Tópicos em Segurança da Informação
Aula Mineração

Ivan Sendin

FACOM - Universidade Federal de Uberlandia
ivansendin@yahoo.com,sendin@ufu.br

28 de maio de 2024

- Tentar ganhar dinheiro com bitcoin é coisa de criminoso, diz professor da USP

"Bitcoin, por exemplo, só gasta energia, não gera nada útil
(desenvolvimento, retorno e bem estar social, o que for! -
e ainda gasta recursos naturais/energia),
e na maioria das vezes é golpe!
Quer investir, invista em algo que seja positivo para o país,
para a indútria, para todos: ações!"

E ai???

- Quase simulamos um cenario de mineração
- A prova de trabalho "controla" o numero de opiniões que voce pode dar
- "Uma CPU = Um Voto"
- Faltou a informação do "negocio"
  Raiz da arvore de Merkle
- Falha no exercicio: faltou a competição por cada bloco
- Se a nota fosse proporcional ao numero de blocos minerados....

- Alguem publicou um bloco descaradamente errado!!
- Muitos(todos acima) seguiram esse caminho errado

Resumo

- Mineradores mineram para produzir um novo bloco
- (PoW ja esta estabelecido como funciona...certo?)
- Ao gerar o novo bloco, o minerador faz a proposta (para os seus vizinhos...)
- Ao receber um bloco, o minerador
  1. Verifica se o bloco é "novo"
  2. **verifica** a corretude
  3. espalha este novo bloco
- Quem gera ou recebe um bloco n inicia a mineração pelo bloco $n + 1$

Resumo

- Ao encontrar o prova de trabalho o minerador ganhou a loteria
- E se o minerador publicar um bloco com informação de negocio falsa
  "Eu sou a pessoa mais rica do mundo"
- (o protocolo do Bitcoin define precisamente o que esta correto ou não)

Resumo

- Existe a expectativa que a maioria dos participantes honestos
- Honestidade pragmática
- Se uma fração da rede decidir fraudar o sistema, criando informações falsas....
- Se a fração for “pequena” a blockchain fraudada será pequena e não terá efeito de fato...investimento dos fraudadores será perdido
- Ser a fração for grande, a blockchain não seguirá o protocolo...o Bitcoin perde a confiança e todo mundo perde
- A Verdade/Corretude esta na maioria...e não em um conceito abstrato(?) de verdade
- Ataque dos 51%

- Forks
- Dois computadores geram ao mesmo tempo o seu bloco (BL_A^n e BL_B^n), e espalham pela rede
  Rede complexa...
- Regra: trabalhar na maior cadeia
- A rede fica “dividida” e empatada
- A rede vai ficar ”dividida”, parte trabalhando sobre BL_A^n e parte sobre BL_B^n,

- Por exemplo, alguem gera BL_A^{n+1} e propaga pela rede.
- Quem estava minerando BL_B^n, inicia a mineração em BL_A^{n+1} (maior chain...)
- os mineradores abandonam a cadeia menor
- (algum minerador "perde" a mineração)
- (algumas transações serão desfeitas!)
- E se "empatar" de novo??
- Garantias probabilisticas

