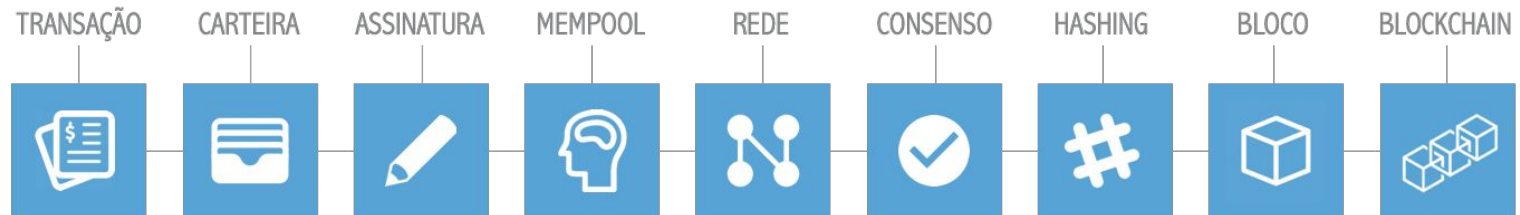


IMD0913

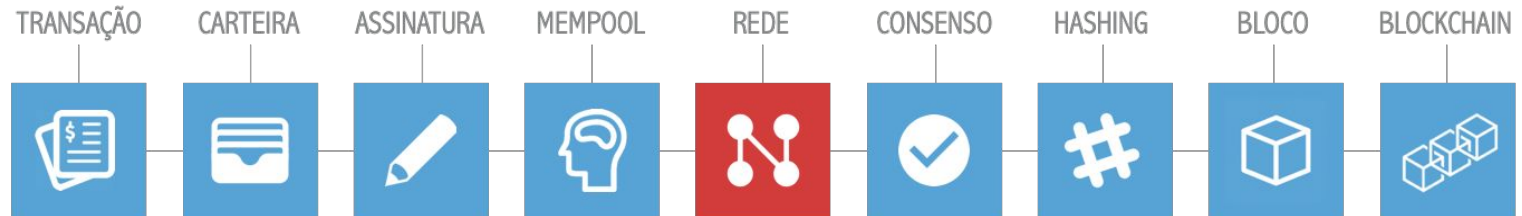
ARQUITETURA DE UM BLOCKCHAIN

REDE e MEMPOOL

ARQUITETURA DE UM **BLOCKCHAIN**



ARQUITETURA DE UM **BLOCKCHAIN**



Rede

Um *blockchain* é suportado por uma **rede distribuída *peer-to-peer***

Não existe o papel de servidor

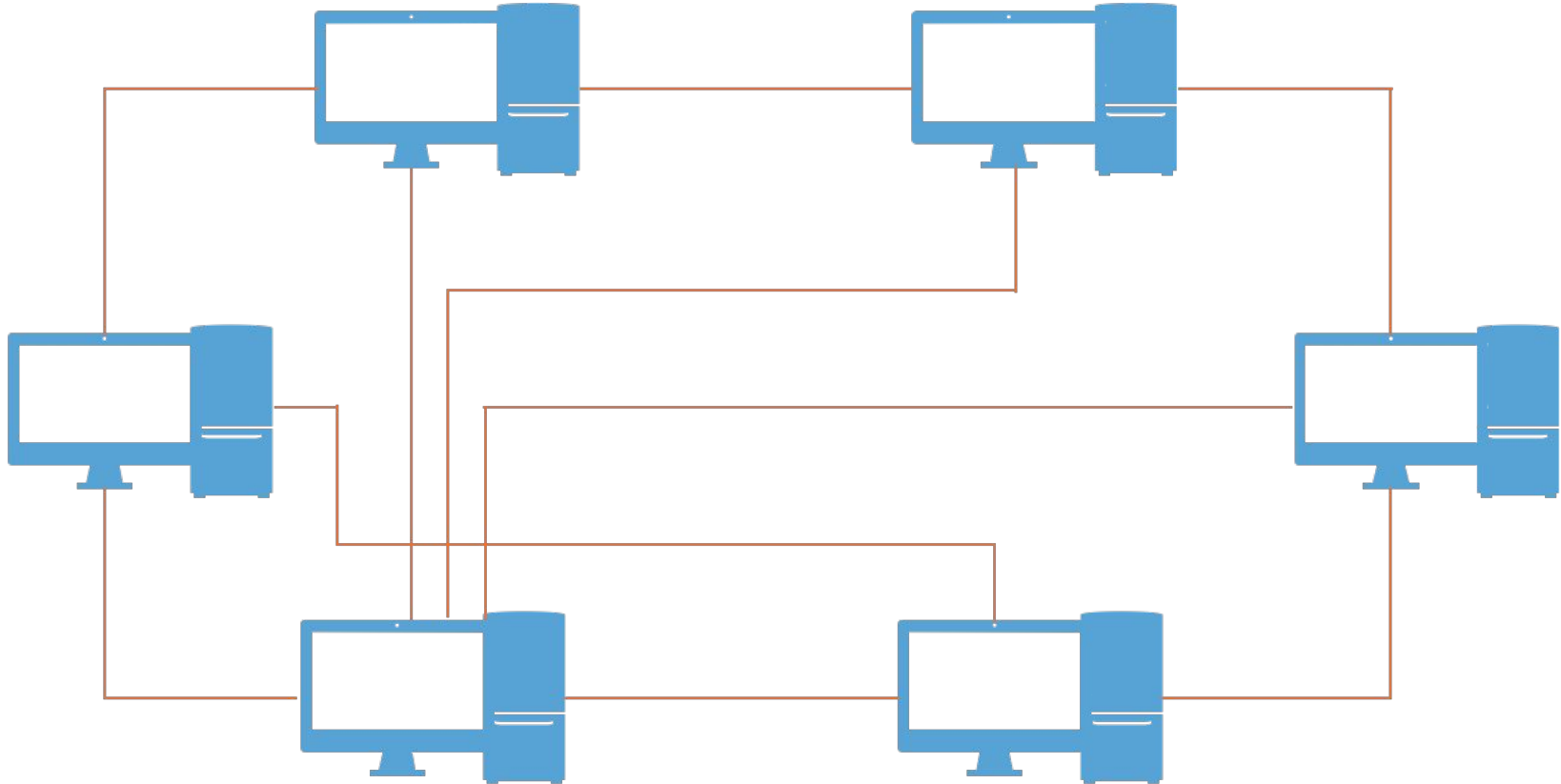
