3d1

Dificuldade

0x1903a30c

$$\text{alvo} = \text{coeficiente} * 2^{(8 * (\text{expoente} - 3))}$$

coeficiente = 0x03a30c

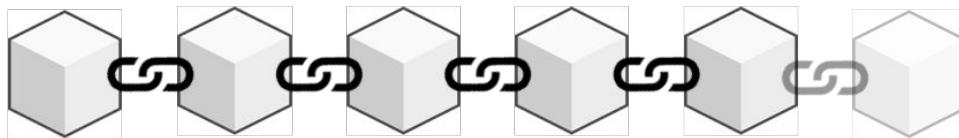
expoente = 0x19

PoW

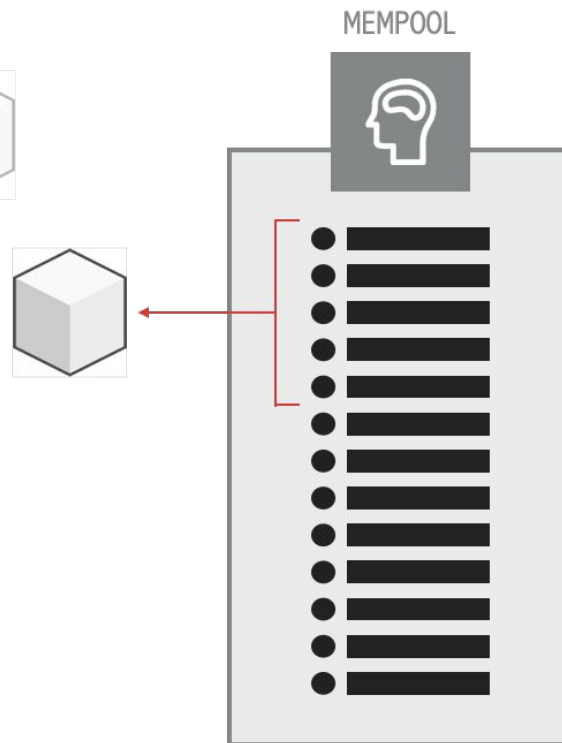
<https://andersbrownworth.com/blockchain/block>

