

# Variação do Nonce



# Variação do Nonce

Número de 32-bit  
(sem sinal)



Bloco: #3

Nonce:

Dados:

Fernando -> Hadelin 500 hadcoins

Fernando -> Ebay 100 hadcoins

Hadelin -> Joe 70 hadcoins

Hash Anterior: 0000DF2E57FB432A

Hash:



0

4 bilhões



# Variação do Nonce

Algumas estimativas:

Dificuldade:

Todos números hexadecimais de 64 dígitos possíveis:  $16 \times 16 \times \dots \times 16 = 16^{64} \approx 10^{77}$

Total de hashes válidos (com 18 zeros à esquerda):  $16 \times 16 \times \dots \times 16 = 16^{64-18} \approx 2 \times 10^{55}$

Probabilidade de gerar um hash válido aleatoriamente:  $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0,00000000000000000002\%$

Nonce:

O Nonce é um número de 32-bit, o nonce máximo =  $2^{32} = 4,294,967,296 = 4 \times 10^9$

Supondo que não haja colisões, isso significa  $4 \times 10^9$  hashes diferentes

Probabilidade que um deles seja válido:  $4 \times 10^9 \times 2 \times 10^{-22} = 8 \times 10^{-13} \approx 10^{-12} = 0,0000000001\%$



Conclusão: a variação de um Nonce não é suficiente

# Variação do Nonce



Um minerador modesto faz 100 milhões de hashes por segundo  
 $4 \text{ bilhões} / 100 \text{ milhões} = 40 \text{ segundos}$



# Variação do Nonce



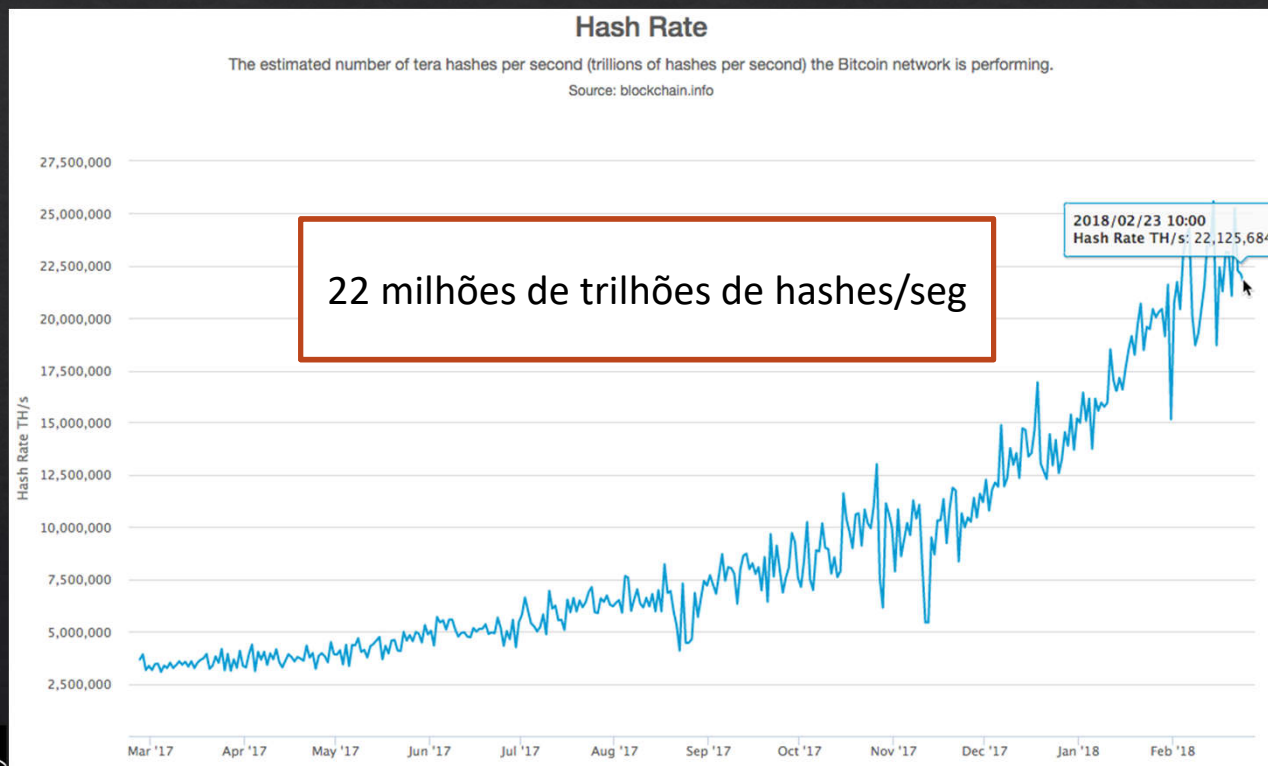
Bloco: #3
Timestamp: 1519181244
Nonce:
Dados: Fernando -> Hadelin 500 hadcoins Fernando -> Ebay 100 hadcoins Hadelin -> Joe 70 hadcoins
Hash Anterior: 0000DF2E57FB432A
Hash:



# Variação do Nonce



# Variação do Nonce



**PROF. FERNANDO AMARAL**  
www.datascientist.com.br