BLOCKCHAIN

DESAFIOS E OPORTUNIDADES

MARCELO FREITAS

O que significa **ter** um **Bitcoin**?

Moeda digital

Governo central

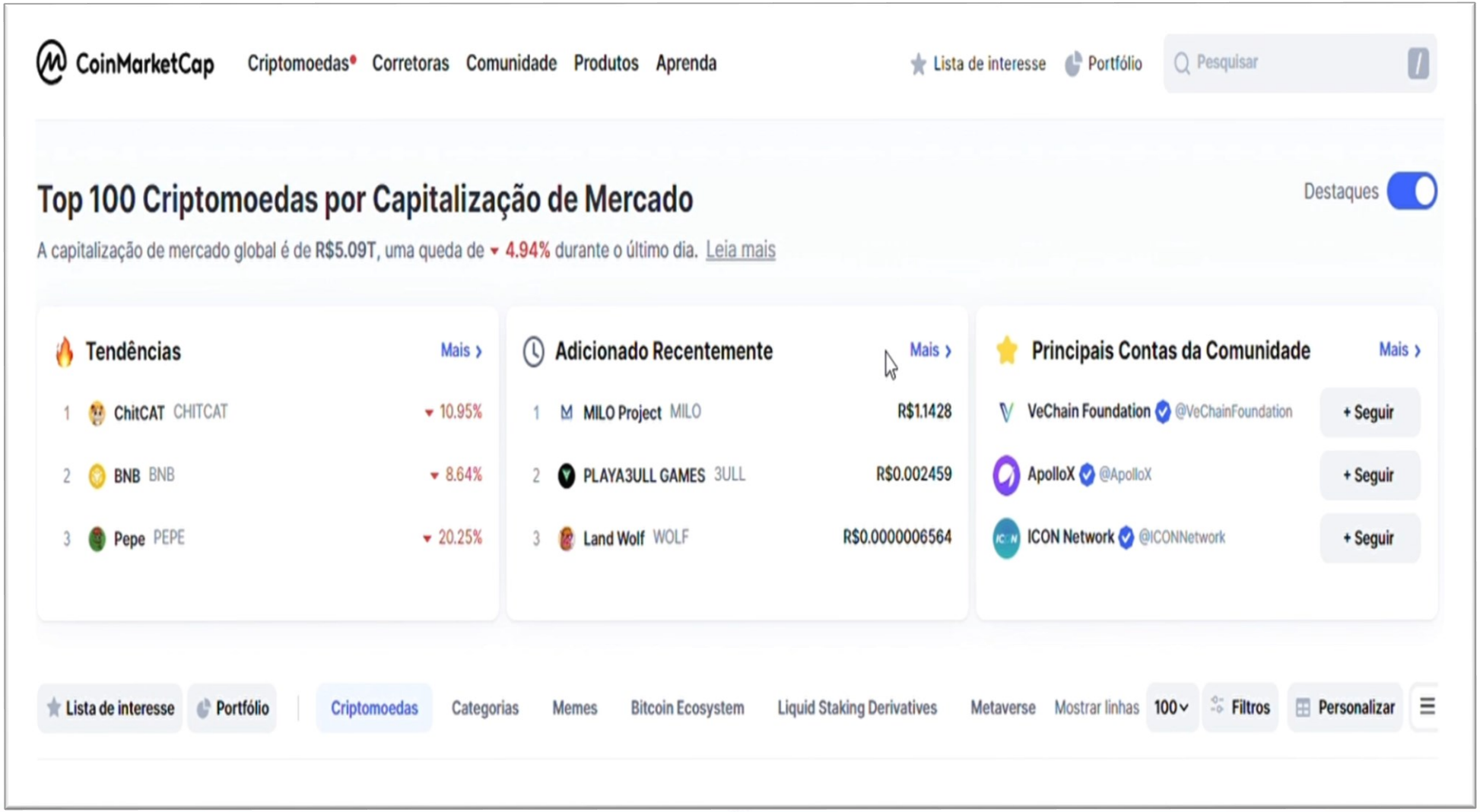
Bancos

Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.


