Tópicos em Redes de Computadores

BlockChain

Prof. Elias P. Duarte Jr.
Universidade Federal do Paraná (UFPR)
Departamento de Informática
www.inf.ufpr.br/elias/topredes

Sumário

- Vamos ver o que é blockchain
- Uma classificação de blockchains
- Vamos estudar o funcionamento do Bitcoin

Blockchain: Funcionalidade

- Blockchain é uma tecnologia que permite o registro distribuído de dados & transações entre entidades que não se conhecem (atenção: aqui não permissionado)
  - se não se conhecem: não confiam entre si!
- Não há nenhum componente centralizado
- Os dados e transações são tanto de acesso público como privado → sigilosos ou não
- Registrados de forma a garantir autenticidade e integridade
  - é sempre possível checar a autenticidade e integridade

Além das Criptomoedas

- Uma das aplicações mais importantes de blockchain são as criptomoedas
- Há diversas, como a “original”: Bitcoin e a Ethereum
- Recursos desenvolvidos para blockchain como por exemplo “contratos inteligentes” estendem seu uso para diversos domínios
  - empresas de todos os setores, organizações diversas, governos...

Uma Classificação de Blockchains

- Uma classificação muito adotada hoje é entre:

  → Blockchains Públicas

  → Blockchains Permissionadas

- A Profa. Fabíola Greve da UFBA tem um minicurso sobre blockchain publicado no SBRC e disponível na Internet:
  - F. Greve, et. al., “Blockchain e a Revolução do Consenso sob Demanda,” Minicurso do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2018.
  - Em português: masculino ou feminino? a blockchain (fem)

Blockchains Públicas

- Uma blockchain pública forma uma rede P2P planetária
- A composição do sistema é dinâmica: nodos entram e saem a todo momento
- Em geral, os nodos são anônimos: não precisam de identificação para participarem do sistema
- Sem controle de participantes, que não confiam entre si
- Exemplos: Bitcoin, Ethereum, outras criptomoedas

Blockchains Permissionadas

- Também chamadas de privadas ou federadas
- Têm composição conhecida: sistema consiste de N processos que devem ter permissão explícita para entrar e sair
- Os nodos são: identificados, autenticados, autorizados
- Usadas em aplicações corporativas, entre organizações
- Exemplo: HyperLedger

Bitcoin

- A seguir vamos estudar o primeiro esforço da área: o Bitcoin
- Artigo seminal amplamente disponível na Internet:

Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Decentralized Business Review*, 2008.

Bitcoin

- “Electronic Cash System”:
  - Um sistema monetário na Internet, que permite pagamentos e transferências financeiras
  - em uma rede não confiável como a Internet
  - entre partes que não necessariamente confiam entre si
- Base: as transações recebem “assinaturas” que são obtidas através de uma sequência de hashes

Bitcoin: Motivação

- Eliminar a necessidade de terceiros que fazem o intermédio das transações financeiras
- Encarece processos, necessários para resolver litígios:
  - eliminar terceiros traz muitos benefícios!

Base do Bitcoin: Prova de Trabalho

- Para alterar uma transação do Bitcoin é necessário apresentar uma “prova de trabalho” que é inviável para o invasor
  - computacionalmente difícil para o invasor
- A prova de trabalho corresponde à sequência de hashes (*hash chain*)
- Pode ser chamada de “prova criptográfica”
- Uma prova computacional que reflete a ordem (sequência) em que as transações foram executadas

Bitcoin: A Premissa

- Para que a estratégia do Bitcoin funcione, há uma premissa que deve ser atendida:

  → a quantidade de poder computacional (processamento em CPU) do conjunto de usuários honestos deve ser maior que a dos desonestos que cooperam entre si

  - Uma premissa razoável!

Antes do Bitcoin

- Definição: uma moeda digital é uma sequência de assinaturas digitais (a chain of digital signatures)
- Cada indivíduo que faz parte do sistema (*owner*) transfere uma *transação* para o seguinte:

