CONSENSO VIA PROOF

PROOF-OF-WHAT?

Prof. Dr. Bruno de Carvalho Albertini
Curso Blockchain Developer

Mineração (PoW – *Proof-of-Work*)

- Processo de inserir um bloco no Blockchain
  - *double-spending* e cadeia mais longa
  - Exige a solução de um problema difícil
  - Verificação da solução é trivial
- Impede DoS
  - Um ataque DoS exigiria MUITO esforço computacional
- Não é dependente do *payload* da BC
  - BitCoin: não interessa a quantidade de moedas
  - Ninguém consegue "mandar" na rede

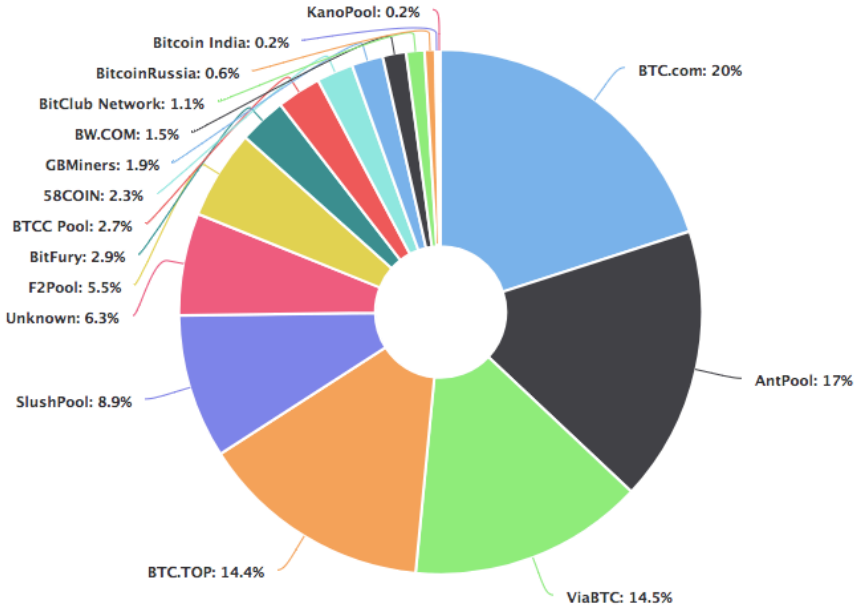
Problema difícil (PoW)

- Função de *hash* (inversão)
  - Como encontrar a entrada sabendo a saída
- Fatorização de inteiros
  - Como apresentar um número como sendo a multiplicação de dois outros números
- Cadeia de hashes
  - Se alguém suspeitar de um DoS, solicita que determinados nós encontrem um *hash*, em sequencia (encontrar uma cadeia de *hashes*)

Problemas possíveis (PoW)

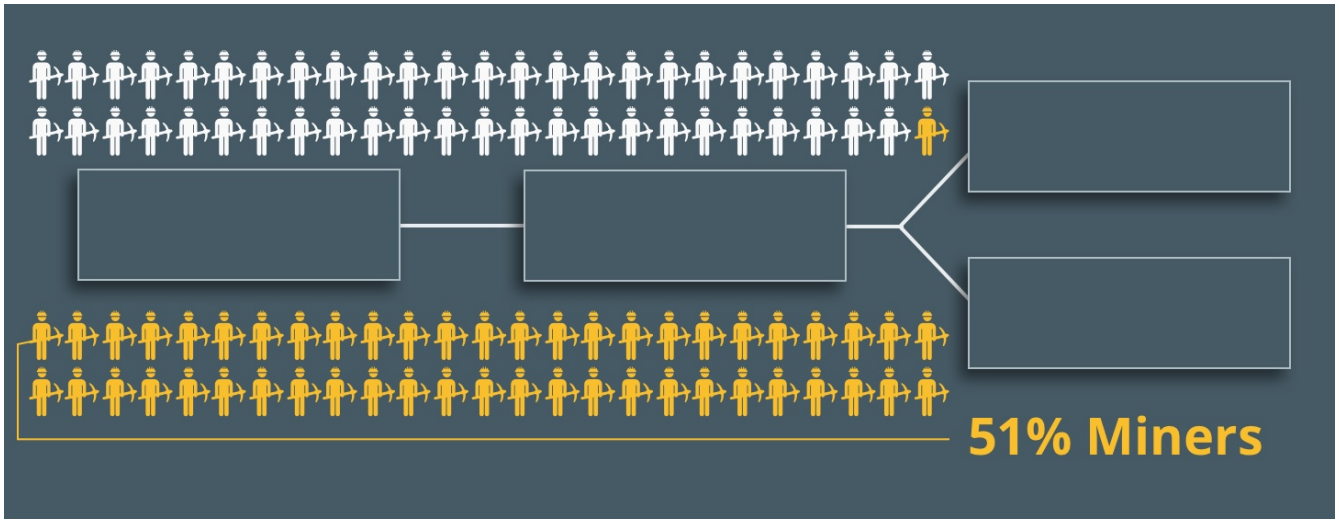
- Se muito difícil, registro de blocos demora muito
  - Se muito fácil, sujeito a DoS, spams, etc.
- A solução precisa ser remunerada
  - Minerar de graça?
- Usuário com mais $ (de verdade) pode pagar por melhor poder computacional
- Utilidade do trabalho realizado
  - Energia gasta foi desperdiçada?