Não existe serviço centralizado

Não existe hierarquia na rede

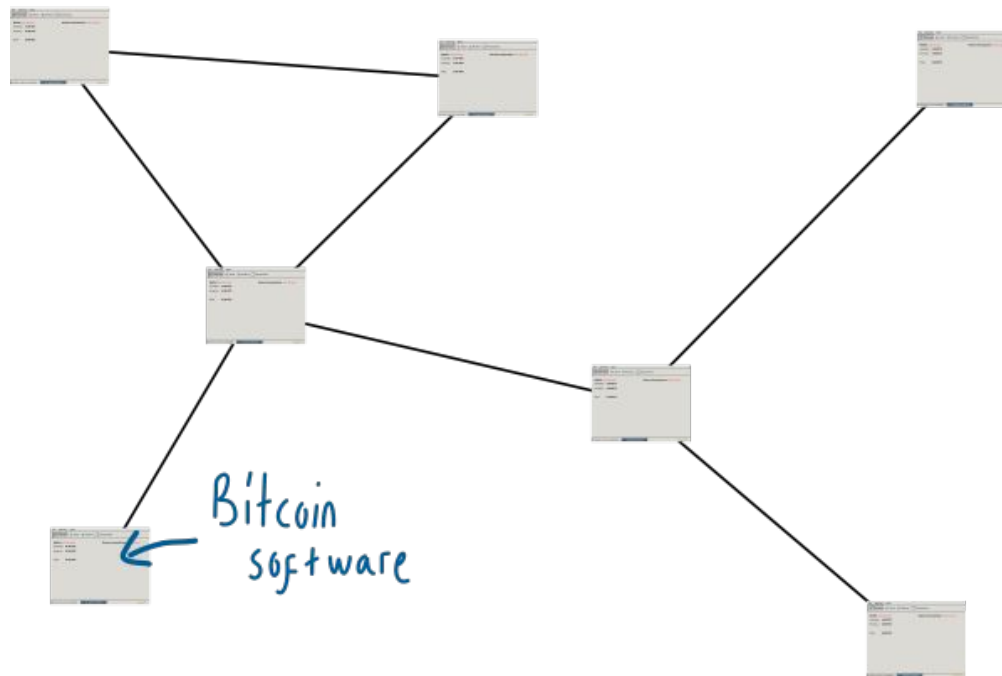
Rede Bitcoin se refere a coleção de nós executando o protocolo P2P Bitcoin

Rede P2P

Uma rede de computadores que permite dados serem compartilhados diretamente entre seus nós/usuários.

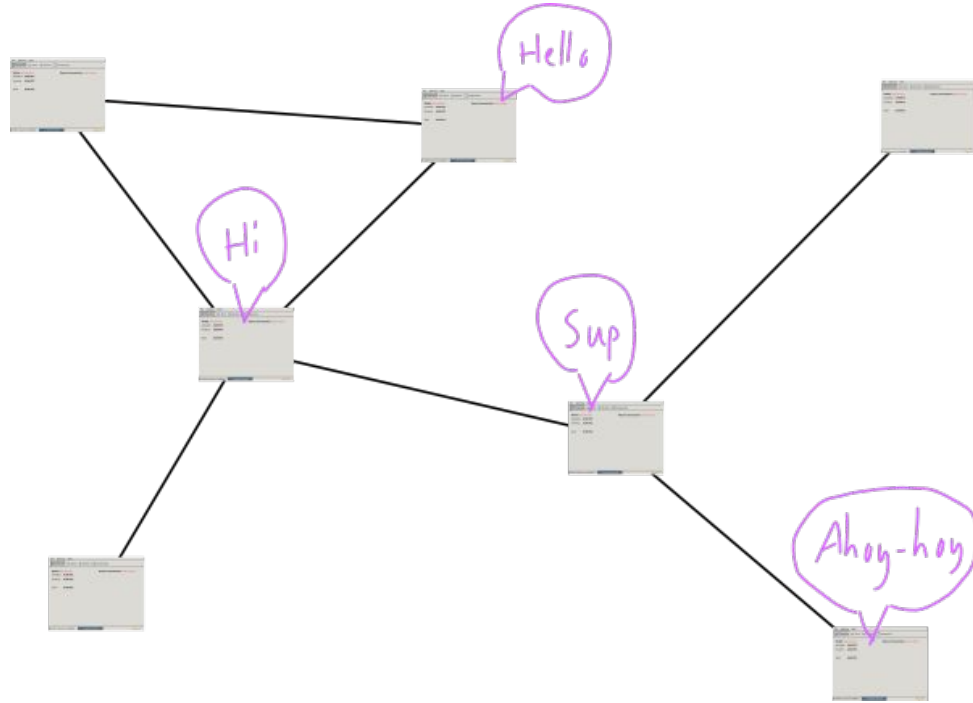


O que é a rede Bitcoin?