1) Gera um hash da última versão da transação

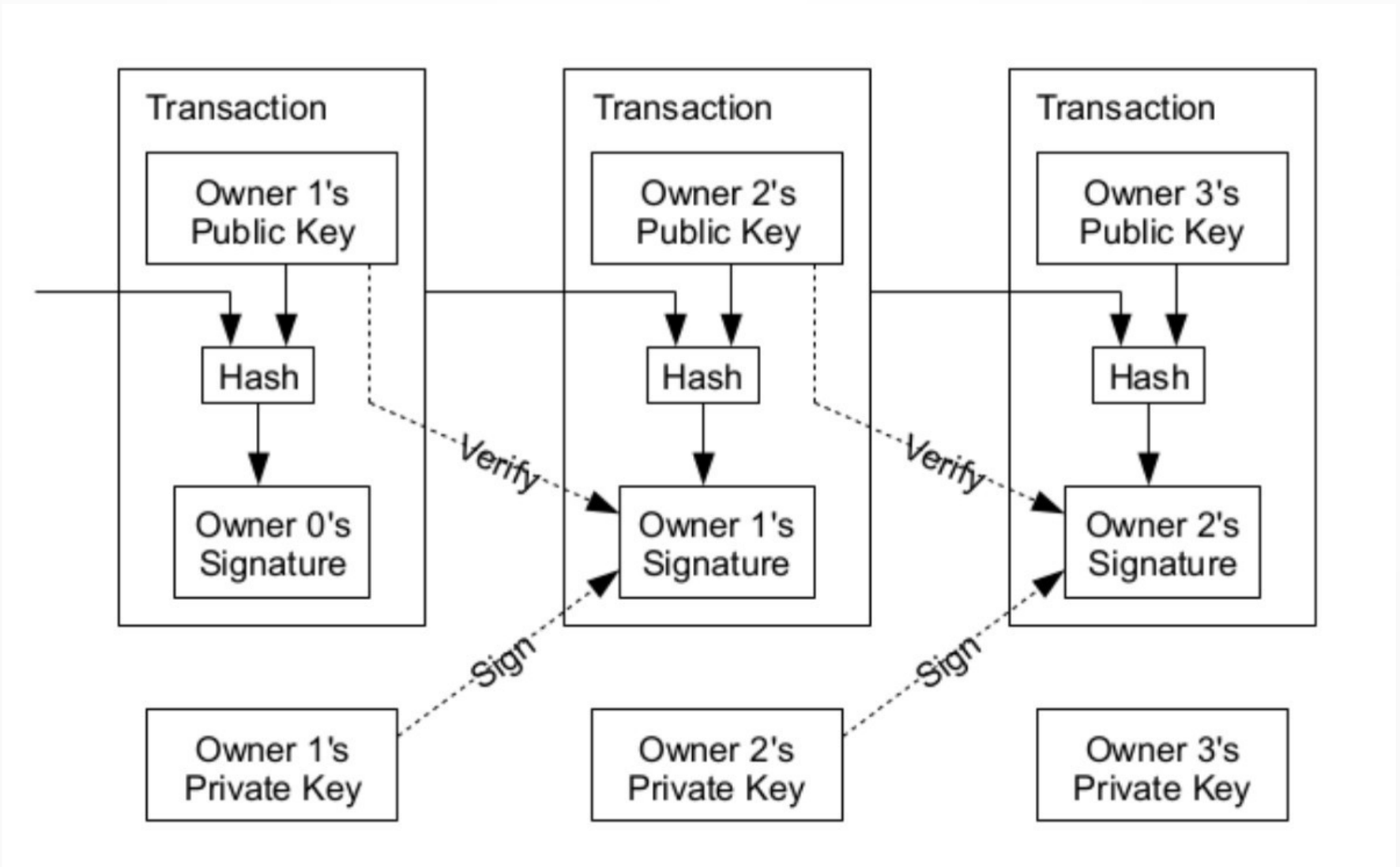
2) Criptografa com a chave pública do indivíduo seguinte e depois, mais uma vez...

3) ... o hash é criptografado com a chave privada do indivíduo processando a transação

A Transação e sua Verificação

- Uma transação consiste de um conjunto de instruções/dados mais uma sequência de hashes
- Um indivíduo que recebe a transação assinada:
  - descriptografa a assinatura com a chave pública do anterior
  - e descriptografa com a sua própria chave privada
  - recalcula o hash e vê se é o mesmo; se for está tudo certo!

Digital Signature Chain



Problemas: *fork*!