Problemas possíveis (PoW)



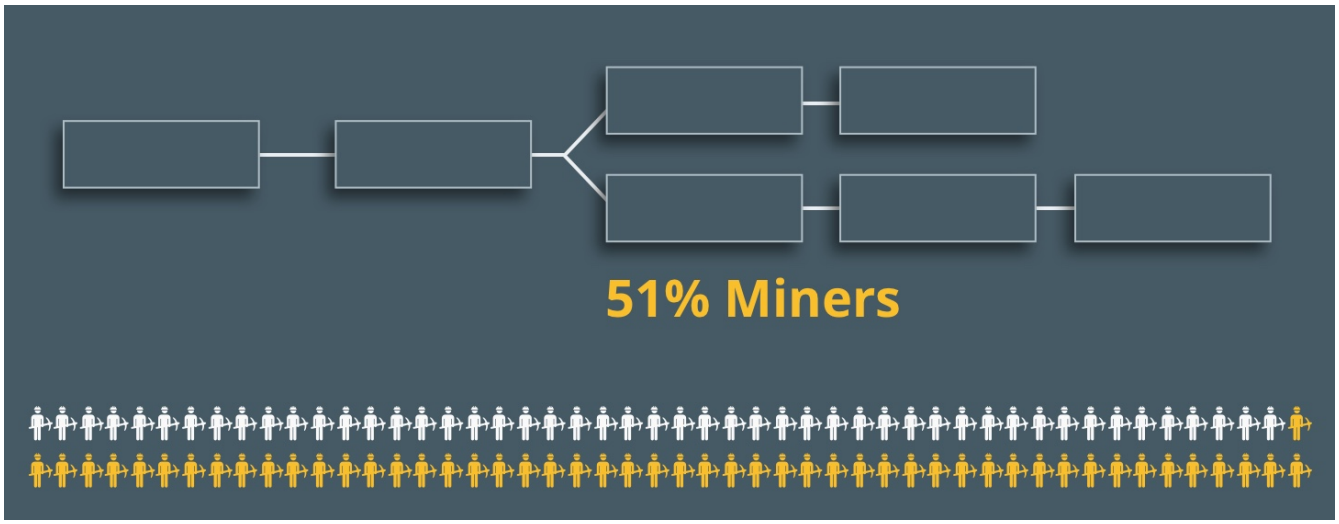
Ataque de 50%+1

- Um (grupo) de usuários domina 50%+1 do poder computacional da rede da Blockchain



