BITCOIN

Introdução

- Sistema de pagamento eletrônico peer-to-peer
- Não depende de uma instituição financeira
- Baseado em provas criptograficas e não em confiança
- Histórico de transações distribuido
- O histórico mais longo atesta o histórico válido
- Será seguro enquanto o poder computacional dos nós honestos for maior que o poder computacional malicioso

Introdução

- Para que não haja uma entidade central intermediando as transações, foi implementado um banco de transações distribuido, onde cada nó da rede conhece todas as transações
- ""
- Resolve o problema em transações casuais de baixo valor
- Sistema de transções irreversíveis

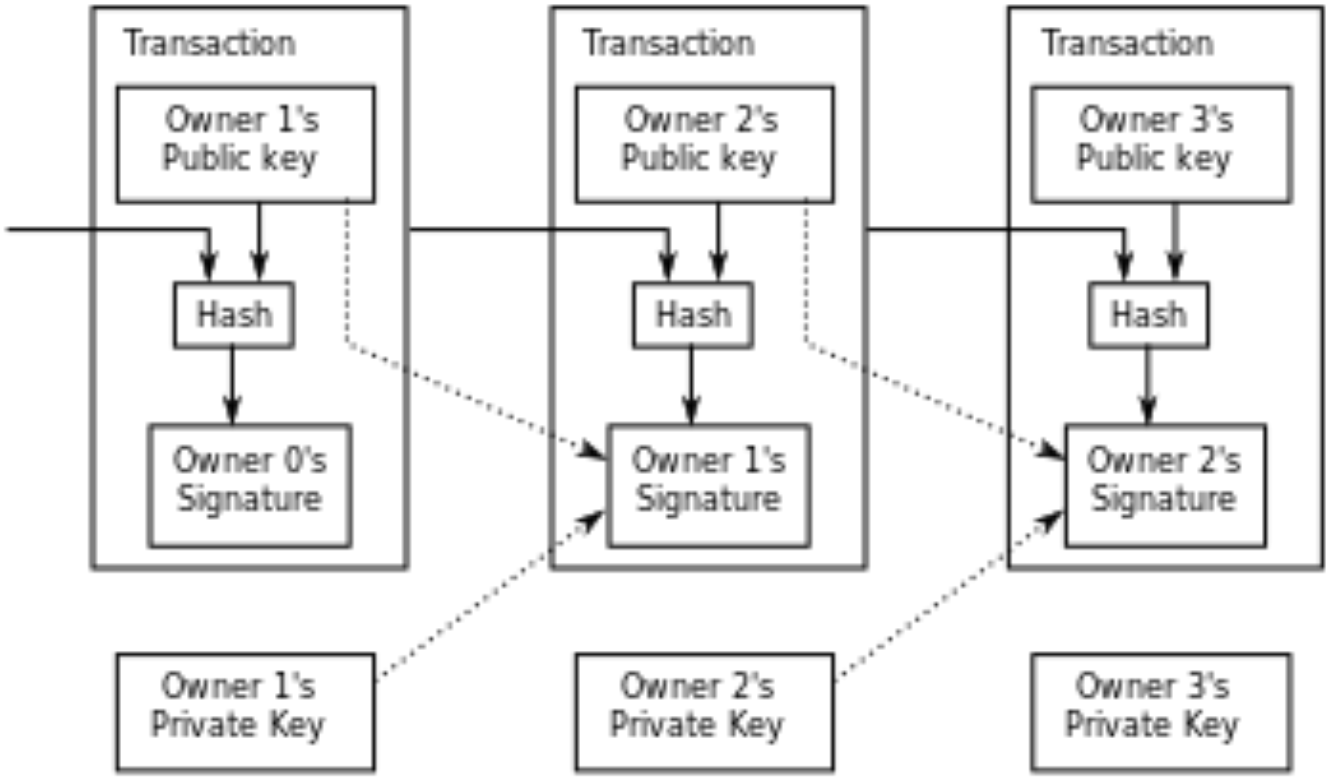
Características

- Há um limite na quantidade total de bitcoins
  - Cerca de 21 milhões
- Pode ser dividido até a 8ª casa decimal
- Após o termino da mineração, os bitcoins poderão ser obtidos por taxas de transação.

Transação

- Cada endereço bitcoin (chave publica) possui uma quantidade de bitcoins associado a ele
- Para transferir o dinheiro, o remetente deve saber o endereço do destinatário (chave publica)
- O remetente cria uma transação que envia uma quantidade X de bitcoins ao destinatário, esta transação é assinada com a chave privada do remetente
- A rede verifica a transação a partir da chave publica do remetente

Transação

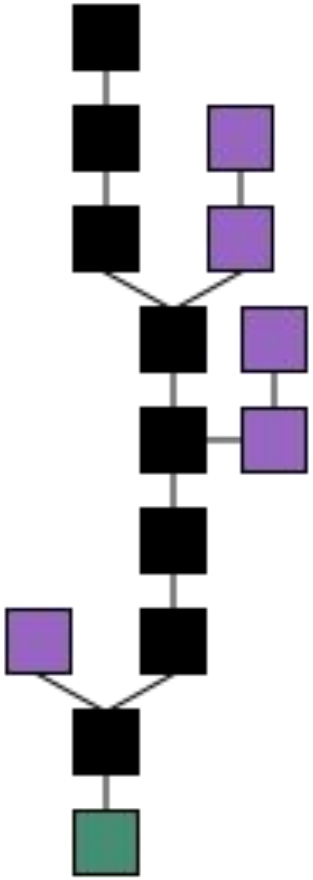

Transaction
Owner 1's Public key
Hash
Owner 0's Signature
Transaction
Owner 2's Public key
Hash
Owner 1's Signature
Transaction
Owner 3's Public key
Hash
Owner 2's Signature
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

Segurança

- As transações são agrupadas em blocos que são gerados a cada 10 minutos em média
- Para garantir a integridade do sistema, os blocos são colocados em um sistema de hash em que a hash do bloco anterior influencia na hash do proximo bloco
- Para que um cliente mal intencionado altere alguma transação, ele mesmo teria que re-processar toda a cadeia a partir de um certo ponto

Segurança

- A rede toma como válido a cadeia mais longa a partir do bloco original
- O bitcoin permanecerá segura enquanto o poder computacional honesto seja maior que o malicioso



Mineração

- A geração de bitcoin é feita solucionando o problema de hash
- O primeiro mineirador que solucionar de maneira valida o hash de um bloco pode reinvidicar para si uma quantidade de bitcoins
- Outra maneira de se obter bitcoins é através de taxas de transferências, onde as transferencias que pagam a taxa têm preferencia no processamento

Anonimato

- Uma das principais vantagens do bitcoin em relação ao sistema de pagamento convencional é o anonimato
- Um usuário pode criar gratuitamente seus pares de chave publica/privada
- Não há nenhum tipo de informação pessoal na rede bitcoin

Referencias

- Nakamoto Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. Disponível em: http://bitcoin.org/bitcoin.pdf