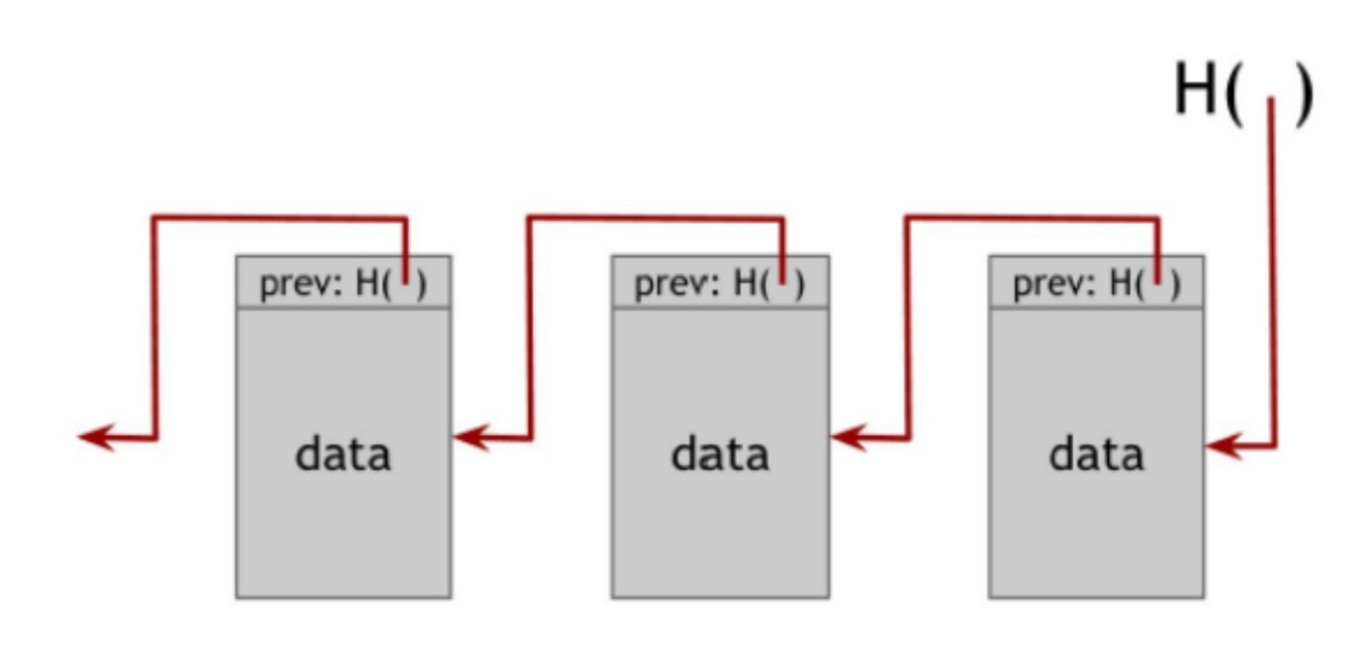
- Nesta estratégia é possível que um indivíduo [ab]use: envia uma mesma transação 2 vezes
  - para dois indivíduos seguintes, ambos aceitam!
  - muitas vezes chamado de *fork*
- Como evitar este tipo de situação?
  - podemos usar uma entidade central (um terceiro confiável) que gerencia toda a cadeia de transações
  - Garantindo que não houve abusos...
  - Ou usar a estratégia que vamos ver a seguir

Blockchain Elimina Entidade Central

- Para entender o que é um blockchain, vamos começar com uma definição importante:
- Um **apontador hash** consiste de 2 partes: (1) um apontador para onde está armazenado um dado e (2) o hash daquele dado
  - em geral o apontador hash está armazenado em um nodo e o dado em *outro* nodo
- Um blockchain é uma sequência de apontadores hash (em inglês: *hash pointer*)

Blockchain

- O hash do bloco corrente é calculado incluindo o hash do bloco anterior
  - O apontador hash é para o bloco anterior
  - Se o dado armazenado em i foi alterado indevidamente, o hash pointer de i+1 vai indicar o erro