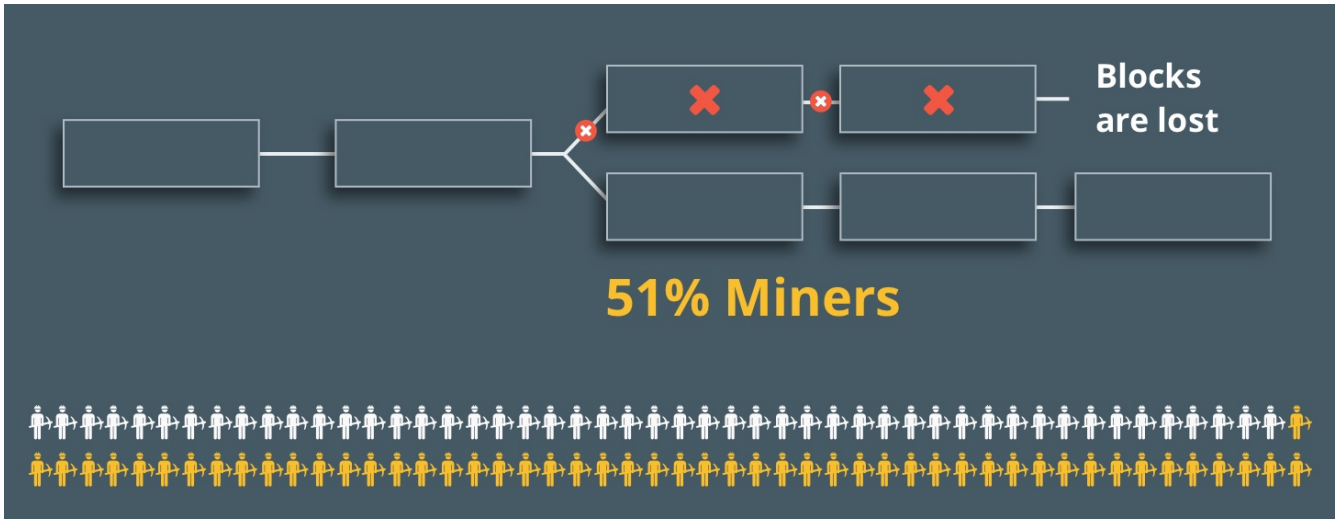
Ataque de 50%+1

- Se alguém tentar inserir um bloco, eles ignoram temporariamente, criando um *fork* dirigido



Ataque de 50%+1

- O fork dirigido eventualmente prevalece pois ele(s) detém 50%+1 do pode computacional da rede



Alternativas ao PoW

- *Proof-of-stake*
- *Proof-of-activity*
- *Proof-of-burn*
- *Proof-of-capacity*
- *Proof-of-checkpoint*
- *Zero-knowledge Proof*

PoS (*Proof-of-Stake*)

- O minerador deve provar que "possui" algo
  - Deve manter consigo durante o processo de mineração

PoS (*Proof-of-Stake*)

- O minerador deve provar que "possui" algo
  - Deve manter consigo durante o processo de mineração
- Seleção aleatória de blocos
  - Escolhe o menor valor de hash combinado com o tamanho do *stake*
  - *Stakes* são públicas (obviamente os blocos também)
  - Criptomoedas: Nxt e Blackcoin

PoS (*Proof-of-Stake*)

- Idade das moedas
  - Número de moedas enviadas multiplicado pela média de idade das moedas
  - Idade: quantidade de tempo em que as moedas ficaram disponíveis (*unspent*)
  - As moedas sempre ficam 30 dias de molho antes de poderem competir pelo próximo bloco

Variações de PoS

- *Proof of Stake Anonymous* (PoSA)
  - Usuários encobertam o PoS fornecendo as transações, outros usuários fornecem os dados das transações
  - Há remuneração pela anonimização
  - Foco em anonimizar quem está realizando o PoS
  - Criptomoedas: Cloakcoin

Variações de PoS

- *Delegated Proof of Stake* (DPoS)
  - Usuários votam por um delegado para montar o próximo bloco
  - Criptomoedas: Bitshares
- *Proof of Importance* (POI)
  - Cada conta tem um nível de importância baseado na sua atividade e confiança
  - Nível usado para decidir PoS
  - Criptomoedas: NEM

Variações de PoS

- *Proof of Storage*
  - Usa uma árvore de blocos
  - Cada usuário vê as transações relevantes para ele (na ordem da árvore) e cada nós na árvore mantém uma mini-blockchain
  - Contribuição para o armazenamento global dá o direito ao PoS
  - Criptomoedas: Storj