CoinMarketCap
Criptomoedas
Corretoras
Comunidade
Produtos
Aprenda
Lista de interesse
Portfólio
Pesquisar
Top 100 Criptomoedas por Capitalização de Mercado
Destaques
A capitalização de mercado global é de R$5.09T, uma queda de 4.94% durante o último dia. Leia mais
Tendências
Mais
1 ChitCAT CHITCAT 10.95%
2 BNB BNB 8.64%
3 Pepe PEPE 20.25%
Adicionado Recentemente
Mais
1 MILO Project MILO R$1.1428
2 PLAYA3ULL GAMES 3ULL R$0.002459
3 Land Wolf WOLF R$0.0000006564
Principais Contas da Comunidade
Mais
VeChain Foundation @VeChainFoundation + Seguir
ApolloX @ApolloX + Seguir
ICON Network @ICONNetwork + Seguir
Lista de interesse
Portfólio
Criptomoedas
Categorias
Memes
Bitcoin Ecosystem
Liquid Staking Derivatives
Metaverse
Mostrar linhas
100
Filtros
Personalizar

Antes de falar sobre a estrutura...

Razão

Alice paga Ricardo R$ 50
Marcelo paga Alice R$ 80

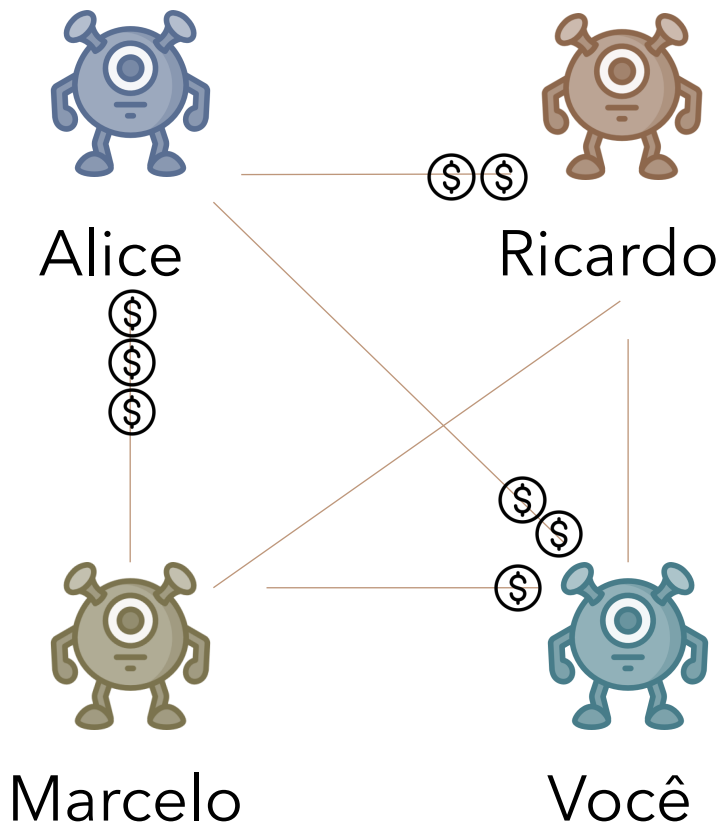
Assinaturas Digitais

Razão

Público e Acessível

Alice paga **Ricardo** R$ 20
Ricardo paga **Marcelo** R$ 40
Marcelo paga **você** R$ 30
Você paga **Alice** R$ 10
...