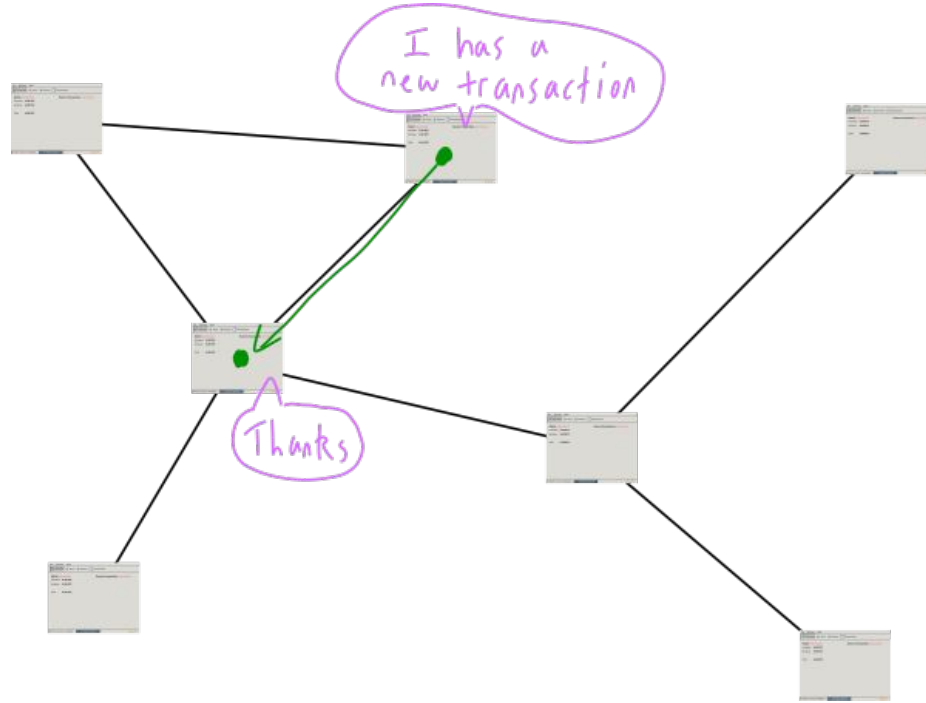
Bitcoin é uma rede de nós executando o mesmo programa de computador.

O que a rede faz?



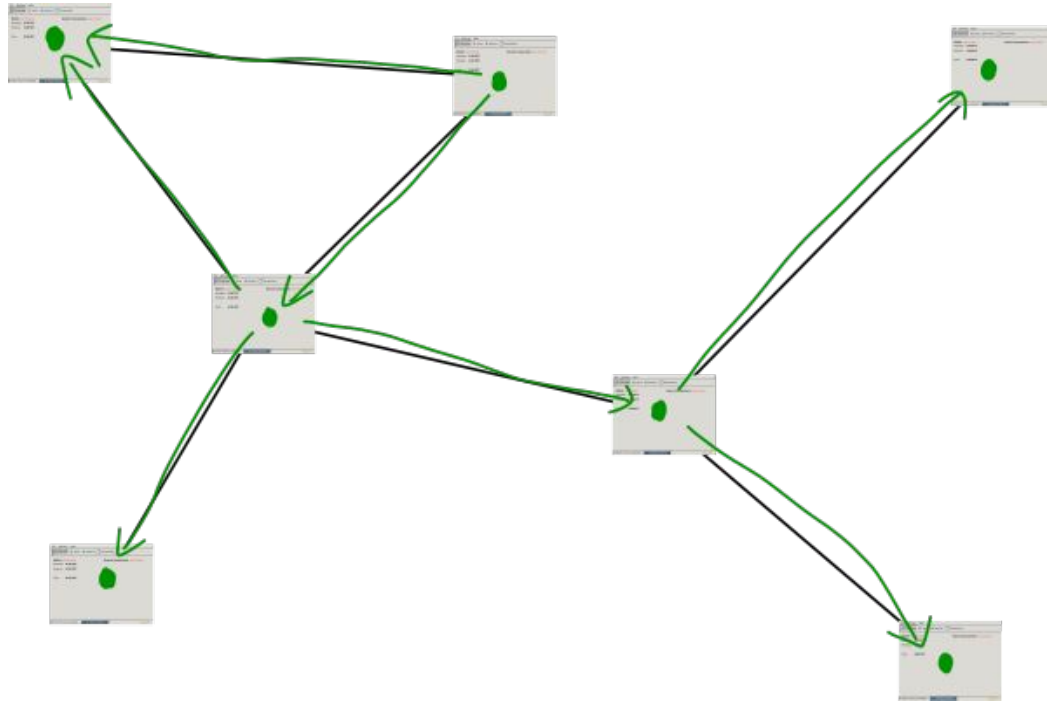
Clientes Bitcoin “falam” entre si.