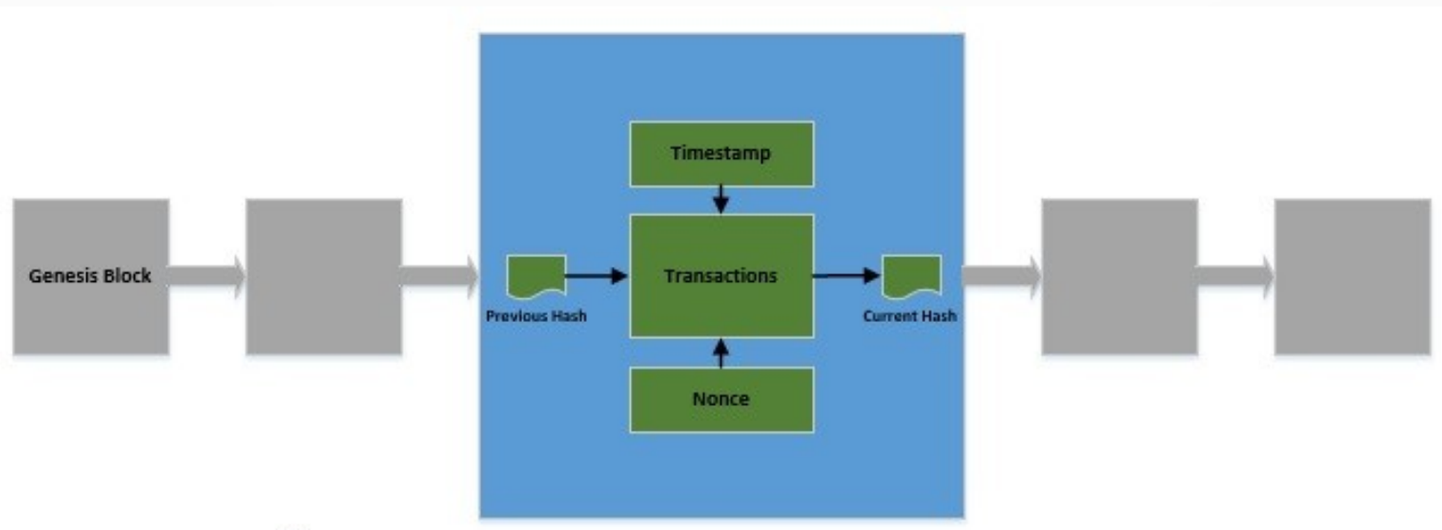


Blockchain

- Um blockchain é uma lista de dados encadeados usando apontadores hash
- O primeiro bloco da lista é chamado de bloco *genesis*
- Cada bloco contém um conjunto de transações e hashes, encadeados da seguinte forma:
  - O hash do bloco corrente é calculado incluindo o hash do bloco anterior
  - que foi calculado incluindo o hash do bloco anterior, ...

Mineração

- A geração do hash de um bloco é chamada de “mineração” do bloco
- Minerar um bloco é computacionalmente caro e serve como “prova de trabalho”