Fechamento

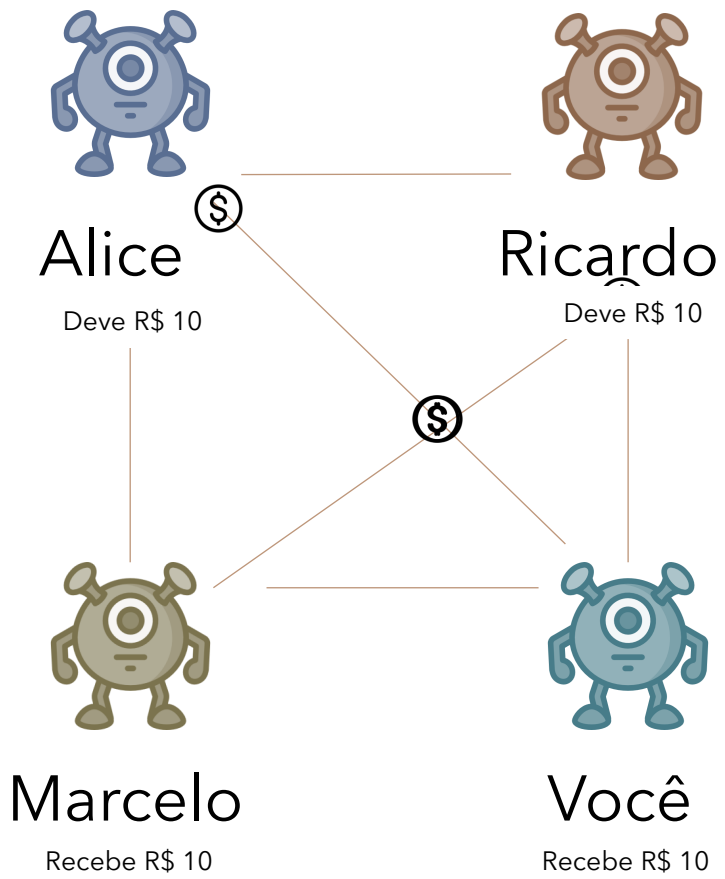


Razão

Público e Acessível

Alice paga **Ricardo** R$ 20
Ricardo paga **Marcelo** R$ 40
Marcelo paga **você** R$ 30
Você paga **Alice** R$ 10
...

Fechamento



Protocolo para fazer parte desse sistema

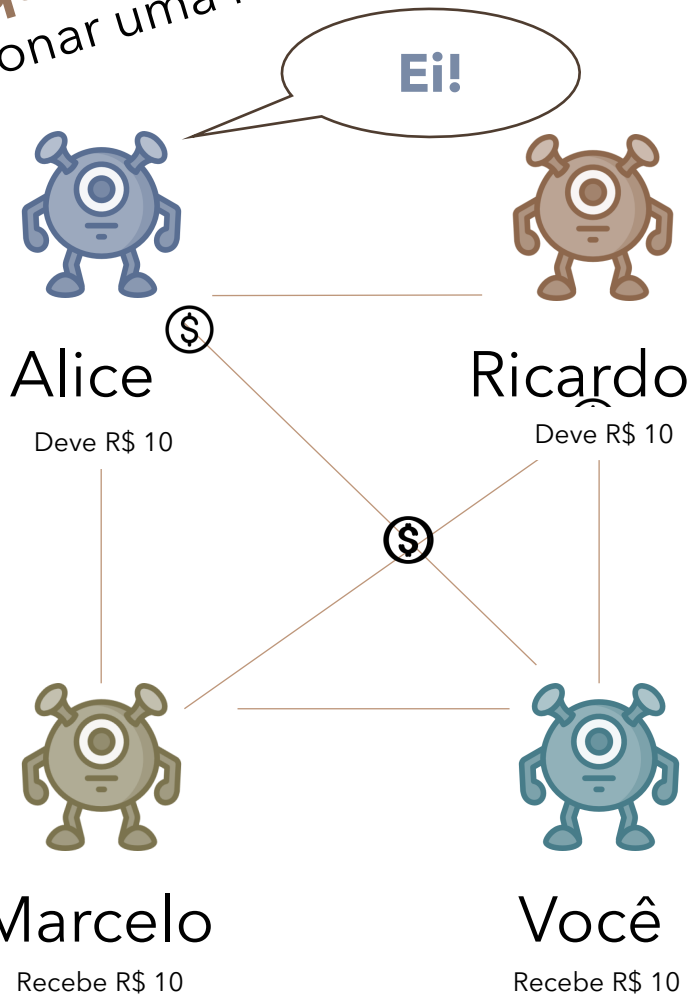
- Qualquer **pessoa** pode **adicionar** uma **nova linha** ao razão
- Ao final de cada mês, as pessoas devem se juntar e **contabilizar** os **valores a receber** e a **pagar** (com dinheiro real)

Razão

Alice paga **Ricardo** R$ 100

Como devemos **confiar** que todas essas transações são o que o remetente **pretendia e que fossem**?

