Variação do Nonce

PROF. FERNANDO AMARAL
www.datascientist.com.br

Variação do Nonce

PROF. FERNANDO AMARAL
www.datascientist.com.br

Variação do Nonce

Algumas estimativas:

Dificuldade:
Todos números hexadicimais de 64 digitos possíveis: $16 \times 16 \times \ldots \times 16 = 16^{64} \approx 10^{77}$
Total de hashes válidos (com 18 zeros a esquerda): $16 \times 16 \times \ldots \times 16 = 16^{64-18} \approx 2 \times 10^{55}$
Probabilidade de gerar um hash válido aleatóriamente: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0{,}00000000000000000002\%$

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 4×10^{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

PROF. FERNANDO AMARAL
www.datascientist.com.br

Variação do Nonce

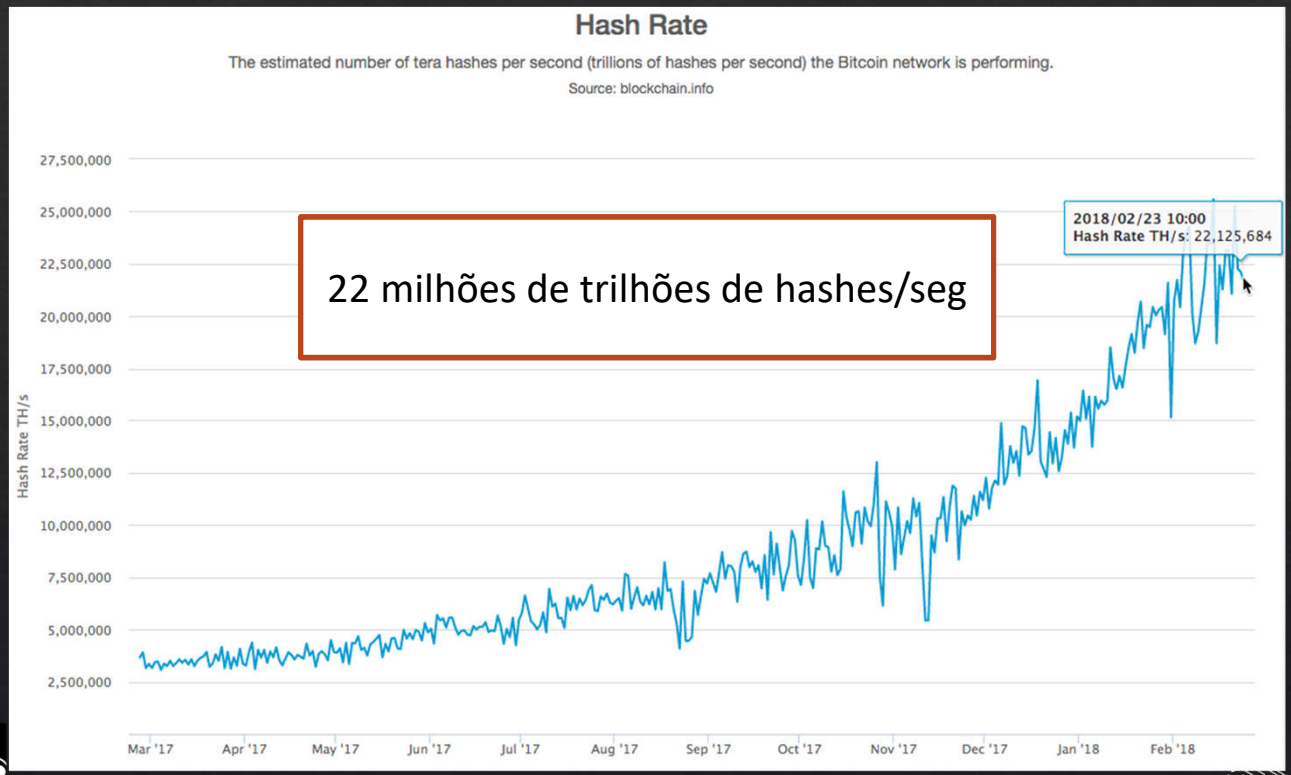
Um minerador modesto faz 100 milhões de hashes por segundo
4 bilhões / 100 milhões = 40 segundos

Variação do Nonce

Variação do Nonce

PROF. FERNANDO AMARAL
www.datascientist.com.br

Variação do Nonce



PROF. FERNANDO AMARAL
www.datascientist.com.br