



Mineração

# Blocos

Bloco 1			
01/01/00			
Débito	Crédito	Valor	
José Dias	Maria Aparecida	0,005	
Pedro Antônio	Fernando Salgado	0,5	
Ruth Arittoles	Michael Tofpht	1	
96E7F4452			



Bloco 2			
02/01/00			
Débito	Crédito	Valor	
José Dias	Maria Aparecida	0,005	
Pedro Antônio	Fernando Salgado	0,5	
Ruth Arittoles	Michael Tofpht	1	
96E7F4452			
2415D595			



Bloco 3			
02/01/00			
Débito	Crédito	Valor	
José Dias	Maria Aparecida	0,005	
Pedro Antônio	Fernando Salgado	0,5	
Ruth Arittoles	Michael Tofpht	1	
2415D595			
2D61091C5			

## Considerações

- Um hash é um número, porém em formato hexadecimal
- Pelo efeito avalanche, não sabemos que número será gerado!



# Todos os Hashs possíveis



Bloco 1

01/01/00

Débito	Crédito	Valor
José Dias	Maria Aparecida	0,005
Pedro Antônio	Fernando Salgado	0,5
Ruth Arittoles	Michael Tofpht	1

Nonce: ?

Timestamp

Hash:

- Você precisa gerar um hash limitado a um intervalo
- Você pode altear nonce e timestamp

1 ~ 10.000



1

10<sup>77</sup>



Bloco 1		
01/01/00		
Débito	Crédito	Valor
José Dias	Maria Aparecida	0,005
Pedro Antônio	Fernando Salgado	0,5
Ruth Arittoles	Michael Tofpht	1
Nonce: 1		
Timestamp: <b>1590097614</b>		
Hash: 6B51D431DF5D		

1 ~ 10.000



1



10^77



Bloco 1		
01/01/00		
Débito	Crédito	Valor
José Dias	Maria Aparecida	0,005
Pedro Antônio	Fernando Salgado	0,5
Ruth Arittoles	Michael Tofpht	1
Nonce: 2		
Timestamp: <b>1590097614</b>		
Hash: B4D999A68		

1 ~ 10.000



1

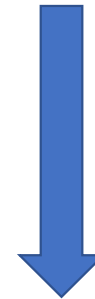


Bloco 1		
01/01/00		
Débito	Crédito	Valor
José Dias	Maria Aparecida	0,005
Pedro Antônio	Fernando Salgado	0,5
Ruth Arittoles	Michael Tofpht	1
Nonce: 3		
Timestamp: <b>1590097614</b>		
Hash: CC197EB410B		

1 ~ 10.000



1



10<sup>77</sup>





Bloco 1		
01/01/00		
Débito	Crédito	Valor
José Dias	Maria Aparecida	0,005
Pedro Antônio	Fernando Salgado	0,5
Ruth Arittoles	Michael Tofpht	1
Nonce: 3.451.213.215		
Timestamp: <b>1590097614</b>		
Hash: 254B		



1 ~ 10.000



1

10<sup>77</sup>



# Quebra cabeça criptográfico

- Achar o hash no intervalo especificado é denominado "quebra cabeça criptográfico"
- A única forma de encontra-lo é por "força bruta"
  - Custa tempo e energia elétrica: Alto custo computacional



# Regra!

- Só consegue adicionar um novo bloco ao Blockchain quem "desvendar" o quebra cabeças!




# Perguntas




Por que é preciso minerar?