Problema: **qualquer um** pode adicionar uma linha

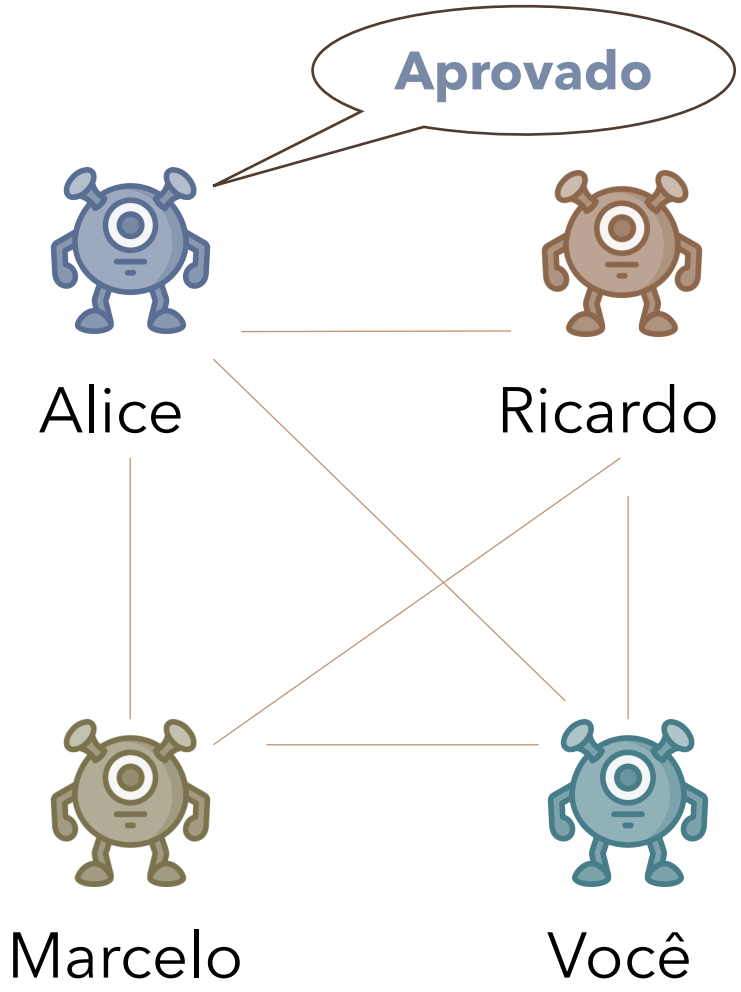


Criptografia

Razão

Alice paga **Ricardo** R$ 20 *Alice*
Ricardo paga **Marcelo** R$ 40 *Ricardo*
Marcelo paga **você** R$ 30 *Marcelo*
Você paga **Alice** R$ 10 *Você*
...