Mineração - PoW

Blockchain

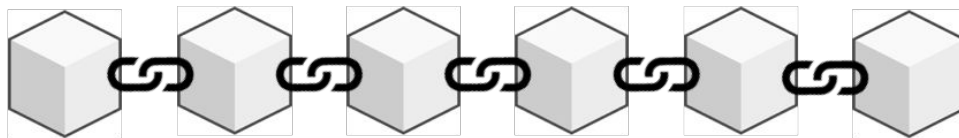


Nós da rede



Mineração - PoW

Blockchain



Nós da rede

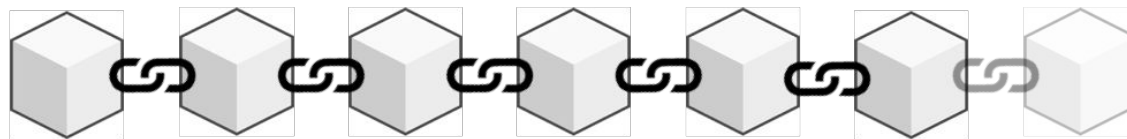


MEMPOOL

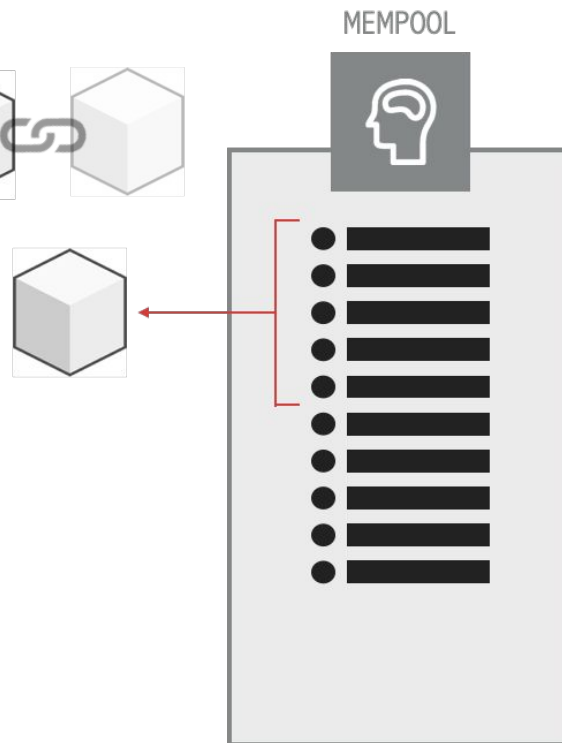


Mineração - PoW

Blockchain



Nós da rede





1

Um usuário cria uma transação



2

A transação é incluída em um bloco que é minerado



3