O que a rede faz?



Por exemplo, informação sobre uma nova transação.

O que a rede faz?

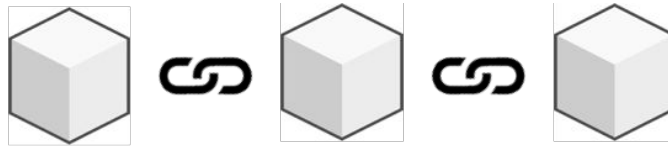


Eventualmente, todo mundo vai saber da nova transação.

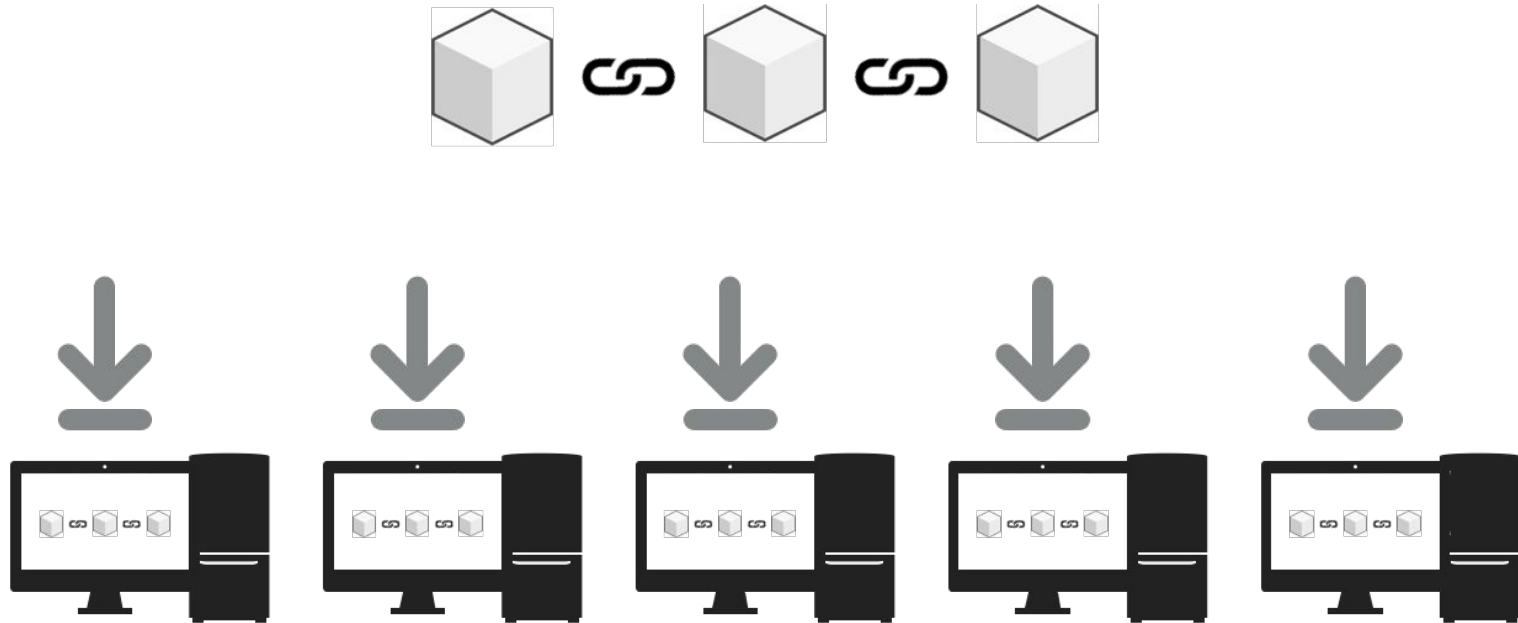
Rede distribuída

Uma rede que permite que dados sejam propagados através de vários nós/usuários.

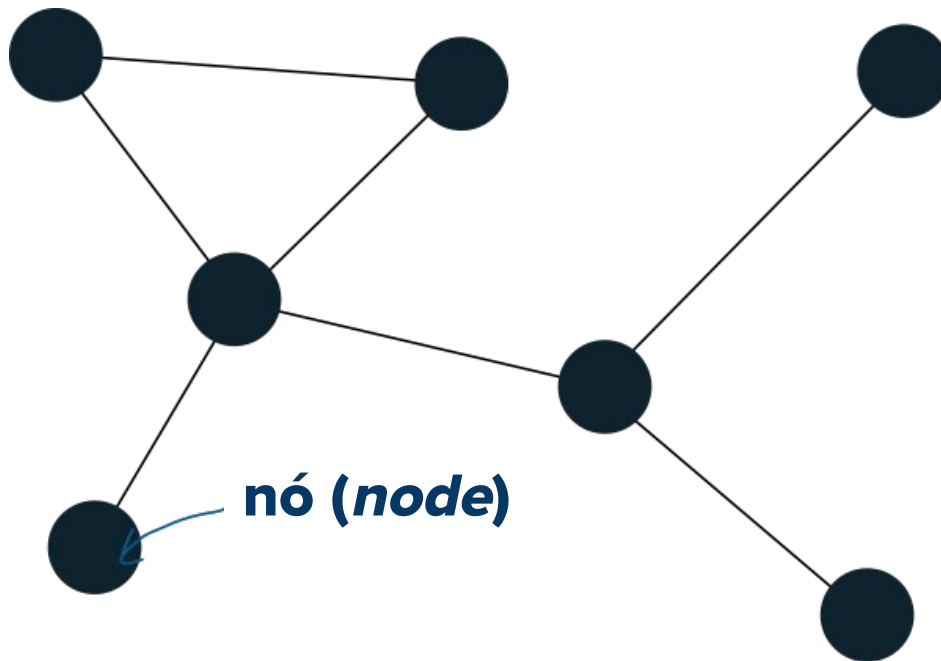
Rede P2P distribuída



Rede P2P distribuída



Quem faz parte da rede?