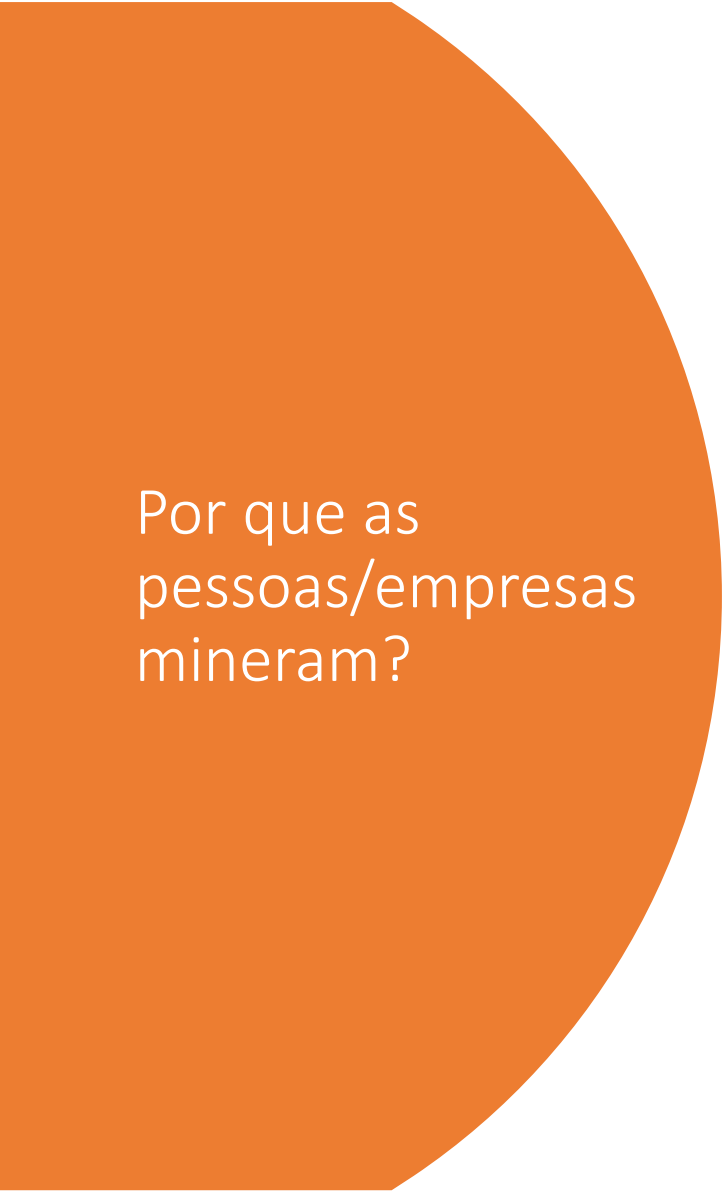


Por que as pessoas/empresas  
mineram?

A large orange shape on the left side of the slide, consisting of a rectangle with a quarter-circle cutout on its right side.

Por que é  
preciso  
minerar?

- A única forma de "produzir" novas criptomoedas é através da mineração
  - O esforço/dificuldade/raridade para minerar torna a criação da moeda valiosa
  - Consequentemente, a moeda criptográfica tem valor agregado
- 
- A decorative yellow line in the bottom right corner, composed of several short, curved segments that form a larger, sweeping curve.

A large orange shape on the left side of the slide, consisting of a rectangle with a quarter-circle cutout on its right side.

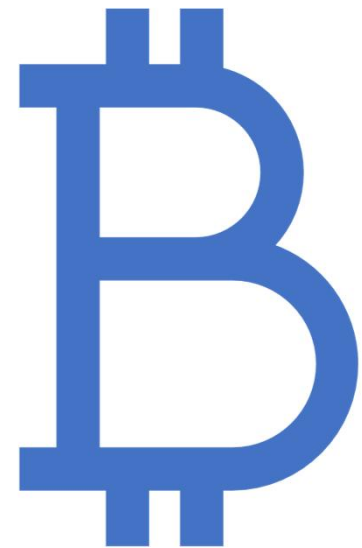
Por que as  
pessoas/empresas  
mineram?

Porque existe uma recompensa financeira (em  
moedas criptográficas) para quem consegue  
resolver o quebra cabeças criptográfico!



## Exemplo:

- Minerar 1 bloco: 12,5 bitcoins
- Cotação do bitcoin: R\$ 50.000,00
- Recompensa: R\$ 625.000,00
- Mas tem mais!





# Taxas

- Além disso mineradores recebem "taxas"
  - Valores incluídos pelos usuários para incluir suas transações no bloco!







# Pools de Mineração

- Grupos de Mineração: mineram em conjunto!



# Mempool

As transações não são incluídas automaticamente em um bloco

Os mineradores montam blocos escolhendo as transações

Escolhem as transações com maiores taxas!

Diferentes mineradores podem tentar minerar mesmos blocos (mesmo número) ao mesmo tempo!

# Competição!

## Menpool

Débito	Crédito	Valor
Marcio Delgado	Pablo Avini	0,005
Pedro Antônio	Fernando Salgado	0,5
Leão Dias	Michael Tofpht	1
José Dias	Maria Aparecida	2
Ruth Arittoles	Michael Tofpht	0,6

Bloco 5000		
02/01/00		
Débito	Crédito	Valor
Marcio Delgado	Pablo Avini	0,005
Pedro Antônio	Fernando Salgado	0,5
Leão Dias	Michael Tofpht	1
96E7F4452		
2415D595		

Podem Haver  
Transações Comuns

Bloco 5000		
02/01/00		
Débito	Crédito	Valor
José Dias	Maria Aparecida	2
Pedro Antônio	Fernando Salgado	0,5
Ruth Arittoles	Michael Tofpht	0,6
2415D595		
2D61091C5		

# Competição!

## Menpool

Débito	Crédito	Valor
Marcio Delgado	Pablo Avini	0,005
Pedro Antônio	Fernando Salgado	0,5
Leão Dias	Michael Tofpht	1
José Dias	Maria Aparecida	2
Ruth Arittoles	Michael Tofpht	0,6

Bloco 5000		
02/01/00		
Débito	Crédito	Valor
Marcio Delgado	Pablo Avini	0,005
Pedro Antônio	Fernando Salgado	0,5
Leão Dias	Michael Tofpht	1
96E7F4452		
2415D595		



Bloco 5000		
02/01/00		
Débito	Crédito	Valor
José Dias	Maria Aparecida	2
Pedro Antônio	Fernando Salgado	0,5
Ruth Arittoles	Michael Tofpht	0,6
2415D595		
2D61091C5		