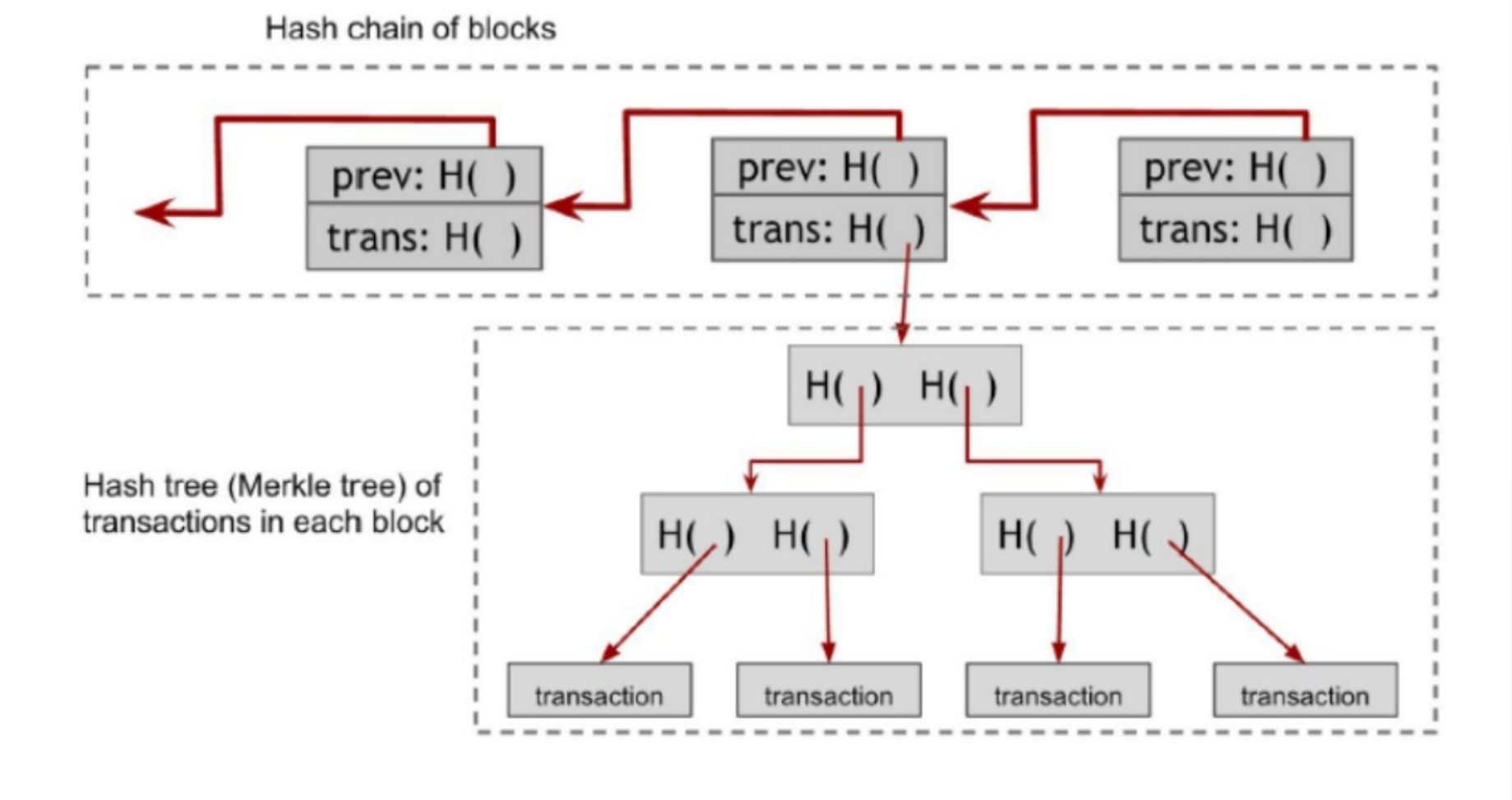
Mineração

- A mineração do bloco (isto é: a geração do seu hash) consiste, em primeiro lugar das suas transações
- O hash também inclui o timestamp da hora da sua criação
- Tem também um *nonce*, um número aleatório usado na criptografia
- Finalmente, o hash do bloco corrente é calculado incluindo o hash do bloco anterior
  - que foi calculado incluindo o hash do bloco anterior, ...

O Bloco

- Cada bloco da blockchain contém na parte de dados um conjunto de transações
- Um conjunto de transações é armazenado no Bitcoin como uma árvore binária que utiliza apontadores hash
  - São as chamadas “árvores de Merkle”

