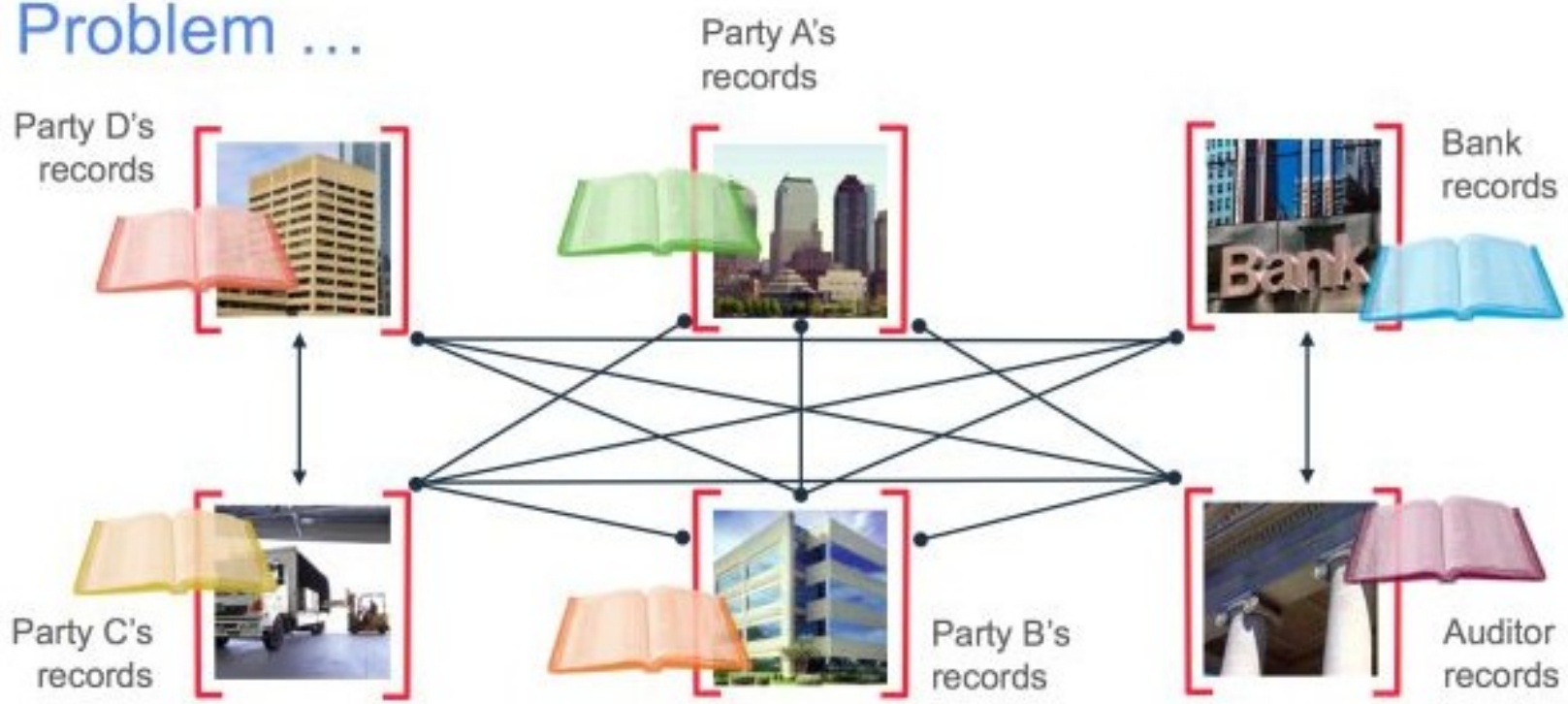
Universidade Federal do ABC

Segurança de Redes

Blockchain e Bitcoin

Prof. João Henrique Kleinschmidt

Problem …

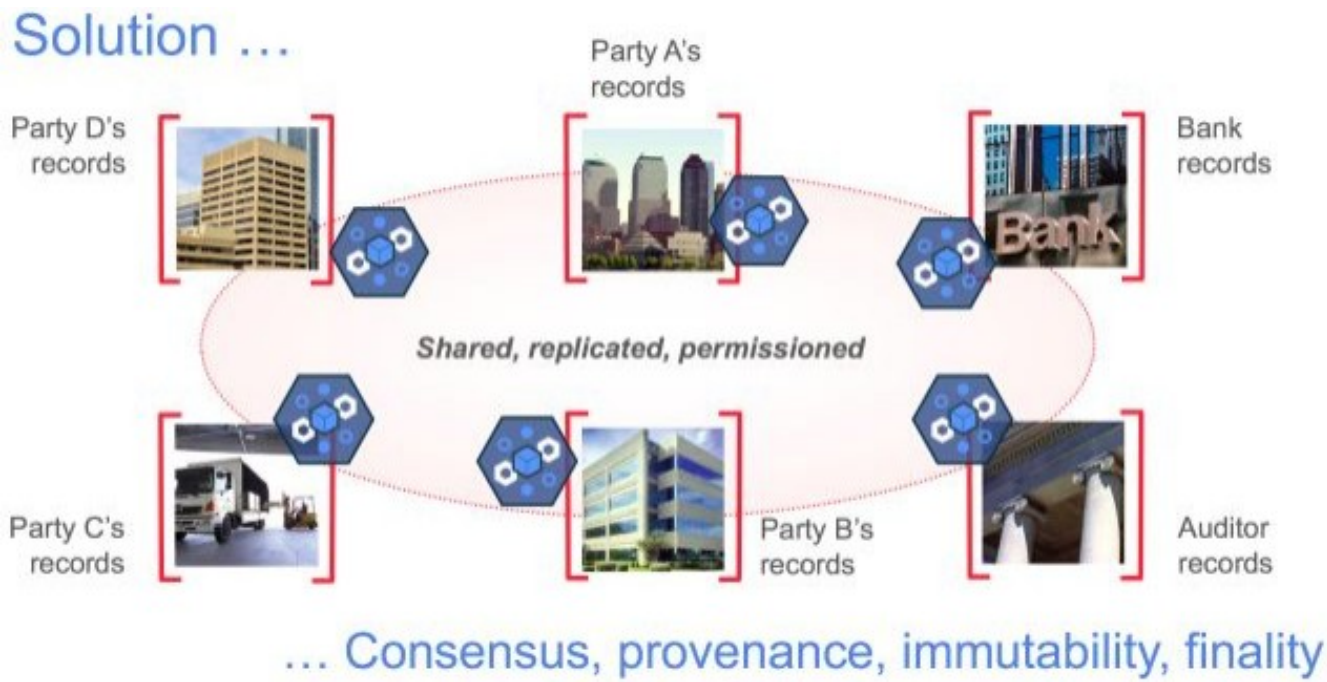


… Inefficient, expensive, vulnerable

Blockchain - Definição

Um banco de dados distribuído e seguro que guarda um registro de transações permanente e à prova de violação.

