Blockchain: O que é, como funciona, Aplicações e Desafios para o Futuro

INOVAtic NE
26 de Março de 2018
Fortaleza/CE

Prof. Marcial P Fernández, D.Sc.

Professor Associado

Universidade Estadual do Ceará (UECE)

Blockchain: Histórico

- Mecanismo para registro de transações certificadas por meio de consenso.
- Originou-se a partir da publicação do artigo "Bitcoin: A Peer-to-Peer Electronic Cash System" de Satoshi Nakamoto em 2008.
  - O autor nunca apareceu em público. Desde 2011 ele não aparece nos fóruns de Bitcoin, permanecendo como um fantasma.
  - Em 2009 ele lançou a rede Bitcoin, que é hoje a criptomoeda mais usada no mundo.
- O Blockchain é considerado uma das tecnologias mais revolucionárias e promissoras do Século XXI.

Blockchain: Registro compartilhado e distribuído

- As transações são registradas em um bloco.
  - Um bloco pode ter uma ou várias transações
  - Cada transação é assinada com uma chave pública do usuário
- Todos os nós tem uma cópia de todas as transações
  - Se um nó falhar os registros permanecem nos demais nós
- Cada bloco é certificado pelos demais participantes.
  - Se metade mais um dos participantes confirma, todas as transações do bloco são válidas.
- Como validar uma transação (block)?
  - Valor de um desafio matemático computacionalmente difícil.
  - Os “mineradores” calculam esse desafio

Blockchain: Criptografia

- Usa uma função Hash (SHA-256) para cada bloco.
  - Certifica que não houve adulteração
- Para cada entrada (registro) existe apenas um número do hash
  - Qualquer pequena mudança na entrada vai causar um novo Hash.
  - O Hash tem um tamanho fixo
- Para calcular um novo Hash quando muda a entrada não é possível deduzir do Hash anterior
  - É necessário recalcular o Hash da nova entrada.

Blockchain: Criptografia

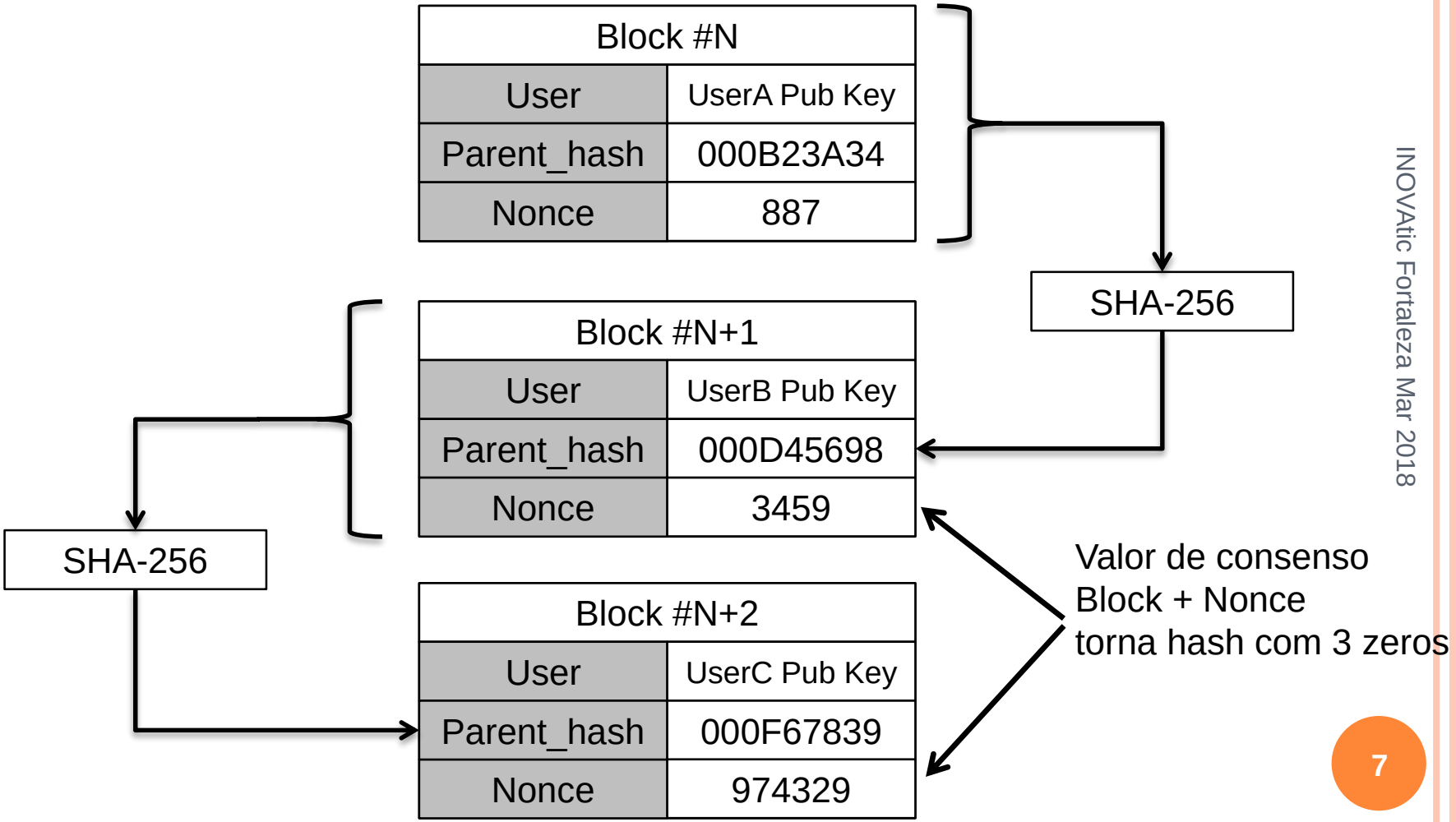
- Prova de Trabalho: desafio matemático para certificar um bloco
- Achar um número, chamado **nonce**, que somado a entrada faz que o Hash tenha uma certa quantidade de zeros
  - Lembrando: É impossível calcular a entrada a partir da saída da função hash. É preciso testar todos os números.