nó (node)

Qualquer um com conexão a Internet e rodando um cliente Bitcoin.
Quando está ativo e executando você é conhecido como um **nó** da rede Bitcoin

Como fazer parte da rede?

Tudo que você precisa é baixar (e executar) um [cliente Bitcoin](#)

Ao executar o cliente, ele se conectará a outros nós e começará a baixar uma cópia completa do *blockchain*

Depois disso, seu cliente começará a receber transações de outros nós e a retransmiti-las pela rede.

Parabéns, agora você é um nó da rede Bitcoin!

O que um nó faz?

1. Segue as regras
2. Compartilha informação
3. Mantém uma cópia das transações confirmadas

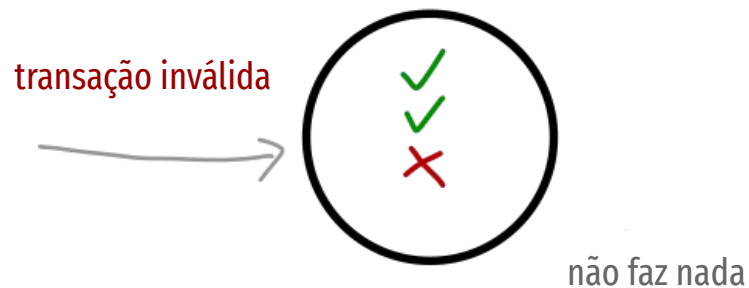
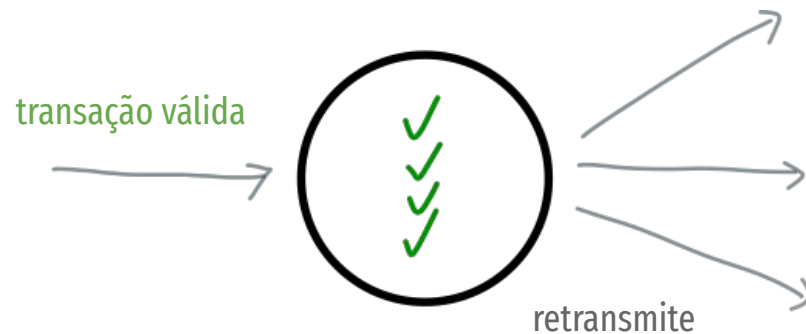
1. Segue as regras

Cada nó (cliente bitcoin) foi programado para seguir um **conjunto de regras**.

Seguindo essas regras, um nó é capaz de **verificar as transações** que recebe e apenas retransmiti-las se tudo estiver OK

Se houver algum problema, a transação não é repassada.

1. Segue as regras



2. Compartilha informação

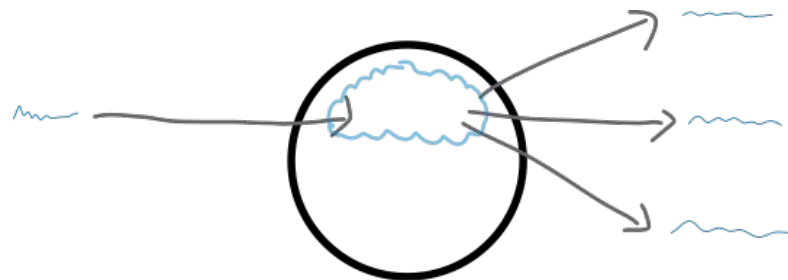
O principal trabalho de um nó é compartilhar informações com outros nós, e a principal informação que um nó compartilha são **transações**.

Existem dois tipos de transações que os nós compartilham:

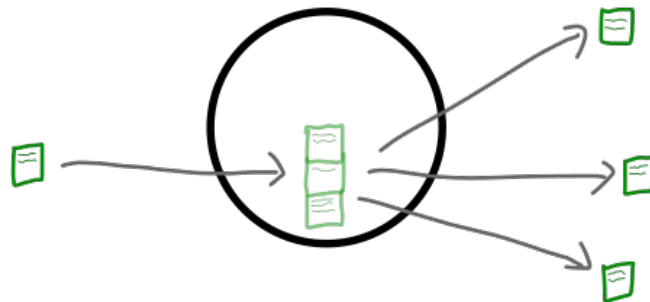
Transações novas – **transações** que entraram recentemente na rede.

Transações confirmadas – transações que foram “confirmadas” e gravadas em um arquivo. Estes são compartilhados em **blocos de transações**, e não individualmente.