As moedas digitais foram as primeiras a usar o conceito de blockchain.



Bitcoin

- Um **protocolo** que suporta uma moeda digital ponto-a-ponto, descentralizada e pseudo-anônima

- Um **livro-razão** (*ledger*) de transações publicamente divulgado e armazenado em uma blockchain

- Um sistema orientada a **recompensas** para atingir consenso (**mineração**) baseada em **Provas de Trabalho** (Proofs of Work)

Bitcoin Whitepaper – 2008.10.31*

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest

* Halloween

Características do Bitcoin

- Essencialmente “deflacionária” – a recompensa é cortada pela metade aproximadamente a cada 4 anos
- Moeda divisível que suporta 8 casas decimais 0.00000001 (conhecidos como Satoshi)
- Taxa das transações paga para a rede
  - Mesmo custo para enviar $.01 ou $1,000,000
- Orientada a consenso – sem autoridade central
- Resiliente a falsificações
  - Moedas não podem ser adicionadas arbitrariamente
  - Não existe “gasto duplo”
- Não-repúdio

Economia do Bitcoin

- Taxa limitada pela criação de novos blocos
  - Adaptada a capacidade da rede
  - Um bloco criado a cada 10 minutos em média (6 blocos cada hora)
    - Como ? A dificuldade é ajustada para manter a taxa fixa na medida que a capacidade computacional aumenta
- N novos Bitcoins para cada novo bloco: creditado aos mineradores → é o incentivo
  - N era inicialmente 50. Em 2013, N=25. Hoje, N= 12,5.
  - O total de Bitcoins não irá exceder 21 milhões (após isso os mineradores ganham uma taxa)
  - Bitcoins também podem ser comprados/vendidos em corretoras

Quando começou?

- Satoshi Nakamoto criou a implementação de referência que começou com o Bloco Genesis de 50 moedas

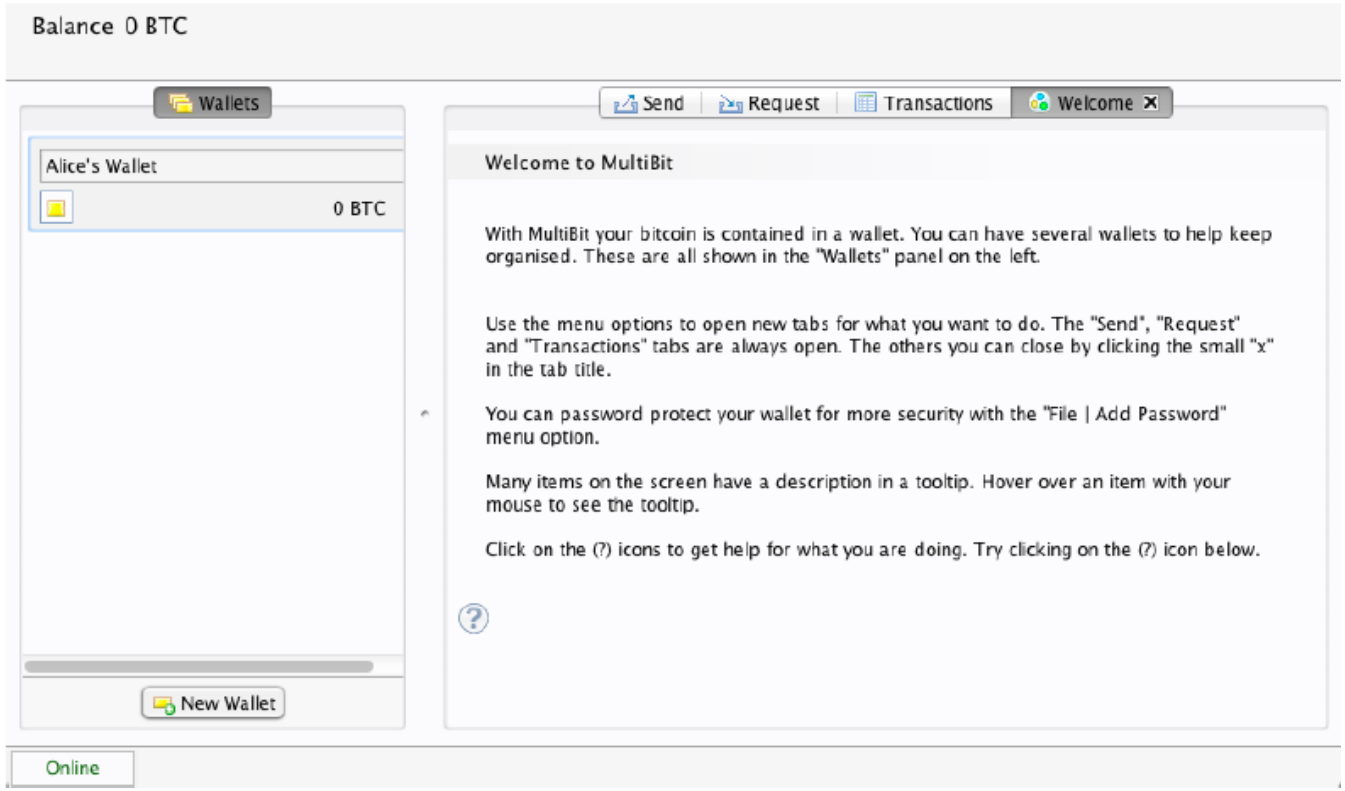
- **2008**
  - **Agosto 18** Nome de domínio "bitcoin.org" registrado
  - **Outubro 31** Artigo do Bitcoin publicado
  - **Novembro 09** Projeto Bitcoin registrado em SourceForge.net