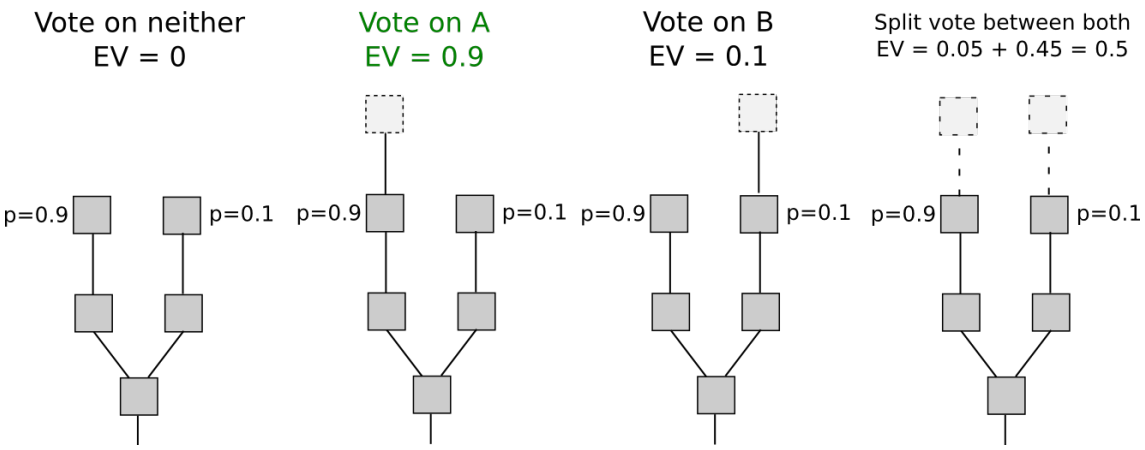
Variações de PoS

- *Proof of Stake Time* (PoST)
  - Usa a idade das moedas, mas relativa ao tempo em que elas ficaram em uma carteira
  - Evita que os ricos fiquem mais ricos
  - Criptomoedas: Vericoin
- *Proof of Stake Velocity* (PoSV)
  - Número de moedas e nível de atividade usando-as
  - Criptomoedas: Reddcoin

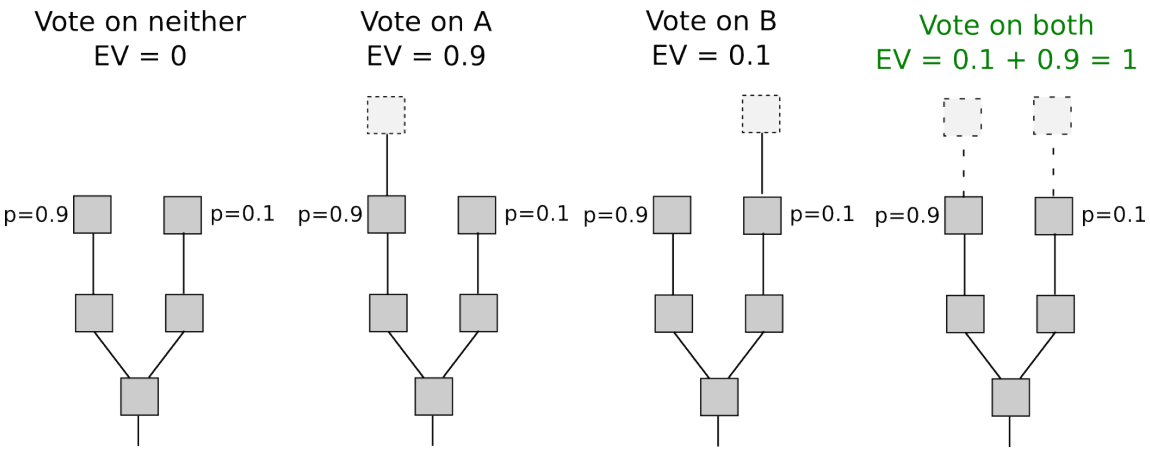
Diferenças PoW-PoS

- PoS é mais eficiente
  - Não é necessário HW específico
  - Não é focado no poder computacional (energia)
- Mais mineradores
  - Qualquer um pode se tornar um nó
- Problema do *Nothing-at-Stake*
- Ataque Sybil