É preciso que seja **inviável**
que alguém consiga
falsificar essa assinatura

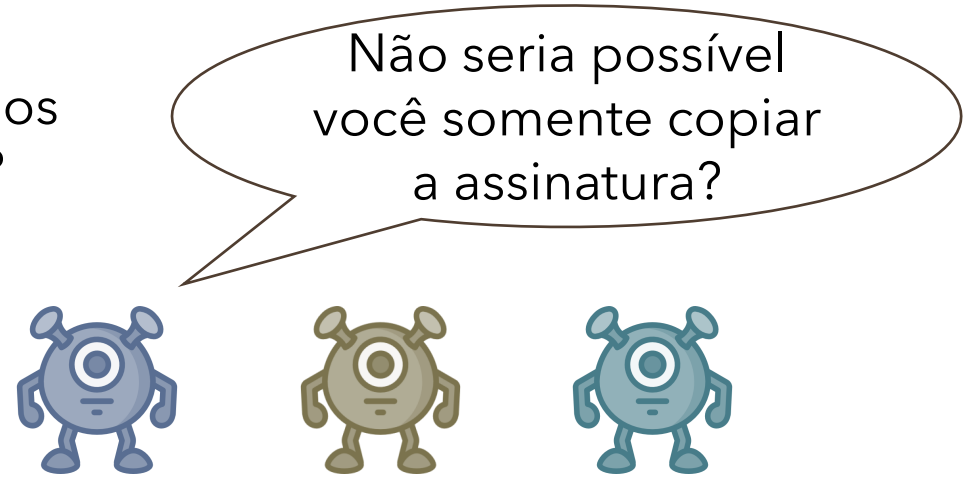


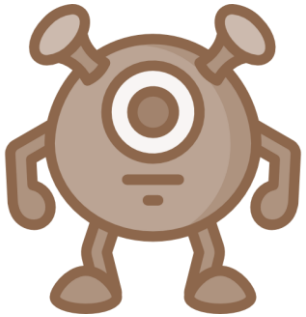
Criptografia

Alice

0110001

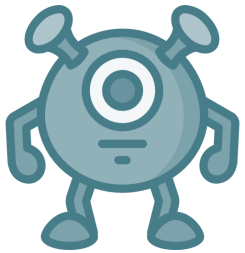
Como prevenimos **falsificações**?





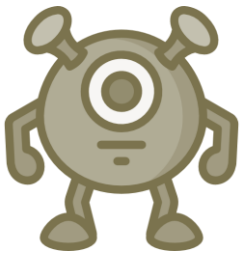
Private Key / **Public** Key

Private Key = **Secret** Key

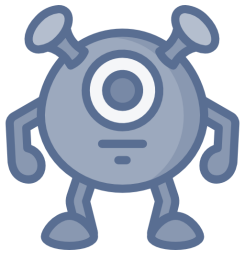


pk: 010001...
sk: 100110...

Sequência de **bits**



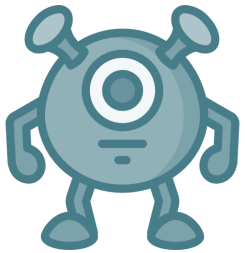
pk: 010010...
sk: 100111...



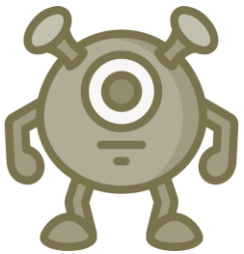
pk: 010100...
sk: 100010...

Secret Key / **Public** Key

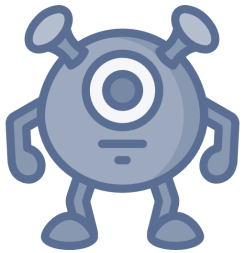
sk / **pk**



pk: 010001...
sk: 100110...



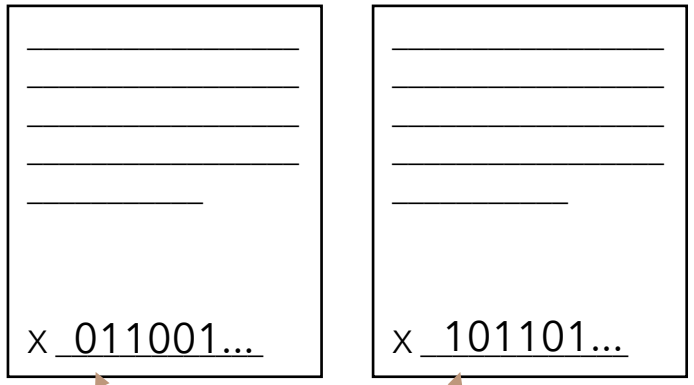
pk: 010010...
sk: 100111...



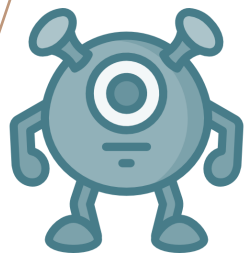
pk: 010100...
sk: 100010...

Secret Key / **Public** Key

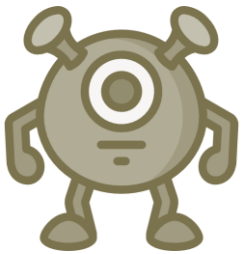
sk / **pk**



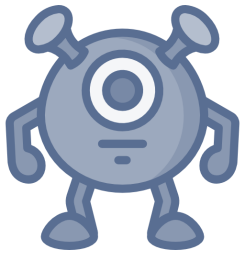
Na assinatura digital, ela muda **conforme** a **mensagem**



pk: 010001...
sk: 100110...