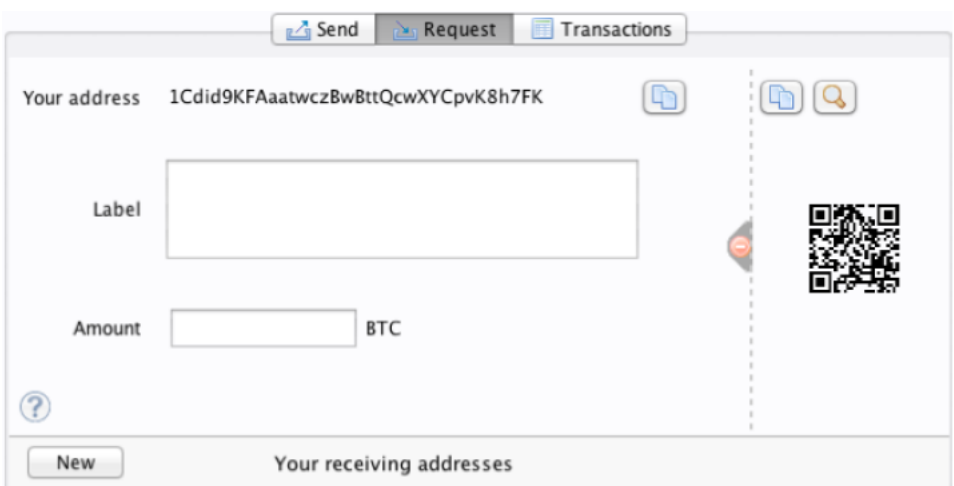
- **2009**
  - **Janeiro 3** Bloco Genesis estabelecido em 18:15:05 GMT
  - **Janeiro 9** Bitcoin v0.1 lançado e anunciado
  - **Janeiro 12** Primeira transação bitcoin

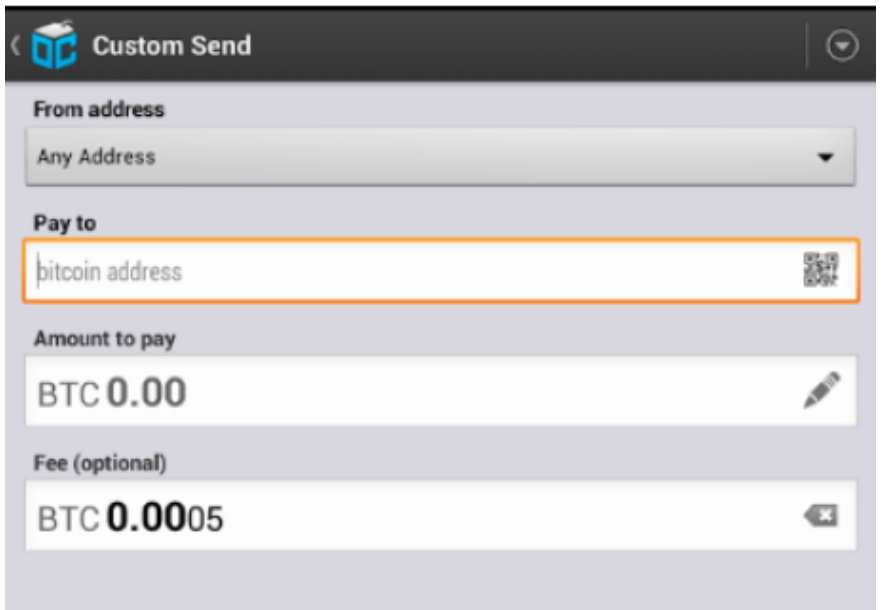
Segurança no Bitcoin

- Autenticação → Criptografia de chave pública: assinaturas digitais
  - Estou pagando para pessoa certa? E não alguém se fazendo passar por outra pessoa?
- Integridade → Assinaturas digitais e hash criptográficos
  - O dinheiro teve "gasto duplo"?
  - Um atacante pode reverter ou alterar transações?
- Disponibilidade→ Mensagens de broadcast para a rede P2P
  - Posso fazer uma transação a qualquer hora?
- Confidencialidade→ "Pseudonimidade"
  - Minhas transações são privadas? Anônimas?

Carteiras (wallets)