Nothing-at-Stake

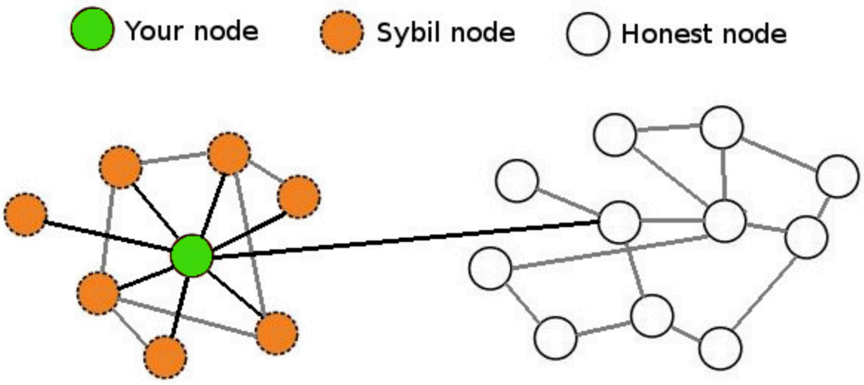


Nothing-at-Stake



Ataque Sybil

- O minerador forja várias identidades para a rede
- Quando há uma disputa por *stake*
  - Cada identidade envia seu "*stake*"



Proof-of-Activity

- Seleciona um nós aleatoriamente na rede para montar o próximo bloco
  - Elimina os problemas PoW e PoS
    - Inclusive o ataque de 50%+1
  - Muitas mensagens para decidir!
    - Cada nó da rede deve enviar uma mensagem para todos na rede e receber uma mensagem de cada um da rede
    - Mecanismo de garantia de envio/recebimento dobra a quantidade de mensagens
    - Particionamento inviabiliza o método

PoB – Proof-of-Burn

- Minerador gasta moedas para ter o direito de montar o próximo bloco
  - Envia as moedas para um endereço que nunca poderá gastá-las
- Competição pode tonar a moeda inviável
  - Inflação virtual

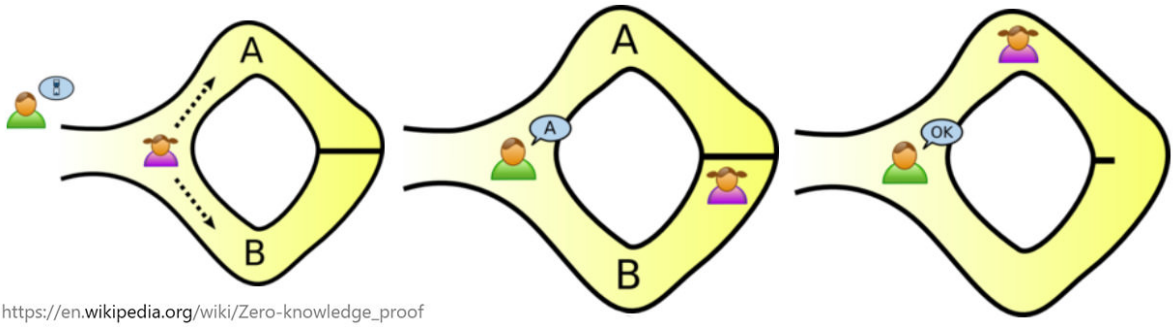
PoC – *Proof-of-Capacity*

- AKA *Proof-of-Space*
- Usuário deve provar que usou um recurso computacional qualquer
  - Disco rígido ou memória
- Implementações
  - Mensagens muito longas
  - *Hash* contínuo de áreas (começando por um dado público, e.g. chave pública)

Proof-of-Checkpoint

- Modo híbrido
  - A cada X blocos minerados por PoS, faz um PoW
- Visa eliminar os problemas de ambos
- Redes separadas para PoS e PoW
  - Cada bloco PoW está ligado a ambas
  - Normalmente o bloco PoW não tem transações

Zero-Knowledge-Proof



https://en.wikipedia.org/wiki/Zero-knowledge_proof

Zero-Knowledge-Proof

- Minerador diz: “este bloco de transações é válido”
  - Outros da rede podem verificar se isso é verdade
  - Não é necessário saber quais transações
- Não há uma autoridade central
  - Código do Blockchain verifica aleatoriamente um nó
  - Nó verificado tem a chance de validar um bloco
- Criptomoedas: ZCash