in 3e-05 seconds, nonce = 0 yielded 0 zeros. value = 4c8f1205f49e70248939df9c7b704ace62c2245aba9e81641edf...
in 0.000138 seconds, nonce = 12 yielded 1 zeros. value = **0**5017256be77ad2985b36e75e486af325a620a9f29c54...
in 0.000482 seconds, nonce = 112 yielded 2 zeros. value = **00**ae7e0956382f55567d0ed9311cfd41dd2cf5f0a7137...
in 0.014505 seconds, nonce = 3728 yielded 3 zeros. value = **000**b5a6cfc0f076cd81ed3a60682063887cf055e47b...
in 0.595024 seconds, nonce = 181747 yielded 4 zeros. value = **0000**af058b74703b55e27437b89b1ebcc46f45ce55d6....
in 3.491151 seconds, nonce = 1037701 yielded 5 zeros. value = **00000**e55bd0d2027f3024c378e0cc511548c94fbeed0e....
in 32.006105 seconds, nonce = 9913520 yielded 6 zeros. value = **00000**77a77854ee39dc0dc996dea72dad8852afbde6....
in 590.89462 seconds, nonce = 186867248 yielded 7 zeros. value = **0000000**225060b16117b23dbea9ce6be86ac439d....
in 4686.171007 seconds, nonce = 1424462909 yielded 8 zeros. value = **00000000**2dd743724609a9f57260e2492908d....

Blockchain: Consenso

- Uma transação válida é quando a maioria dos nós concordam com uma transação (calculam o mesmo nonce)
- Verificar é uma tarefa simples:
  - Calcula o hash adicionando o nonce e verifica a quantidade de zeros.
- Para fraudar um registro, é necessário que metade mais um dos participantes (mineradores) informem o mesmo valor errado.

Blockchain: Vamos ao jogo!



Blockchain: Aplicações

- Pagamentos
- Registro de propriedade
- Cadeia de suprimento
- Sistemas de votação
- Registro de contratos e acordos
- Cartões de fidelidade
- Autenticação de usuários
- Controle de propriedade intelectual
- Armazenamento de registros médicos
- Rastreamento de produtos controlados

Desafios do Blockchain para o Futuro

- Blockchain é ineficiente para guardar dados
  - Tamanho do arquivo (ledge) e tempo para calcular o Hash
  - Incluir no bloco apenas um endereço (URL do recurso?)
- Computadores Quânticos
  - Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, Marco Tomamichel, *Quantum attacks on Bitcoin, and how to protect against them.* **Quantum Physics**, *Nov 2017*
    - Criptografia do Bitcoin será inútil daqui a 10 anos.
  - Post-quantum cryptography?

OBRIGADO!!!!

PERGUNTAS?

marcial.fernandez@uece.br
http://marcial.larces.uece.br