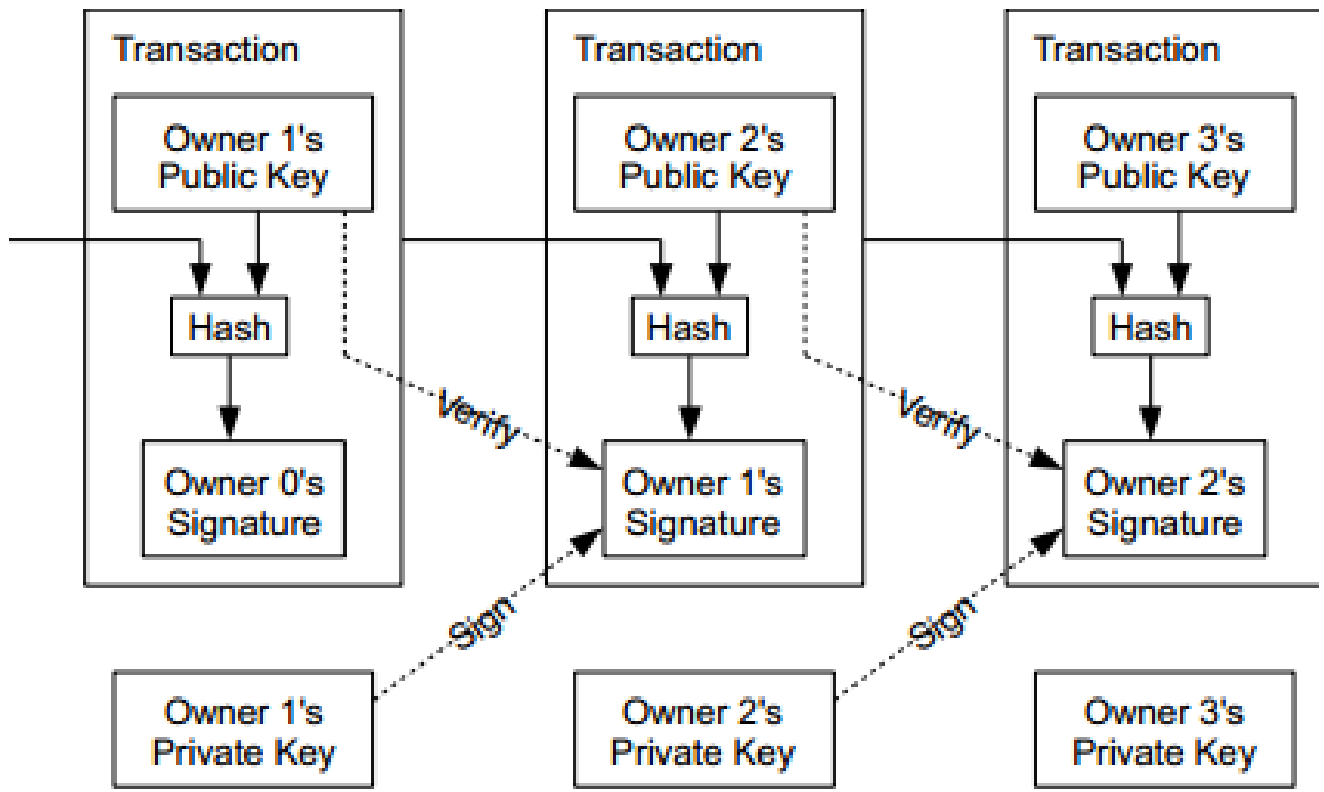




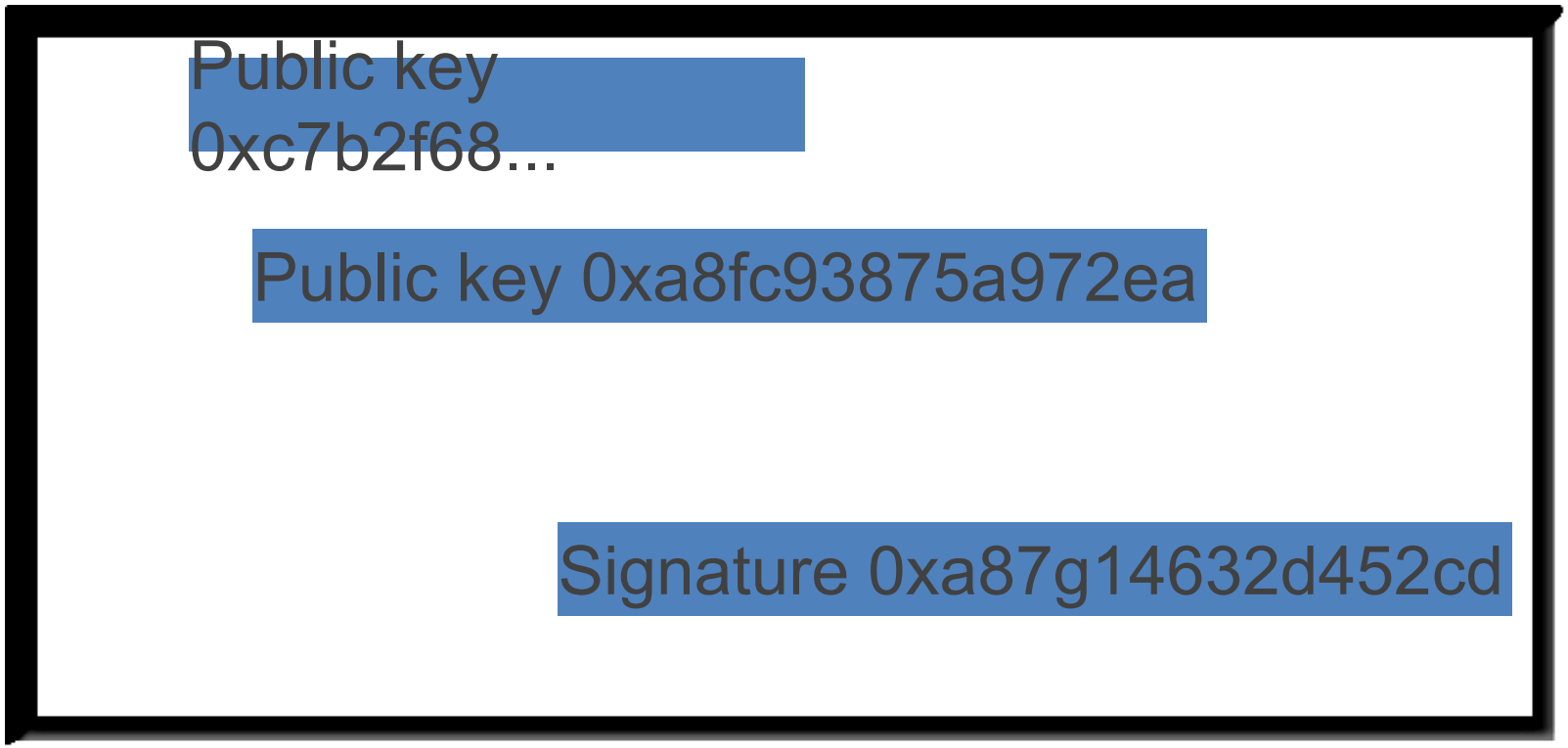


Moedas fluem de Entradas para Saídas

Um proprietário de Bitcoins transfere moedas assinando digitalmente (com ECDSA) um hash da transação anterior e a chave pública do próximo proprietário. Esta assinatura é anexada no fim da transação.



Transações Bitcoin



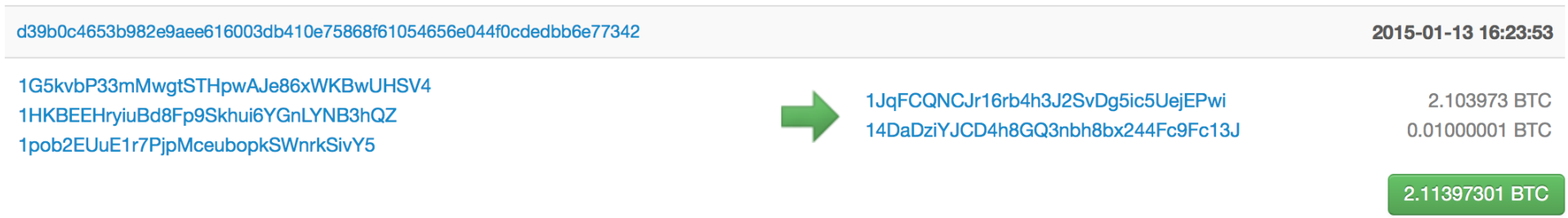
	Origem	Valor	Destino
#0		25	Alice
#1	Alice	17	Bob
#2	Bob	8	Carol
#3	Carol	5	Alice

Pseudo Anônimo

- Usa criptografia de chave pública (curvas elípticas), devido a força das chaves e chaves menores
- Transações são enviadas para endereços de chave pública