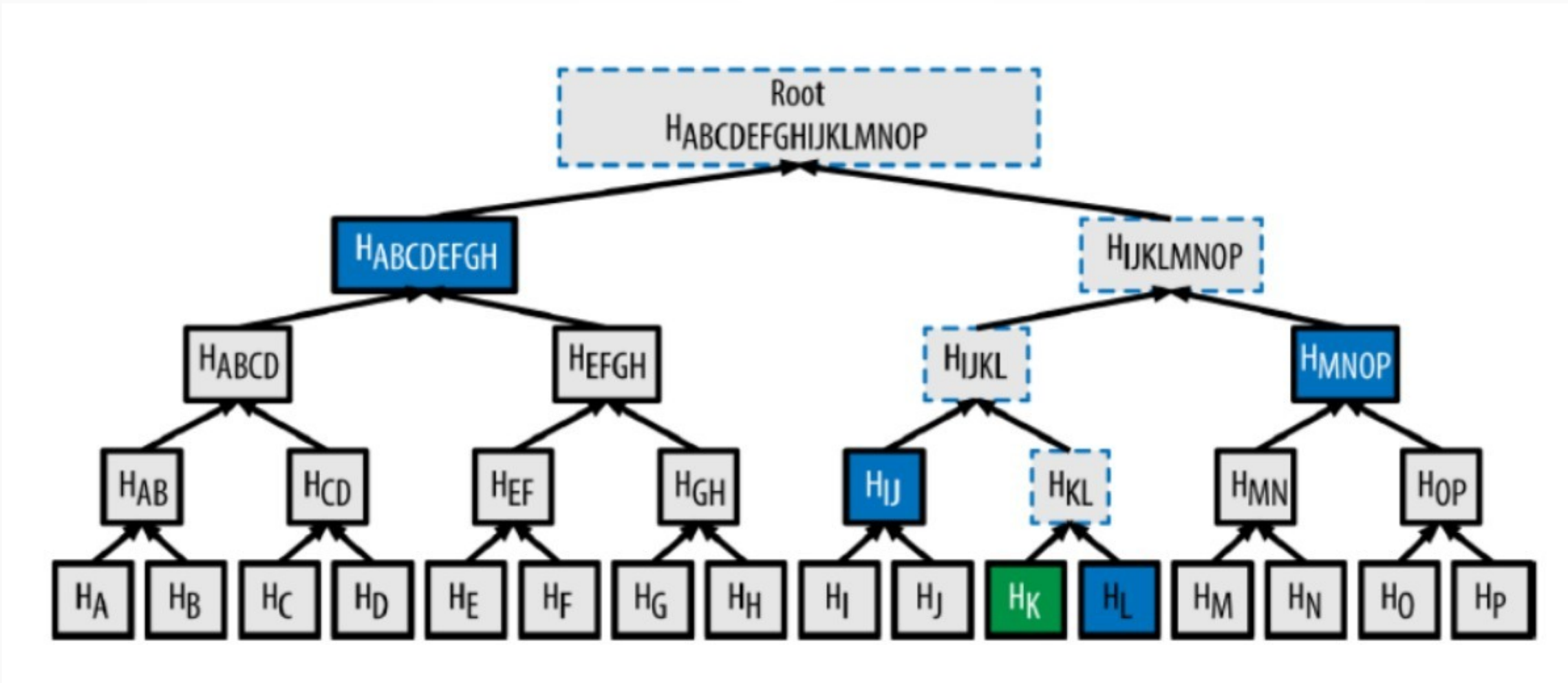
O Bloco do Bitcoin



Árvore de Merkle

- Eficiente para provar que uma transação da árvore está correta → log(n) passos para n transações
  - se diz “provar a filiação” da transação
  - em inglês: membership
- Os hashes de 2 folhas são utilizados para calcular o hash do seu pai: XOR
  - os hashes de pares de nodos internos idem
  - até chegar na raiz

Árvore de Merkle: Caminho de Merkle



Transações

- Uma transação é uma sequência de operações sobre dados (estado → operação → novo estado)
- Exemplos de operações: pagamentos ou contratos inteligentes
- Um exemplo clássico: uma transação é assinada pela origem, indica o endereço do destinatário e as entradas e saídas correspondentes
- As transações referenciam os hashes das transações anteriores que têm relação com a transação atual

Transações: Exemplo

- t1) Input: ∅; Ouput: Alice ← 25
- t2) Input: t1[0] /* referencia a 1ª op de t1 */;

  Output: Bob ← 17; Alice ← 8; (Assinado: Alice)
- t3) Input: t2[0]

  Output: Carol ← 8; Bob ← 9; (Assinado: Bob)
- t4) Input: t2[1]

  Output: David ← 6; Alice ← 2; (Assinado: Alice)

Validação de Transação

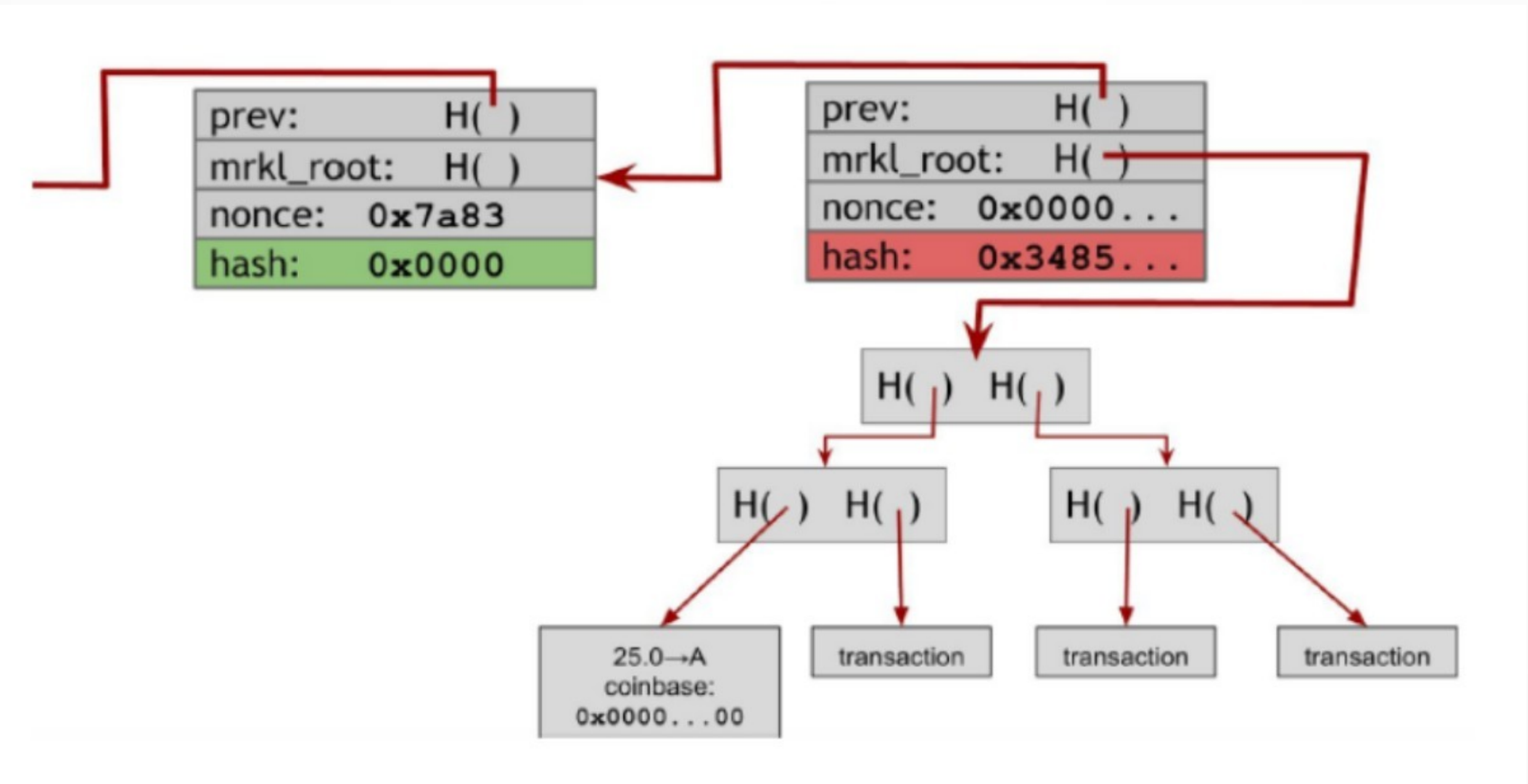
- Conferir assinaturas
- Checar nas transações anteriores se há recursos **e** que os recursos não foram gastos
- As transações são validadas para TODOS os blocos referenciados
  - de forma independente, descentralizada