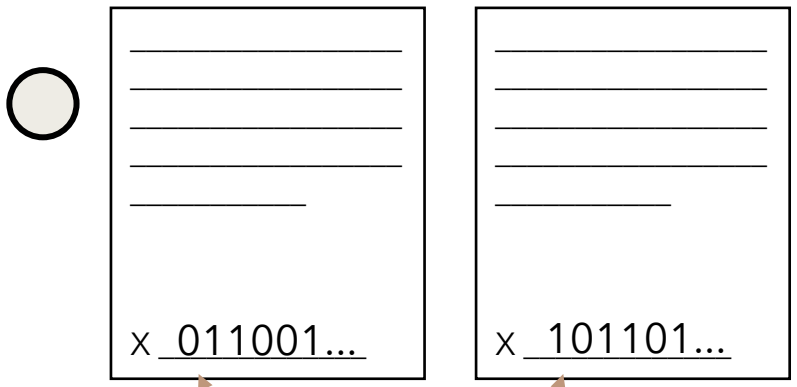


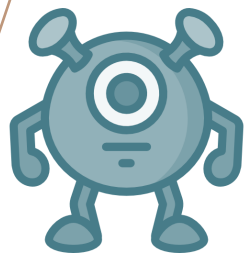
pk: 010010...
sk: 100111...



pk: 010100...
sk: 100010...

Mudanças **mínimas** na **mensagem** mudam completamente como a **assinatura daquela mensagem deveria aparecer**





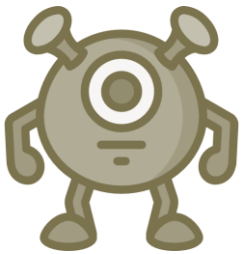
pk: 010001...
sk: 100110...

Função:

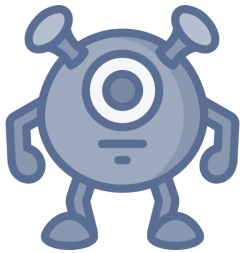
Assinatura (**Mensagem**, **sk**) = **Assinatura**

Sk garante que só você pode produzir a assinatura

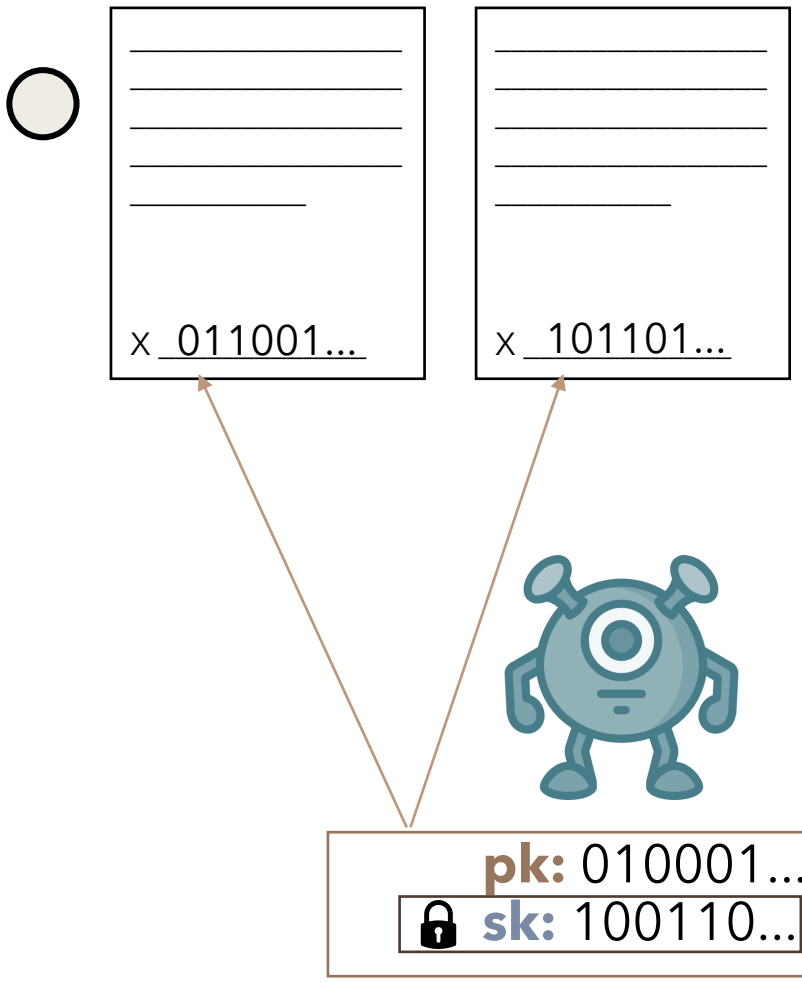
Depende da mensagem: ninguém pode simplesmente copiar e usar em outra mensagem



pk: 010010...
sk: 100111...



pk: 010100...
sk: 100010...