  1AjYPi8qryPCJu6xgdJuQzVnWFXLmxq9s3

  1Give4dbry2pyJihnpqV6Urq2SGEhpz3K

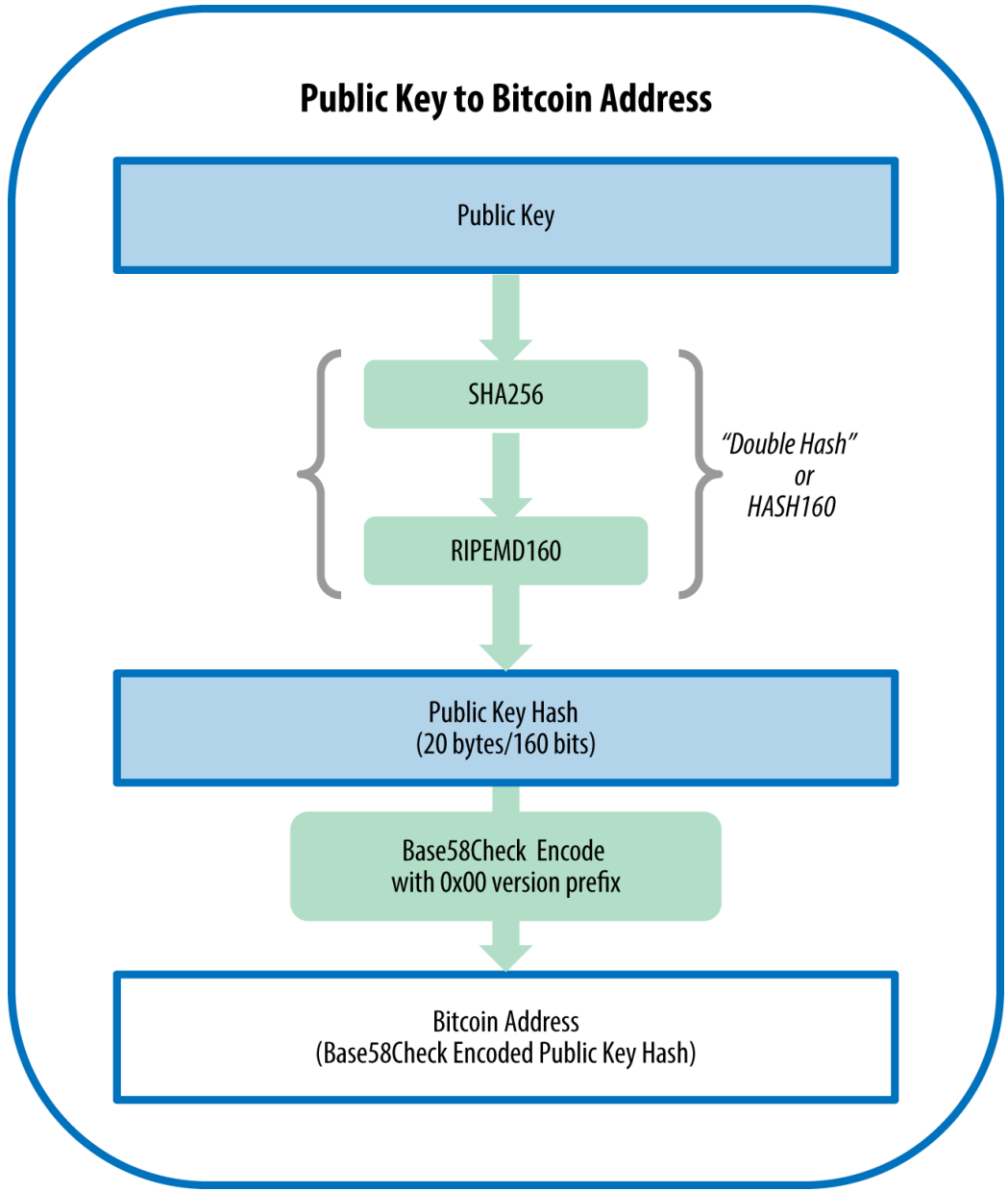


Endereços são as “contas”

- A carteira escuta por transações endereçadas para qualquer uma de suas chaves públicas. É o único nó capaz de decifrar e aceitar a transação

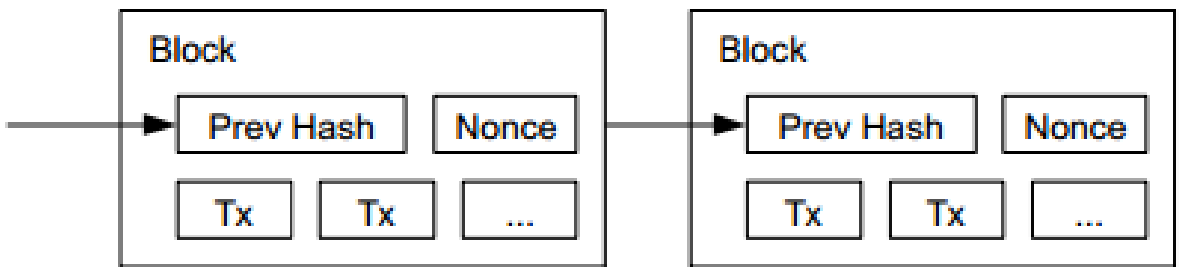
- “Moedas” são “enviadas” por broadcast da transação para a rede, que verifica que são viáveis e adiciona em um bloco

Geração de chaves Bitcoin e endereços



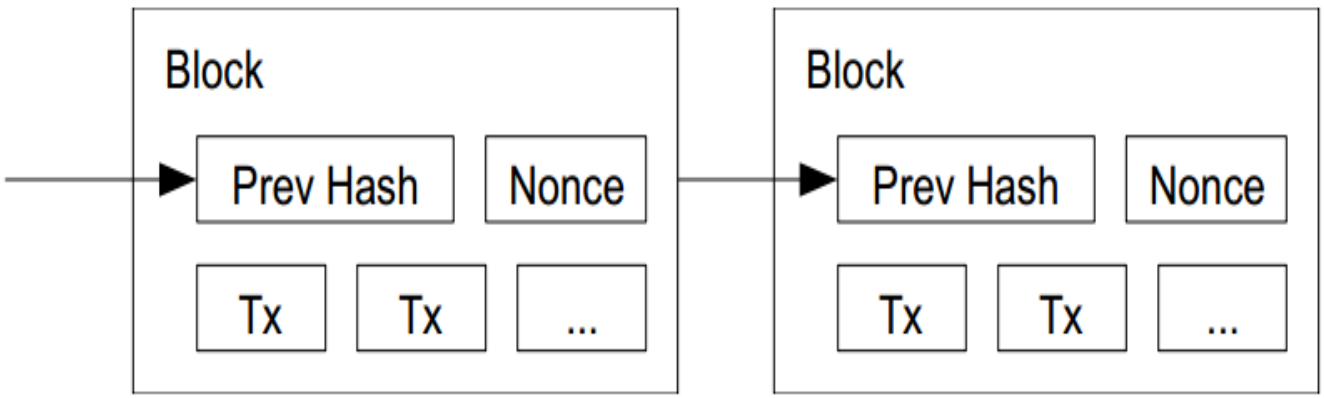
Livro-razão público

- Cada transação é armazenada em um livro razão público
- As transações estão localizadas em blocos, que são ligadas por hashes SHA256
- https://blockchain.info