2. Compartilha informação



compartilhando novas transações



compartilhando blocos de transações confirmadas

3. Mantém uma cópia das transações confirmadas

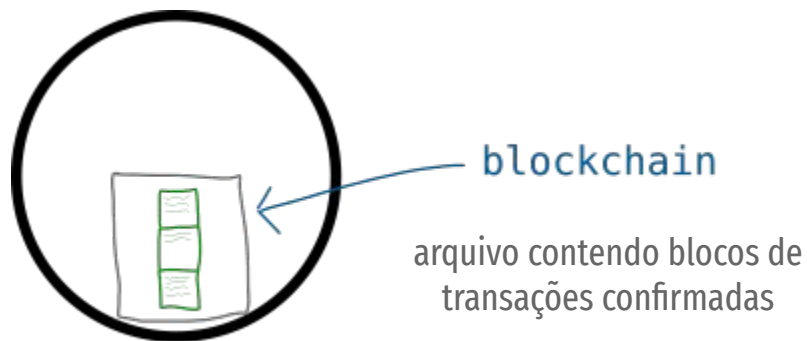
Cada nó também mantém blocos de **transações confirmadas**.

Estes são mantidos juntos em um arquivo chamado ***blockchain***.

Novas transações são encaminhadas pela rede até serem gravadas no *blockchain*, que é um livro de transações confirmadas.

Cada nó tem uma cópia do *blockchain* para segurança e a compartilha com outros nós se sua cópia não estiver atualizada.

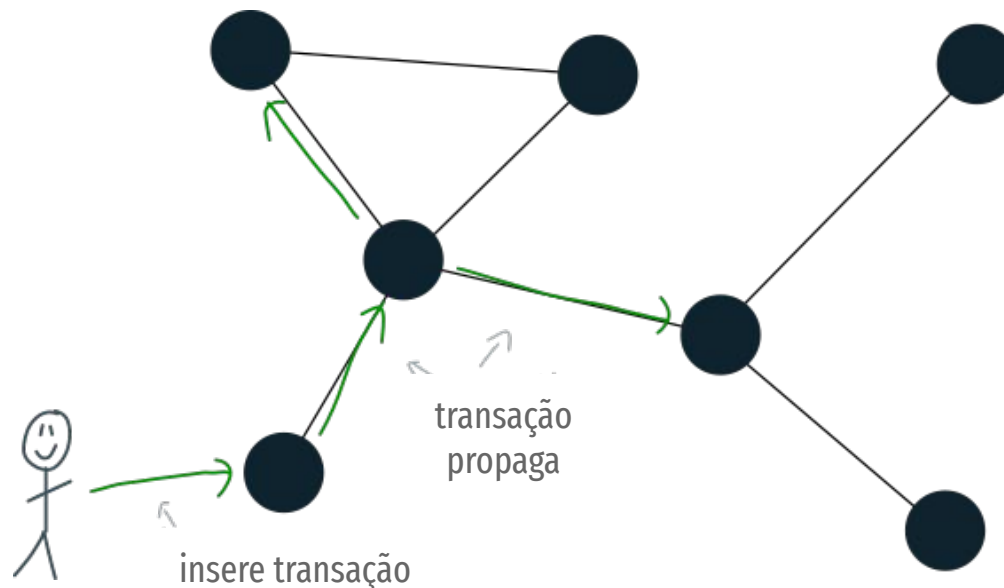
3. Mantém uma cópia das transações confirmadas



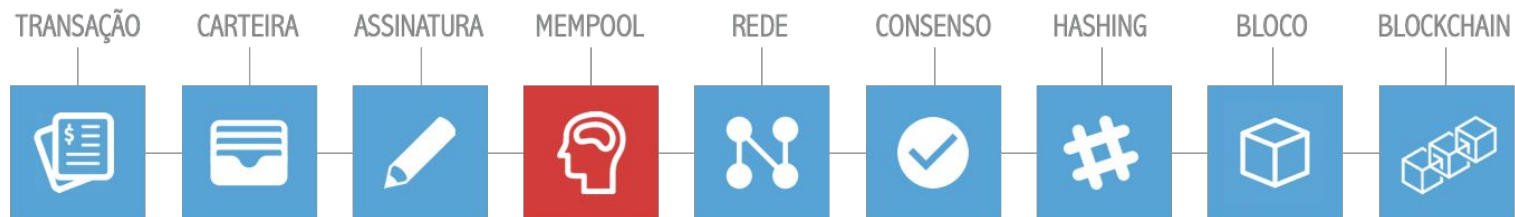
Preciso ser um nó para usar Bitcoin?

Não. Você pode enviar e receber BTC sem precisar ser um nó

Você só precisa fazer a transação na rede bitcoin e pronto.



ARQUITETURA DE UM **BLOCKCHAIN**



Memory Pool

Taxa de novas transações > processamento do *blockchain*

Antes de fazerem parte de um *blockchain*, transações fazem parte do chamado *memory pool* (**mempool**), que funciona como um **backlog de transações**