O bloco se difunde para todos os nós da rede



4

Todos os nós recebem e validam o bloco



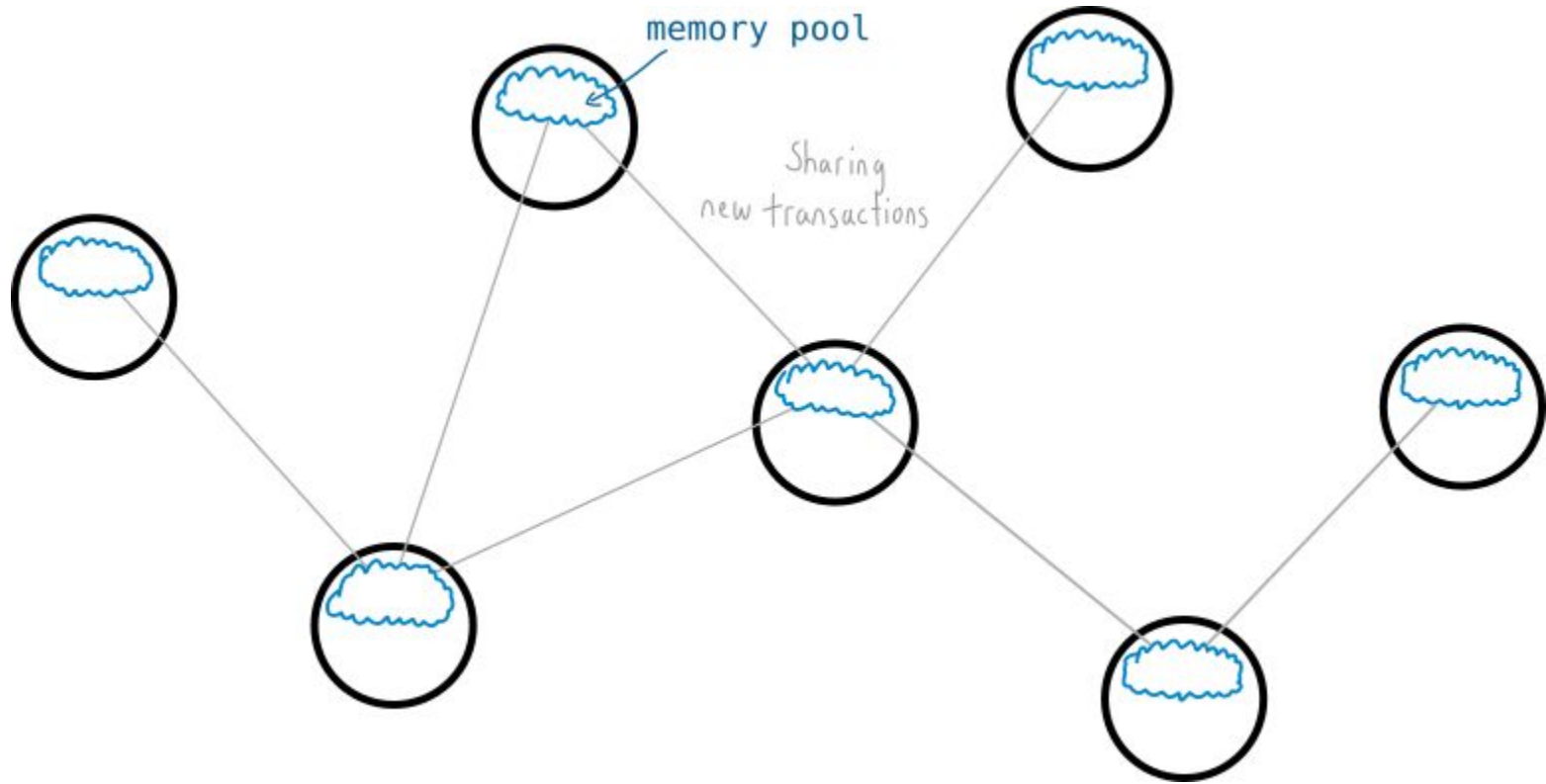
5

O bloco é adicionado ao blockchain

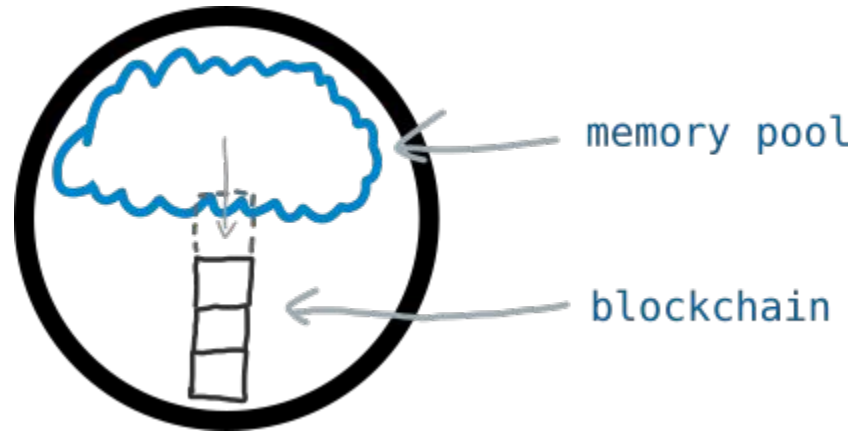


6

A transação é verificada e validada



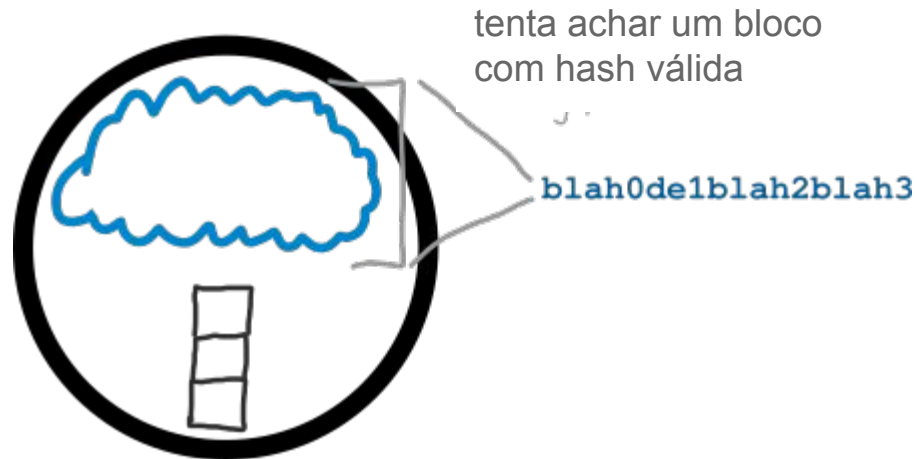
Todo nó compartilha informação sobre novas transações. Elas são armazenadas no *memory pool*.