Uso de Hash Criptográfico

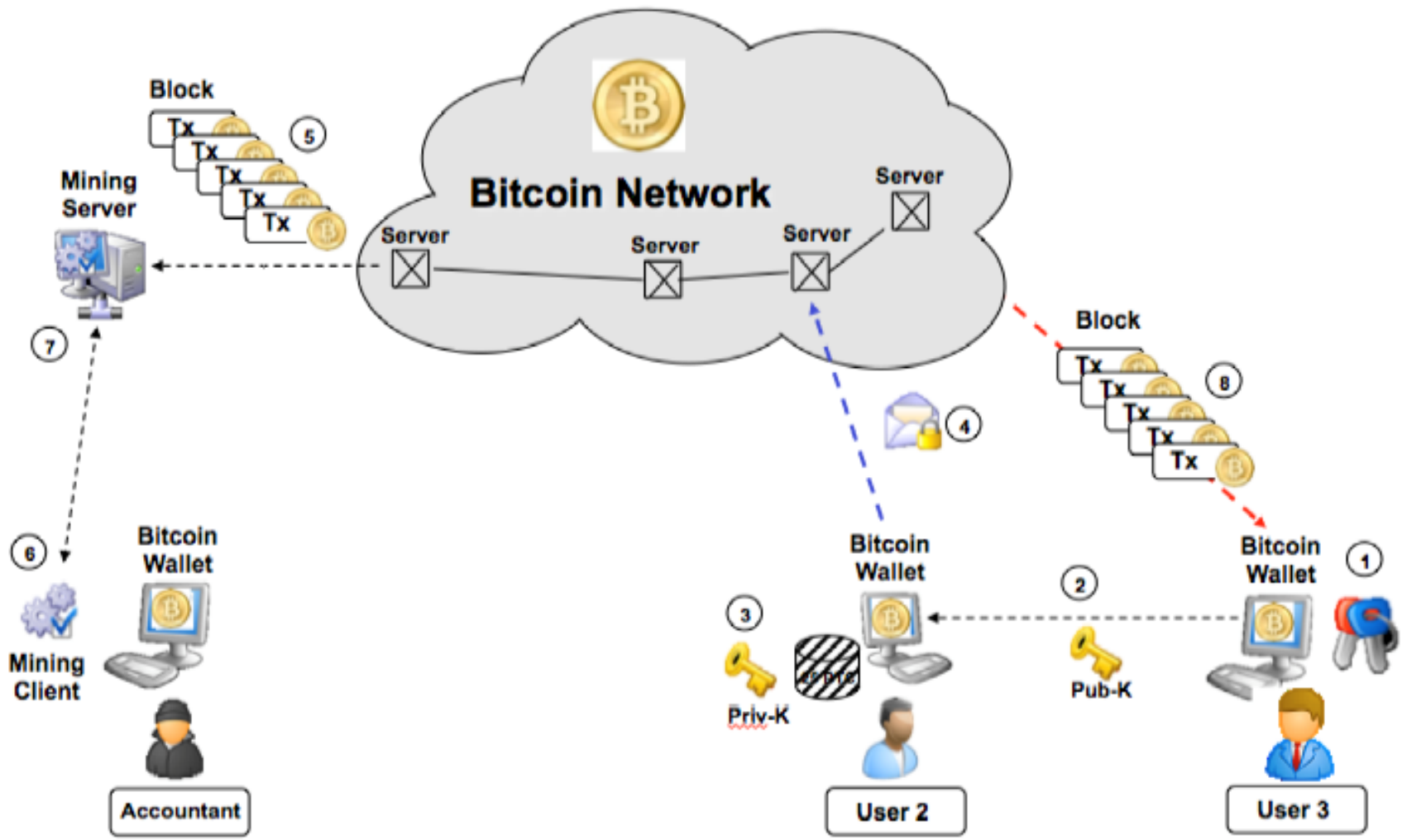
- Prova de trabalho (Proof-of-Work)
  - Um bloco contém as transações a serem validadas e o valor anterior de hash.
  - Escolhe um *nonce* (número) tal que **Hash(hash anterior, nounce, Transações) < E**. E é uma variável que o sistema especifica. Basicamente deve encontrar um valor de hash que inicie com números zero. O trabalho requirido é exponencial ao número de zeros exigidos.
  - A verificação é fácil. Mas a prova de trabalho é difícil.