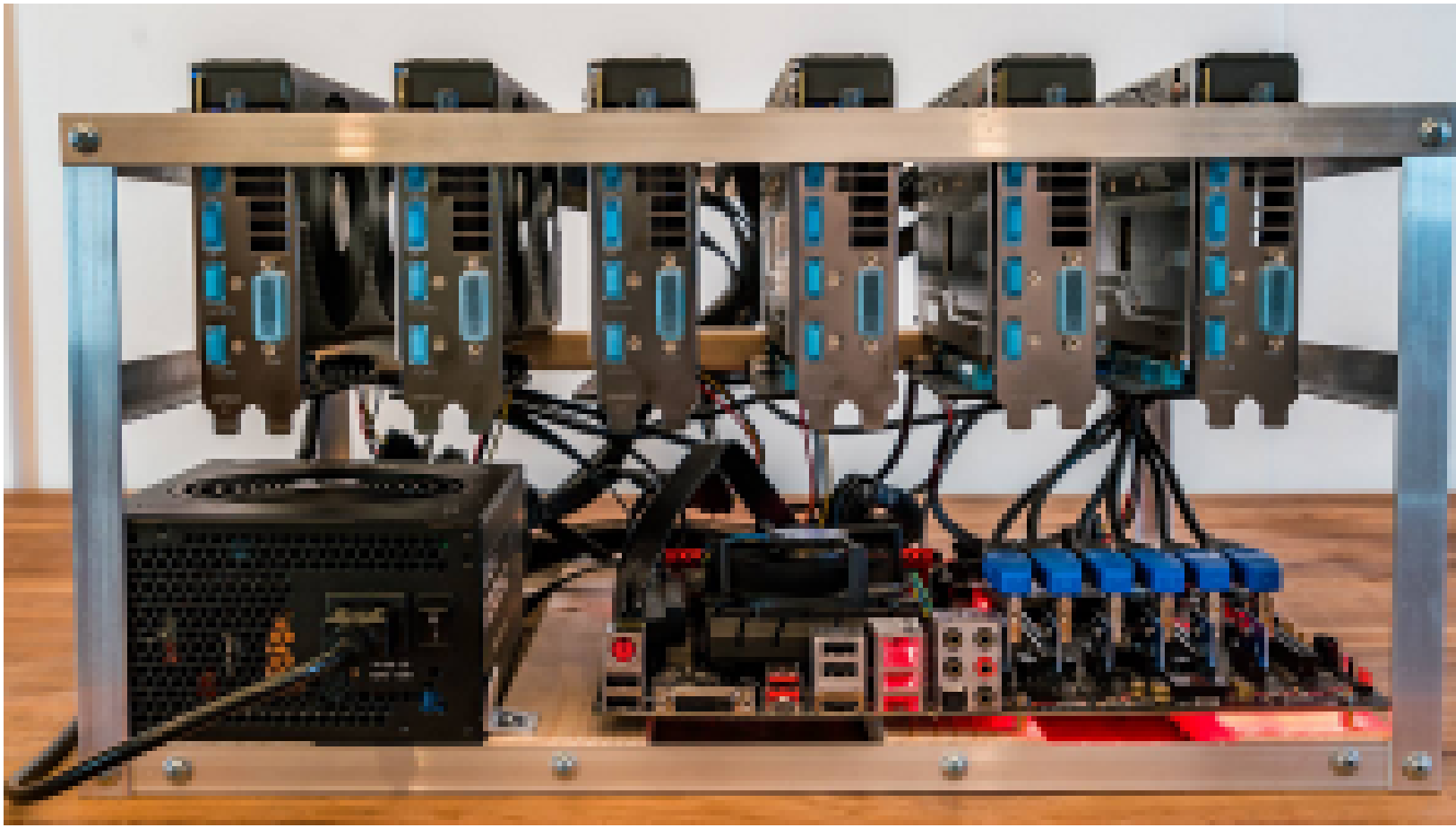
- A probabilidade de minerar o bloco n é a sua proporção de "poder de CPU" na janela
- Analogia ao bilhete de loteria
  Quem é sorteado pode escrever na blockchain....pode escrever besteira
- CPU, GPU e hoje é feita em ASIC
  Google: Genesis...AntMiner

- Uma CPU, um voto
- CPU: 20 MHash/s
- GPU: 5 a 2000 MHash
- ASIC: 1 a 14 THash/s
- (2017)
- Global: $\approx 10^9$ TH/s (2019)
- Qual é a probabilidade de uma CPU minerar?? Comparar com a MegaSena...

$$\frac{20Mega}{10^9 Tera} \approx \frac{20Mega}{10^{15} Mega} = \frac{20}{10^{15}} = \frac{2}{10^{14}}$$

$$\text{MegaSena} \approx \frac{1}{60^6} = \frac{1}{6^6 10^6} = \frac{1}{36 \times 10^6} = \frac{1}{3.6 \times 10^7}$$

Pelo menos vc tem uma tentativa a cada 10 minutos....