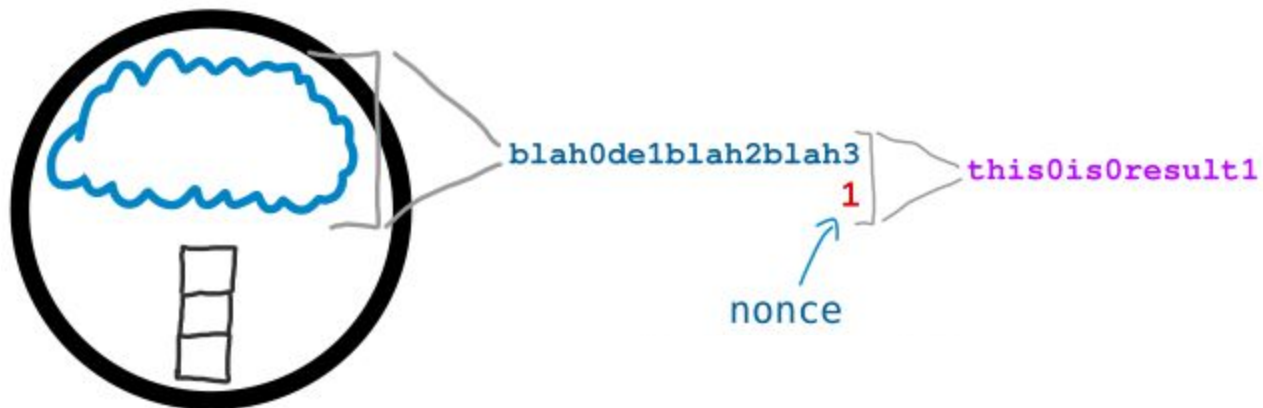
Cada nó tem a opção de tentar minerar transações do seu *memory pool* (em um bloco).

No entanto, para adicionar transações do *memory pool* ao blockchain, um nó precisa usar muito poder de processamento.

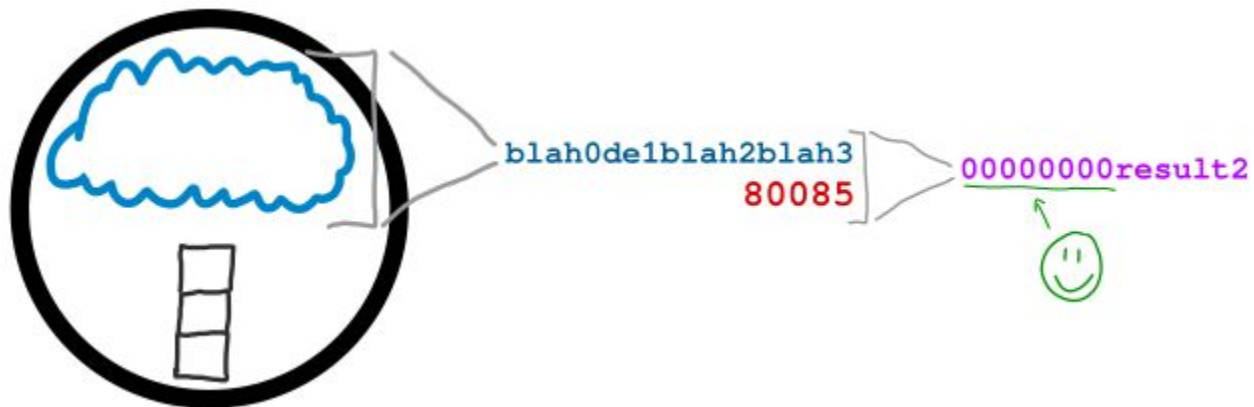
Esse poder de processamento é forçado pela existência de um desafio criptográfico para criar um bloco considerado válido.