Estrutura de um Bloco

- Alguns dos campos de um bloco são:

1) Apontador Hash para o bloco anterior
2) Apontador Hash para a raiz da árvore de Merkle do bloco
3) Nonce: número aleatório, obtido por desafio criptográfico, permite a validação do hash do bloco
4) O timestamp indicando o tempo físico, cronológico em que o bloco foi criado
5) Dificuldade alvo: estabelecida pela prova de trabalho

Campos Básicos de um Bloco



Outros Campos: Metadados

- Outros campos que fazem parte de um bloco são:
  - seu hash, que o identifica na blockchain como um todo
  - sua altura na corrente – o bloco gênesis tem altura 0, e daí por diante...
    - a altura indica quantos blocos foram criados desde o gênesis até o bloco corrente

Validação de um Bloco

- A validação de um bloco inclui 5 passos:

1) verifica se o bloco tem estrutura correta, bem formada

2) checa corretamente o hash do bloco

3) tamanho dentro do limite aceito pela rede

4) o conjunto de transações de um bloco é válido

5) a primeira transação (e só ela) é do tipo chamado "*coinbase transaction*" que gera novas moedas

A Prova de Trabalho do Bitcoin

- Os nodos da rede Bitcoin executam um desafio criptográfico intensivo em computação para determinar quem é o líder → mineração
- Este desafio é chamado de **prova de trabalho** (em inglês: *proof of work*)
- O líder ganha bitcoins pelo trabalho executado
- O líder propaga seu bloco para os demais, que validam o bloco
- Quando o bloco é validado por todos: terminou uma rodada

Minerando um Bloco

- Simplesmente calcular um hash para o bloco: computacionalmente fácil!
- Como fazer para complicar esta tarefa??
- Um exemplo é encontrar um hash que tenha os primeiros 5 bits iguais a zero, ou os primeiros 10 bits
- Para isso o nodo uma o nonce: gera um número aleatório e fica incrementando até chegar num hash como quer!

Minerando um Bloco

- [Passo 1] Concatena: as transações do bloco + hash do bloco anterior + timestamp + nonce
- [Passo 2] Gera o hash
- [Passo 3] Checa uma condição, por exemplo: os 5 primeiros bits são zero? Sim? Sucesso! terminou! Sai da mineração. Caso contrário vá para o [Passo 4]
- [Passo 4] nonce ← nonce + 1
- [Passo 5] volte ao [Passo 1]

Dica de Recurso Poderoso

- A seguinte página me ajudou a esclarecer bastante exatamente o que é blockchain:
- *Implementing a Simple Blockchain in Java by by Kumar Chandrakant*
  - https://www.baeldung.com/java-blockchain

Em outras palavras:

- Múltiplos nodos da rede competem (ao mesmo tempo) para minerar um bloco
- Não apenas geram o hash do bloco: também verificam se as transações do bloco são legítimas
- Ganha a corrida que termina primeiro