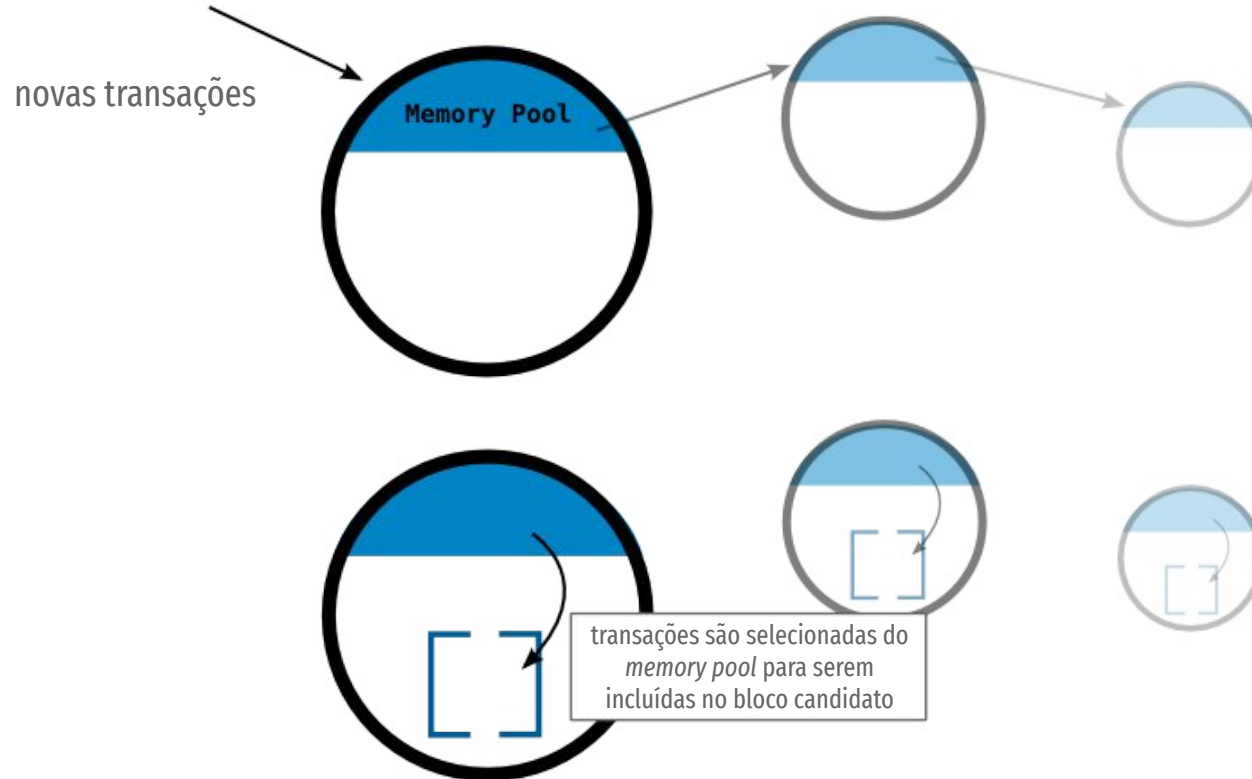
Quando uma nova transação é recebida por um nó, ele a manterá em seu *memory pool* com todas as outras últimas transações recebidas

A partir daqui, a transação espera ser selecionada para inclusão no **bloco candidato**