1ª Função:

Assinatura (**Mensagem**, **sk**) = **Assinatura**

2ª Função:

Verificação (**Mensagem**, **Assinatura**, **pk**) = **V/F**

2^{256} possíveis **assinaturas**

Isso é um número **estupidamente** grande!

2^{32} x 2^{32} x 2^{32} x 2^{32} x 2^{32} x 2^{32} x 2^{32} x 2^{32} — 8x

4 bilhões

Verificação (**Mensagem**, **Assinatura de 256 bit**, **pk**)

Quantas **assinaturas** possíveis?

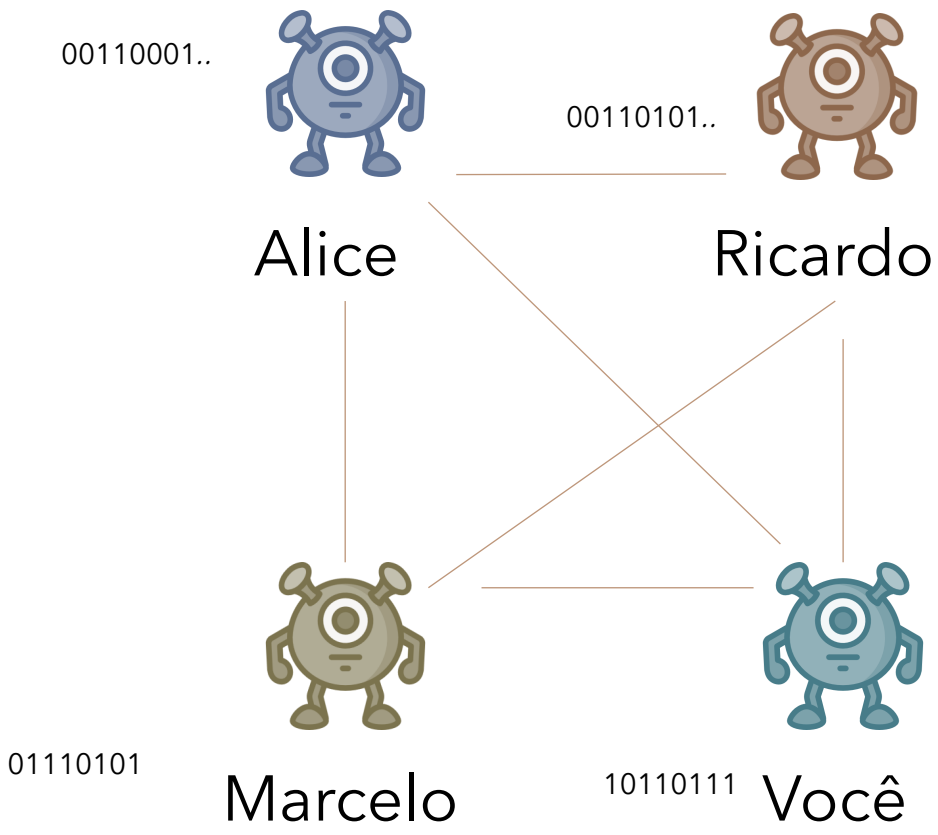
Verificação (**Mensagem**, **Assinatura de 256 bit**, **pk**) = **Verdadeiro**

Pode confiar!

Razão

Alice paga **Ricardo** R$ 20
Ricardo paga **Marcelo** R$ 40
Marcelo paga **você** R$ 30
Você paga **Alice** R$ 10
...

Bom, mas...