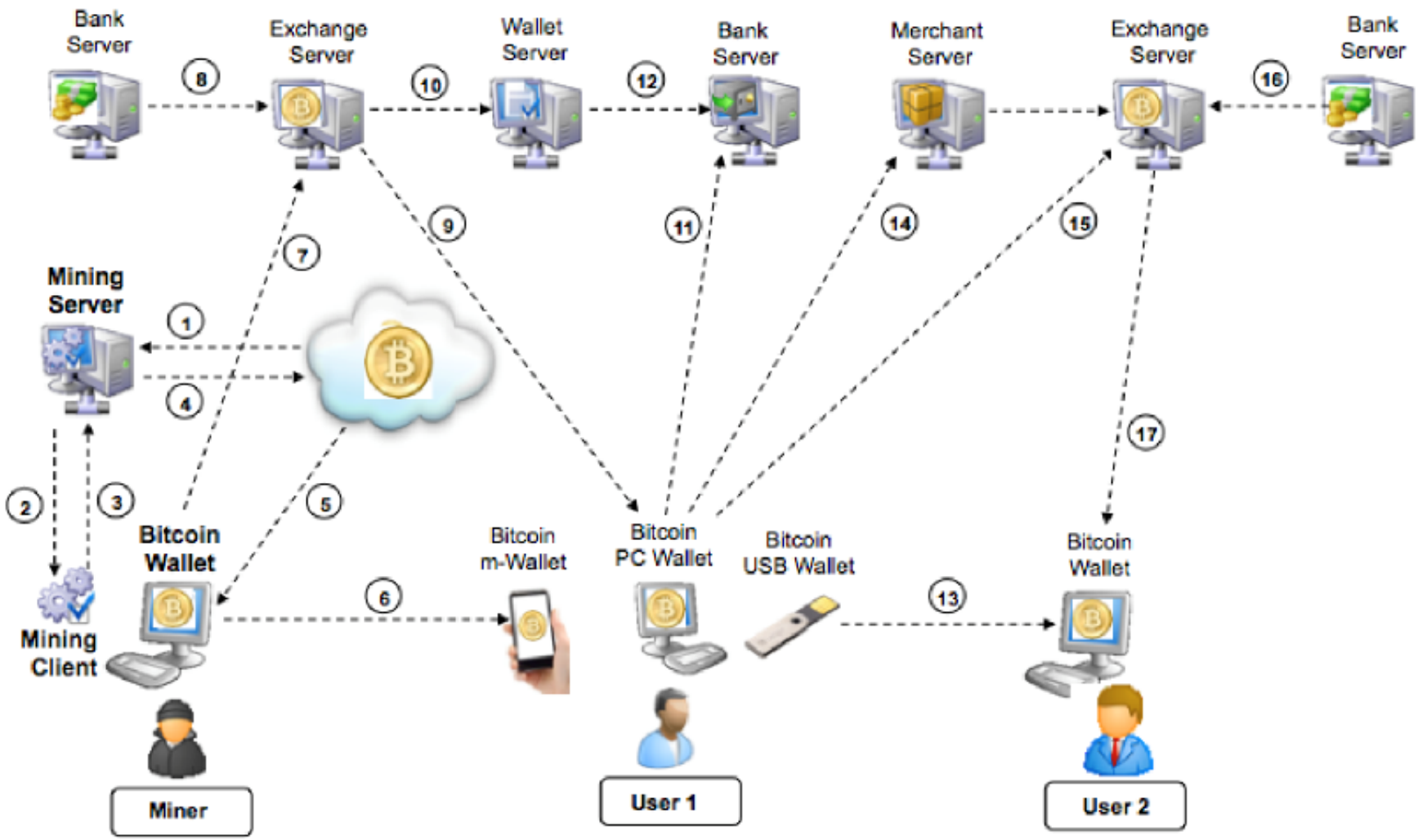
Rede Bitcoin

- Cada nó P2P node executa o seguinte algoritmo:
  - Novas transações são enviadas por broadcast para todos os nós.
  - Cada nó (minerador) coleta novas transações em um bloco.
  - Cada nó trabalha para encontrar uma prova de trabalho para o seu bloco.
  - Quando um nó encontra uma prova de trabalho, faz o broadcast do bloco para todos os nós. Este nó que encontrou a solução ganha uma recompensa (originalmente 50 Bitcoins)
  - Os nós aceitam o bloco apenas se todas as transações são válidas (checagem da assinatura digital) e ainda não foram gastas.
  - Os nós expressam a aceitação do trabalho pelo trabalho em criar um novo bloco na cadeia, usando o hash do blocos aceito como o hash anterior.
  - Aproximadamente 10 minutos para verificar uma transação e inserir na blockchain

Rede Bitcoin



Rede Bitcoin



Estrutura de um bloco

Tamanho	Campo	Descrição
4 bytes	Tamanho do Bloco	O tamanho do bloco, em bytes, após esse campo
80 bytes	Cabeçalho do Bloco	Vários campos formam o cabeçalho do bloco
1-9 bytes (VarInt)	Contador de Transações	Quantas transações seguem
Variável	Transações	As transações registradas nesse bloco

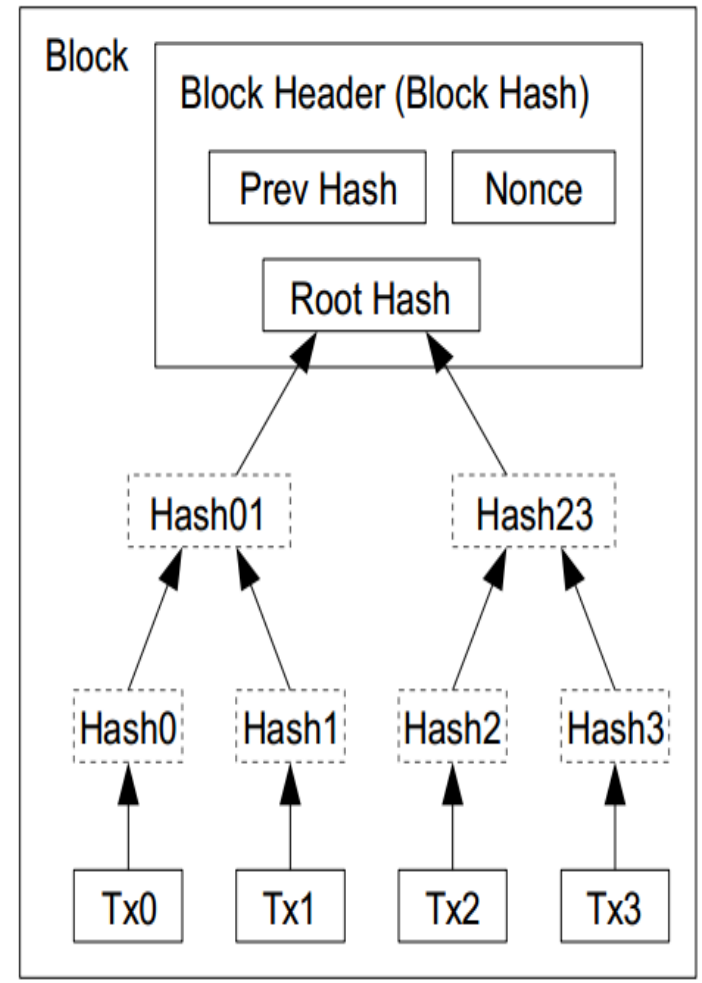
Bloco

Tamanho	Campo	Descrição
4 bytes	Versão	Um número de versão para servir como referência nas atualizações de software/protocolo.
32 bytes	Hash do Bloco Anterior	Uma referência ao hash do bloco anterior (bloco pai) na blockchain
32 bytes	Raiz de Merkle	Um hash da raiz da árvore de merkle das transações desse bloco
4 bytes	Data e Hora (timestamp)	O momento aproximado em que este bloco foi criado (em segundos, usando Unix Epoch)
4 bytes	Dificuldade Alvo	O alvo de dificuldade do algoritmo de prova-de-trabalho deste bloco
4 bytes	Nonce	Um contador usado para o algoritmo de prova-de-trabalho