ANTMINER


+12V
GND
ANTMINER

Mineração Na Nuvem

- Compra um hashpower
- (Eram contratos de tempo ilimitado...)
- Taxa de manutenção
- Hashflare, Genesis, ...
- Lugares Frios, geotermica, hidroeletrica propria,...
- Facilidade de hardware
- **Ganho na escala**

Problemas...

- As mineradoras centralizam o Bitcoin $\approx 20\%$
- Uma CPU, um voto....
- TTP??

Proof of Stake

- Prova de participação/posse
- Prova de trabalho: consumo inútil(?) de energia
- (pegada de carbono...)
- Varias implementações

Proof of Stake

- O "minerador" investe um valor de criptomoedas em "mineração PoS"
  Equivalente a comprar Hardware
- A probabilidade de minerar é proporcional ao valor investido (em relação ao total)
- O ganhador da loteria é que tiver o maior:

$$\mathcal{H}(Id, hashanterior, ...)/2^{256} * Saldo(Id)$$

- Os participante começam a propagar o seus proprios blocos...
- Quando receber um bloco "maior" desistem e propagam o bloco maior

Proof of Stake

- Os mineradores são os maiores interessados nas criptomoedas
- Investimento em hardware(PoW) e criptomoedas (PoS)
- Tecnicamente eles podem fraudar...
- Mas: risco de perda de credibilidade
- (Eles ganham mais Bitcoin...mas o Bitcoin desvaloriza!!)

- Provas de trabalho Diferentes
  Memória, por exmplo
- Trabalho útil
- Proof of Burn Just Enough Security: Reducing Proof-of-Work Ecological Footprint 0.24% do consumo de energia !
- Veja também o Consenso do Ripple

Mineradora Bitcoin Antminer T17+ 58t Bitmain V2.01

R$ 15.000

em 10x R$ 1.500 sem juros

Frete grátis

Nerdminer V2 Com Tela, Case E Cabo - Minerador Solo Bitcoin

5.0 ★★★★★ (6)

~~R$ 399~~

R$ 325[85] 18% OFF

em 10x R$ 32[58] sem juros

Frete grátis

Nerdminer V2 - Minerador Bitcoin (completo)

R$ 298[99]

em 9x R$ 33[22] sem juros

Frete grátis

Mineradora De Bitcoin Spondooliestech Sp20 1,7th/s 1200w

R$ 6.510

em 10x R$ 651 sem juros

Frete grátis

Mineradora 4th/s Bitcoin Sha256 Avalon Nano3 Novo C/garantia

~~R$ 4.299~~

R$ 3.611 16% OFF

em 12x R$ 347[09]

Frete grátis

Nerdminer V2 (minerador Solo Bitcoin) + Case

R$ 278

em 9x R$ 30[89] sem juros

Frete grátis

Disponível 9 dias após sua compra

Pool de Mineradores

- "Loteria"
- A longo prazo, a estatística "funciona melhor"
- Mesmo assim é um negocio arriscado: e se o equipamento quebrar? e se a criptomoeda deixar de existir? Quem paga a conta de luz até voce conseguir minerar?
- Estratégia para dimunuir o risco: fazer um pool de mineradores

Pool de Mineradores

- Um nó faz a "montagem" do bloco
  A string do trabalho de voces...
- Vários nós fazem a prova de trabalho
  Cada um busca em um "espaço" diferente
- Pagamento: trabalho mais fáceis
  - Por exemplo, uma prova de trabalho de 20 bits é a utilizada na criptomoedas...
  - ...quando o minerador obtem uma prova de 10 bits ou mais, ele envia para o nó principal
  - E recebe um pagamento proporcional
  - (O Pool não precisa confiar nos participantes, já o contrário...)

Selfish Mining

- Desvio do Protocolo
- "Incentive Compatible"
  Teoria dos Jogos
- "block withhold"
- Se eu minero o bloco n e não conto para ninguem!!!
- ..até minerar o bloco $n + 1$
- Consequencias?!?