O Algoritmo do Bitcoin

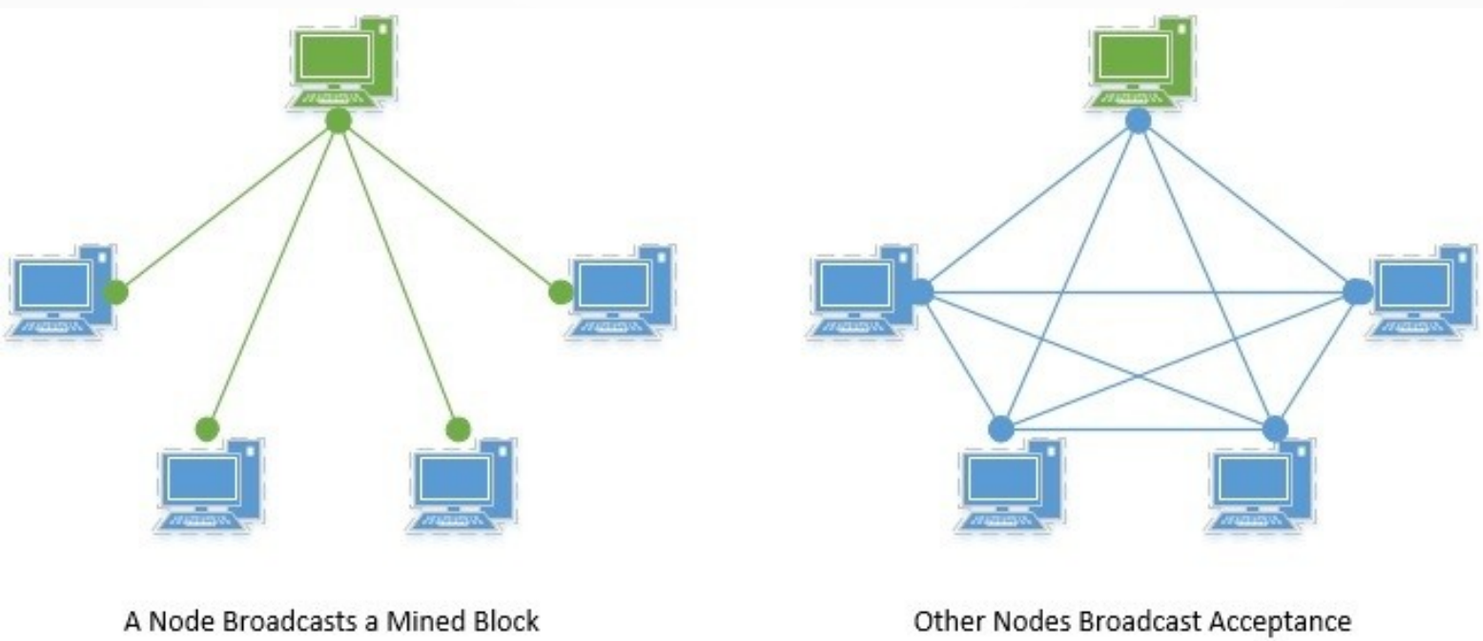
1) Request : Clientes enviam transações para todos os nós da rede;
2) Collect : Cada nodo p_i da rede, ao receber as transações, as adicionam a um bloco b_i ;
3) Election : Em cada rodada k, um líderp_l é eleito para propagar o seu bloco b_l aos demais;
4) Validate : Cada nodo p_i aceita o bloco b_l se ele é válido e se as transações contidas são válidas.
5) no próximo slide

Último Passo do Algoritmo

- Update : O nodo p_i ao aceitar o bloco b_l irá adicioná-lo ao final do blockchain e finaliza a rodada k
- Depois: agregar o hash H(b_l) ao próximo bloco a ser criado, mantendo assim a estrutura de corrente criptográfica

Acrescentando um Bloco

- Para acrescentar um bloco os nodos executam um algoritmo de consenso
- Uma maioria decide concordar



A Node Broadcasts a Mined Block

Other Nodes Broadcast Acceptance

Prova de Trabalho: Controvérsias

- A prova de trabalho (mineração) é computacionalmente intensiva → aumenta a latência para incluir um bloco
- Não é sustentável: gastos de energia e recursos que não se justificam
- Grupos de mineradores mal intensionados poderiam tomar o controle de certas decisões

Outras Aplicações

- Bitcoin é a aplicação original, e disparou a criação de moedas virtuais
- Há várias outras: baseadas nos chamados contratos inteligentes, no contexto de blockchains permissionados – em particular HyperLedger
- Recomendo um livro disponível para download em: https://www.ibm.com/topics/what-is-blockchain
  - Manav Gupta, *Blockchain for Dummies*, 3rd IBM Limited Edition, 2020.

Conclusão

- Nesta aula definimos blockchain
- Classificação: públicos e permissionados
- Estudamos o funcionamento do Bitcoin

Obrigado!

Lembrando: a página da disciplina é:
https://www.inf.ufpr.br/elias/topredes