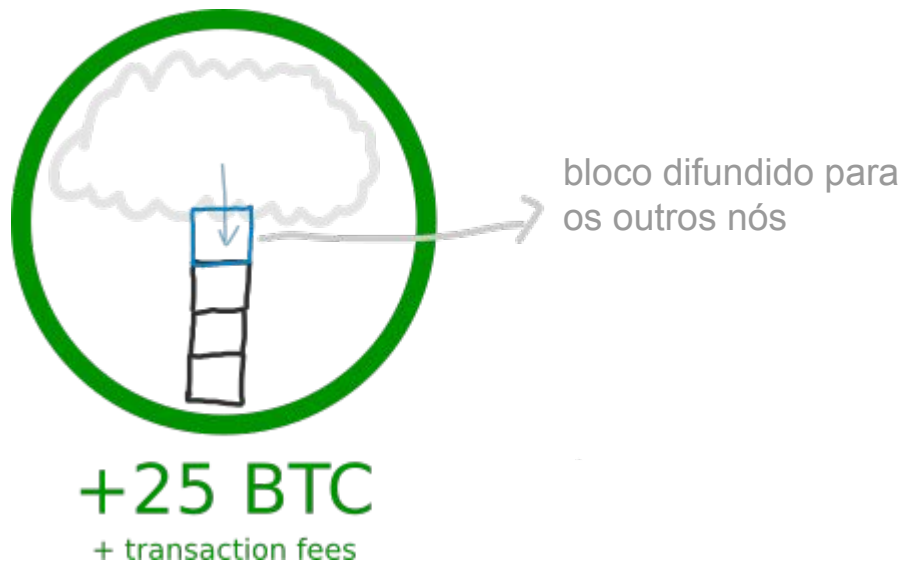


Cada nó minerador "monta" o seu bloco candidato, e começa a tentar achar uma *hash* que atenda os requisitos de dificuldade da rede.



...





Se você tiver a sorte de encontrar uma *hash* bem-sucedida, o seu bloco será adicionado ao blockchain e todos os outros nós da rede adicionarão seu bloco de transações ao blockchain deles. Você também receberá uma recompensa (atualmente, 6,25 BTC) por seu esforço, além de receber quaisquer taxas que foram adicionadas às transações que você acabou de adicionar ao blockchain.

Por que a mineração é necessária?

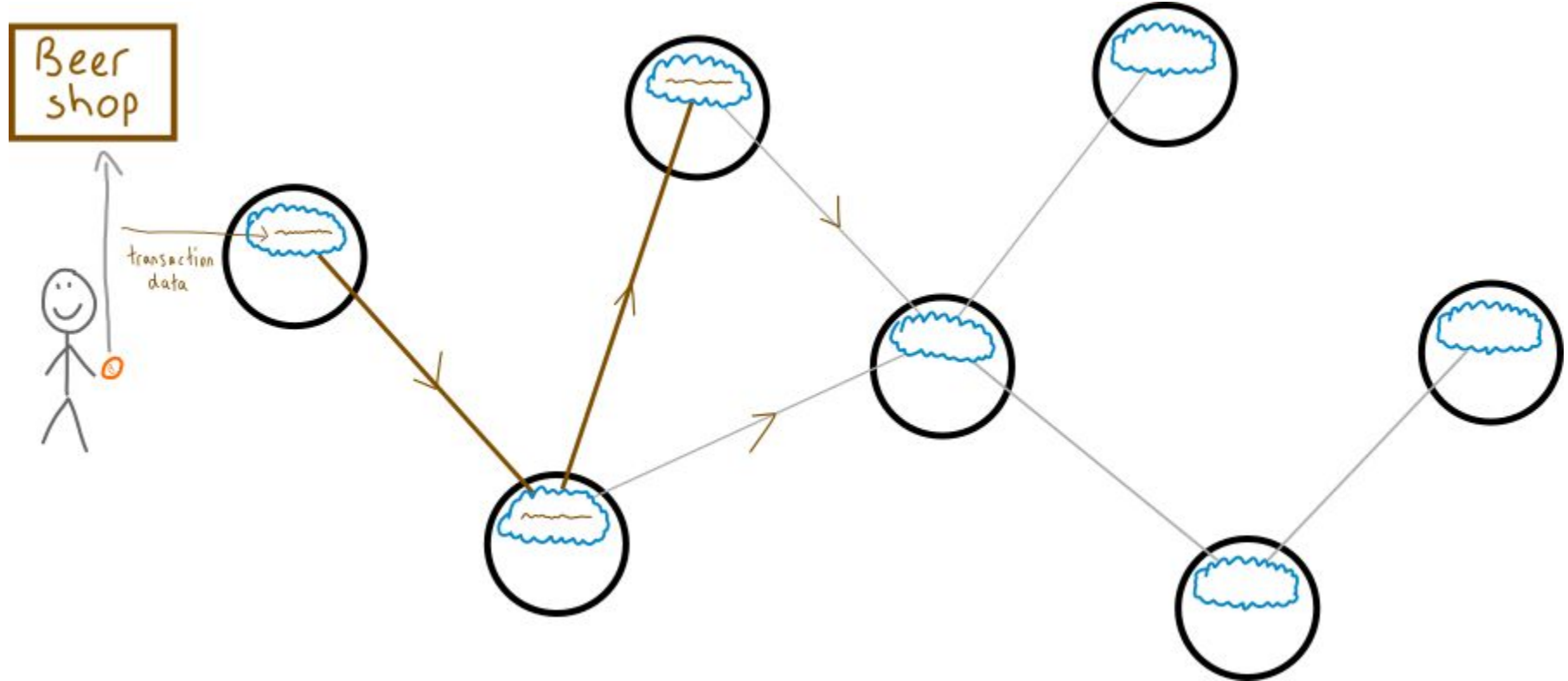
Por que não adicionar as transações diretamente no blockchain?