Cabeçalho

Otimizações

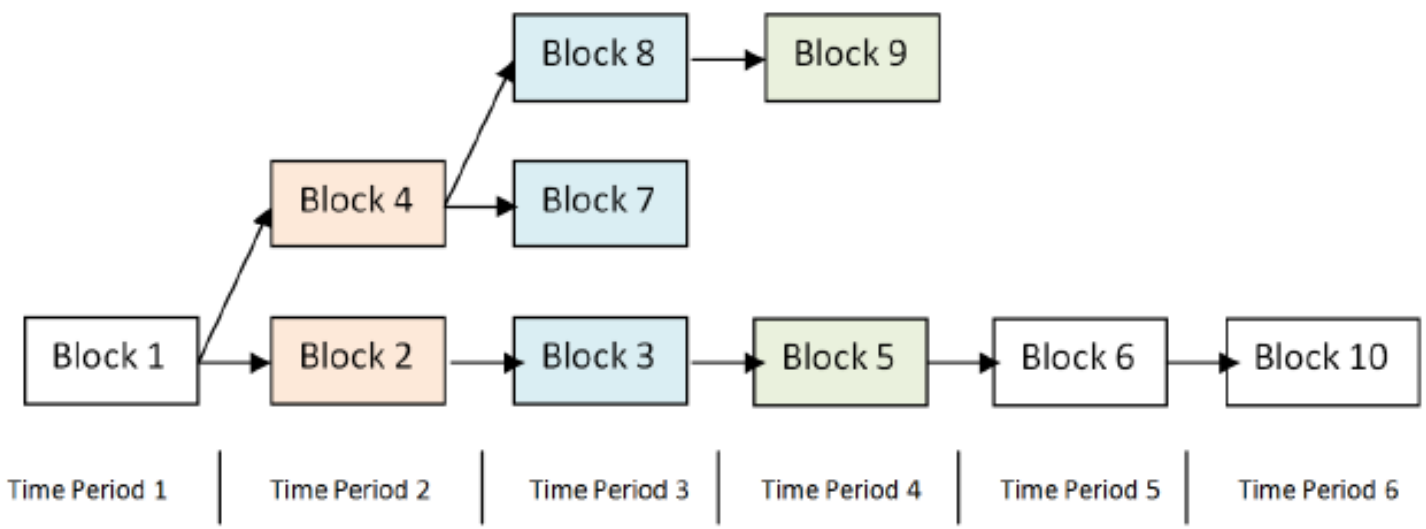
- As árvores de Merkle são usadas no Bitcoin para resumir todas as transações em um bloco, produzindo uma impressão digital eletrônica geral de todo o conjunto de transações.
- Isto fornecendo um processo muito eficiente para verificar se uma transação foi incluída em um bloco.
- Uma árvore de Merkle é construída através do hashing recursivo de pares de nós até que haja apenas um hash, conhecido como a raiz ou raiz de Merkle.



Transactions Hashed in a Merkle Tree

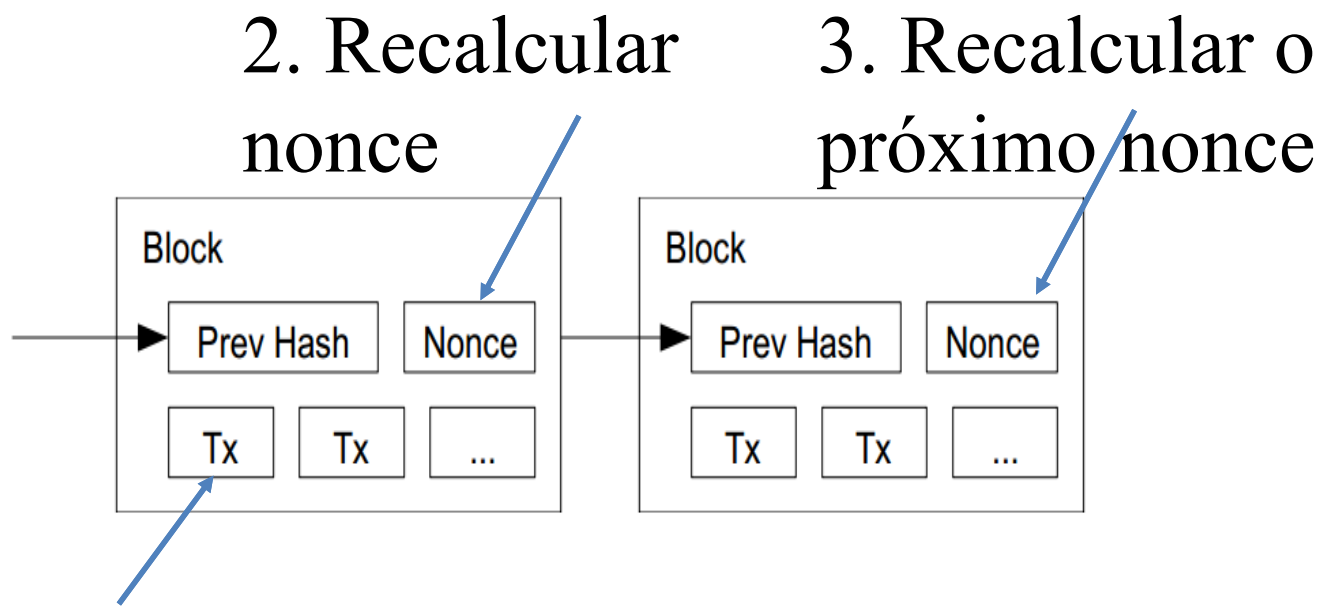
Consenso

- O caminho mais longo representa a cadeia vencedora.
- Um participante que escolhe estender um caminho existente na blockchain indica um voto para o consenso naquel caminho. Quanto mais longo o caminho, mais computação foi gasta em sua construção.



Reversão é difícil

- Quando a cadeia cresce, reverter as transações se torna exponencialmente difícil



Confirmação de transação

- Cada novo bloco aceito na cadeia depois que a transação foi aceita é considerado uma confirmação
- As moedas não são consideradas maduras até que tenham 6 confirmações (em torno de uma hora)
- Novas moedas (Bitcoins) criados pelo processo de mineração não são válidas até em torno de 120 confirmações
- Isto acontece para garantir que um nó com mais de 51% do poder computacional da rede não insira transações fraudulentas

Criptomoedas alternativas

- Hoje existem centenas de moedas virtuais alternativas ao Bitcoin
- Muitas são apenas clones do Bitcoin e com algumas variações no total de moeda emitida, algoritmos hash, prova de trabalho, etc
- Exemplos: Ripple, Litecoin, Dogecoin, etc
- **Ethereum**: lançado em 2015, tem atraído bastante atenção. Executa contratos inteligentes (***smart contracts***) com a tecnologia blockchain.
- http://coinmarketcap.com

Outras aplicações de blockchain

- Rastreamento de produtos
- *Supply chain*
- Indústria 4.0
- Internet das Coisas
- Saúde
- Etc

Bibliografia

- Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf
- “Mastering Bitcoin”, Andreas M. Antonopoulos , O’Reilly Media
- Muftic, Sead, Ignacio Sanchez I. (ed.) and Beslay L. (ed.), *Overview and Analysis of the Concept and Applications of Virtual Currencies, EUR 28386 EN, doi:10.2788/16688*