Transações BTC demoram **em média 10-30 minutos** para serem confirmadas

https://ycharts.com/indicators/bitcoin_average_confirmation_time

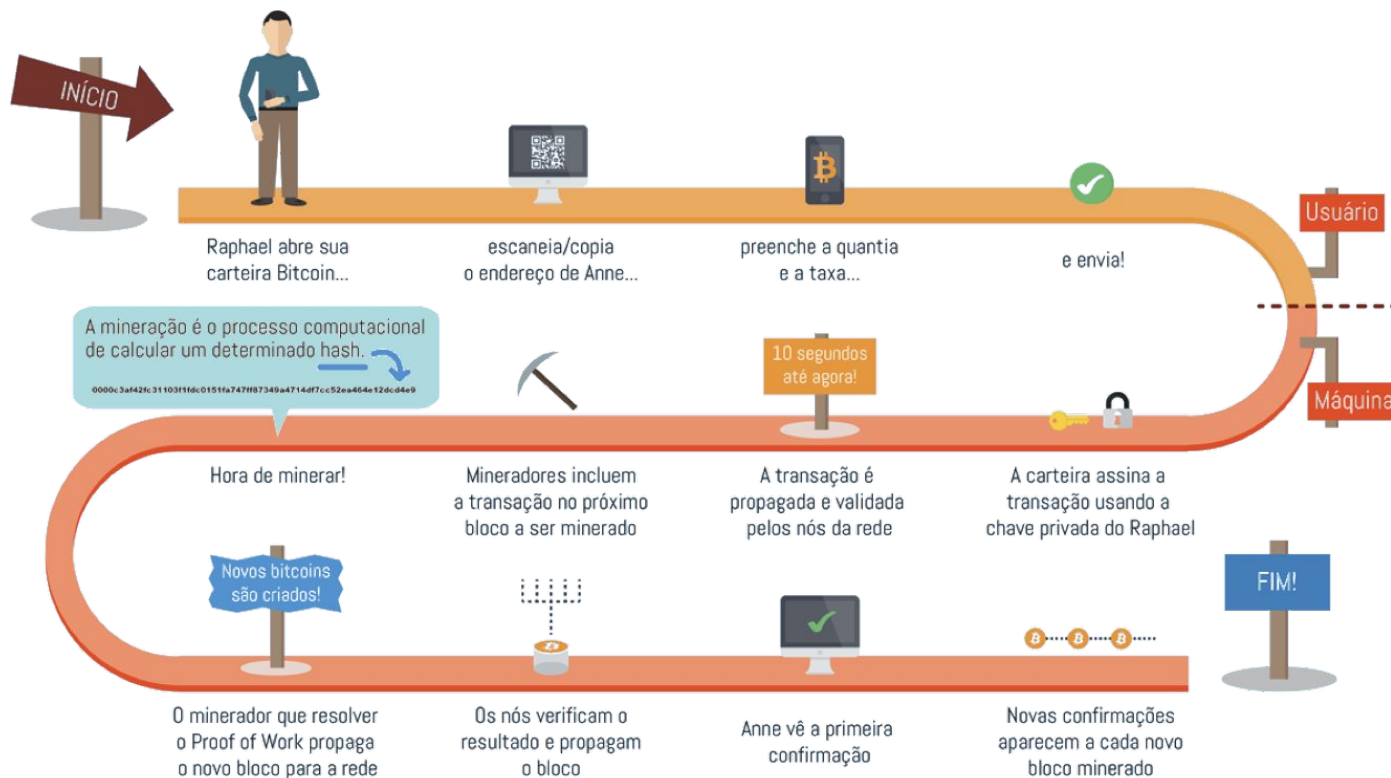
Memory Pool



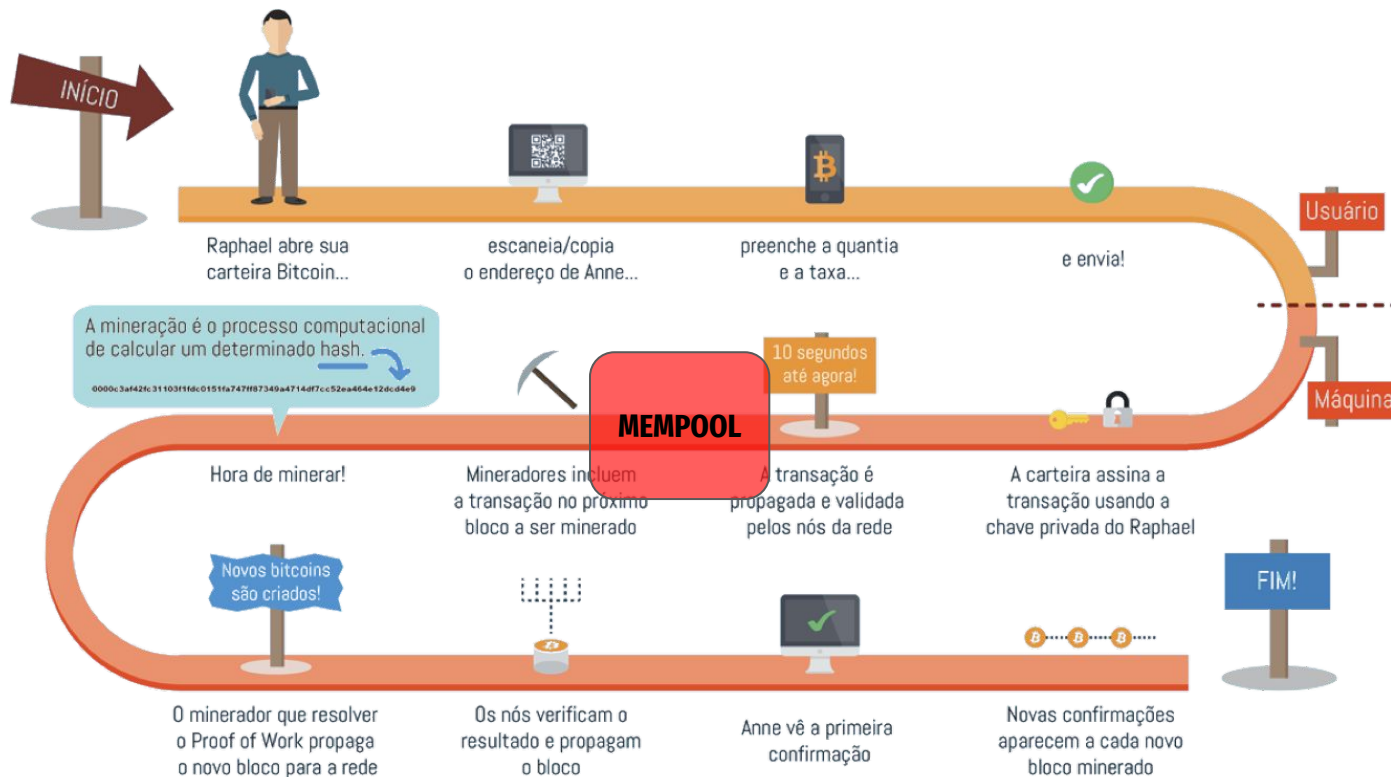
Mempool

Local de espera para transações não confirmadas antes de serem adicionadas ao *blockchain*.

Ciclo de vida de uma transação



Ciclo de vida de uma transação



Memory Pool

<https://www.blockchain.com/btc/unconfirmed-transactions>

<https://www.blockchain.com/charts>

https://ycharts.com/indicators/reports/bitcoin_statistics

<https://mempool.space/pt/>

<https://bitcoinvisuals.com/stats>

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

Quando uma transação sai do mempool?

A transação foi incluída em um bloco;

A transação expirou por *timeout* (por padrão em alguns clientes, 14 dias) *;

A transação estava no fim da *mempool* (ordenadas), o *mempool* atingiu seu limite, e uma nova transação foi aceita, dropando a anterior;

A transação conflita com uma transação que foi incluída em algum bloco.

* teoricamente, uma transação NUNCA expira