Porque a mineração permite que toda a rede Bitcoin concorde sobre quais transações são “arquivadas”, e é assim que você evita fraudes em uma moeda digital.

Por exemplo...

Quando você faz uma **transação** Bitcoin, os nós na rede não ouvem sobre isso instantaneamente. Em vez disso, as transações viajam pela rede Bitcoin sendo **propagadas** de um nó para o próximo.

Por exemplo...

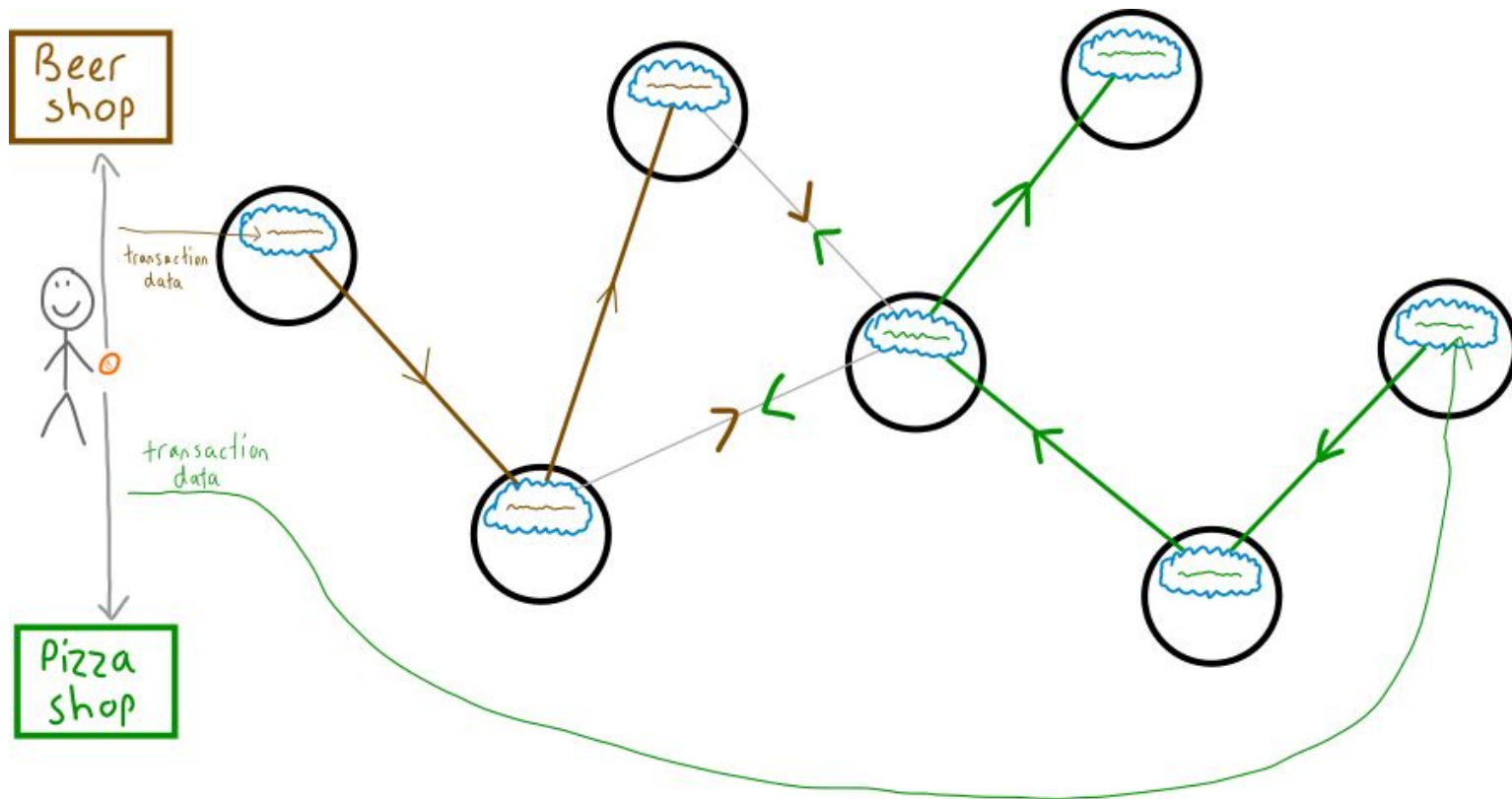


Por exemplo...

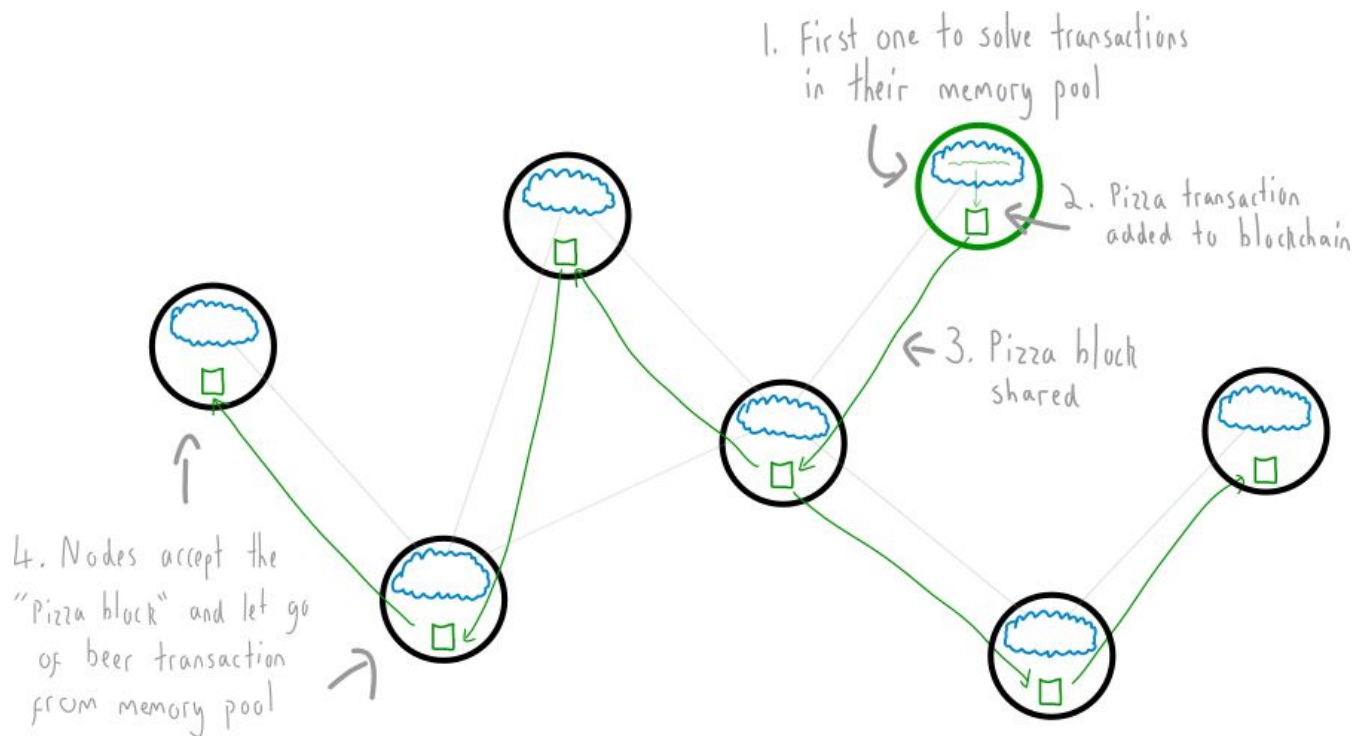
No entanto, é possível fazer outra transação usando esses mesmos Bitcoins (mesmos UTXOs!) e inserir essa transação na rede também. Por exemplo, você pode comprar uma cerveja com alguns BTCs e tentar rapidamente comprar uma fatia de pizza com esses mesmos BTCs também.

Em outras palavras, a velha **fraude**.

Por exemplo...



Como a rede se decidiria?



Se um nó com a transação de pizza for incluída em um bloco com sucesso, então essa é a transação que é adicionada ao blockchain, e a transação de cerveja é excluída da rede.

Outro benefício da mineração...

Se você quiser tentar controlar os blocos (ou seja, as transações) que são adicionados ao blockchain, você precisa **competir** para resolver *puzzles* criptográficos para criar blocos com todos os outros nós de mineração na rede Bitcoin.

Em outras palavras, você precisa ter poder de processamento suficiente que seja capaz de superar o poder de processamento combinado de todos os outros mineradores de Bitcoin (**ataque de 51%**).

O que é totalmente possível – você só precisa gastar alguns bilhões em *hardware* e pronto (embora esse número aumente a cada novo minerador que se junta à rede).

Coinbase

Criar blocos válidos custa:

energia

tempo

dinheiro



Recompensa! \$\$\$

Única maneira onde novos “bitcoins” são **criados**

Ou seja, UTXOs não são consumidos!

Coinbase

<https://www.blockchain.com/explorer/blocks/btc/755780>

Coinbase

Qual é essa recompensa? Começou com **50 BTC**...

Satoshi Nakamoto definiu que **a cada 210.000 blocos minerados**, a recompensa seria diminuída pela metade (chamado de ***halving***)

Novembro/2012: 25 BTC

Julho/2016: 12,5 BTC

Maio/2020: 6,25 BTC

~Março/2024: 3,125 BTC



Taxa de transação

A maioria das transações incluem ***transactions fees*** para recompensar mineradores

Incentivo para que mineradores incluam sua transação em seu bloco candidato

Taxas de transação são recolhidas pelo minerador

$$\text{fees} = \text{sum}(\text{inputs}) - \text{sum}(\text{outputs})$$

Taxa de transação



Taxa de transação

Transaction View information about a bitcoin transaction

6abdd1a5f6067bd30c40f0bda4c6b0d48f27a425ec2afdaf9e69e23a6ab3b6a5

36KCNoPey8WzJcUwyabCu4V7K2hMwrxYt8



38J8VkVaq5MUQ1UpmCxi5AixfRmRmgRwwA
38bNQE3eUXa6zkbYji4Q71erEwjKUMMk1u

0.15 BTC

15.88415613 BTC

21 Confirmations

16.03415613 BTC

Summary	
Size	247 (bytes)
Weight	661
Received Time	2019-06-17 09:39:15
Included In Blocks	581096 (2019-06-17 09:40:18 + 1 minutes)
Confirmations	21
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	16.03476902 BTC
Total Output	16.03415613 BTC
Fees	0.00061289 BTC
Fee per byte	248.134 sat/B
Fee per weight unit	92.722 sat/WU
Estimated BTC Transacted	0.15 BTC
Scripts	Show scripts & coinbase

<https://www.blockchain.com/btc/tx/6abdd1a5f6067bd30c40f0bda4c6b0d48f27a425ec2afdaf9e69e23a6ab3b6a5>

Taxa de transação

<https://bitcoinfees.earn.com/>

Casos notáveis

<https://btc.com/cc455ae816e6cdafdb58d54e35d4f46d860047458eacf1c7405dc634631c570d>

<https://btc.com/7e8fce9686572d8308d8c40fa3cb96fdbf96c0787c147d3159c893fd560aabc7>

<https://btc.com/1a3a7e334d5d894c66830dadd2f94f22f64b0c3aa5fb4cc956ef6734f1bb98ab>

Taxas de transação, recompensa e Coinbase