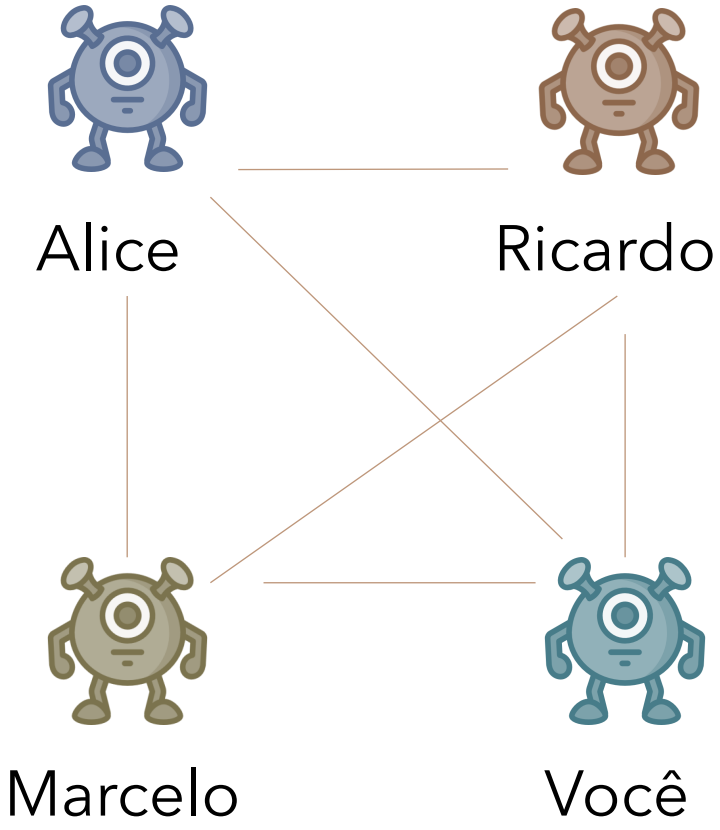


Razão

Alice paga **Ricardo** R$ 20 00110001..

Alice paga **Ricardo** R$ ~~X~~00 **????**

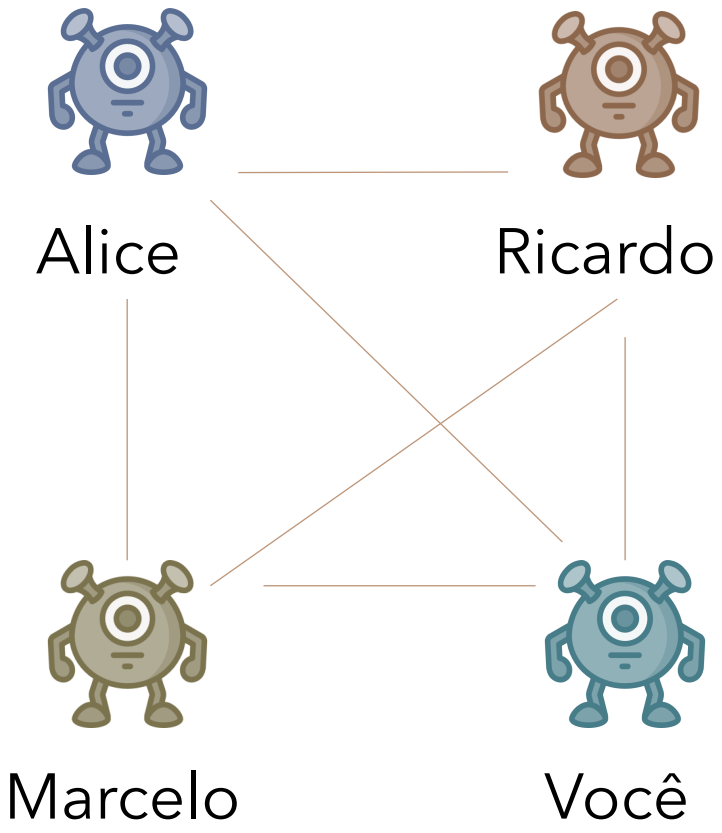
Bom, mas...



Razão

0 **Alice** paga **Ricardo** R$ 20 00110001...
1 **Alice** paga **Ricardo** R$ 20 00110001...
2 **Alice** paga **Ricardo** R$ 20 00110001...
3 **Alice** paga **Ricardo** R$ 20 00110001...
4 **Alice** paga **Ricardo** R$ 20 00110001...

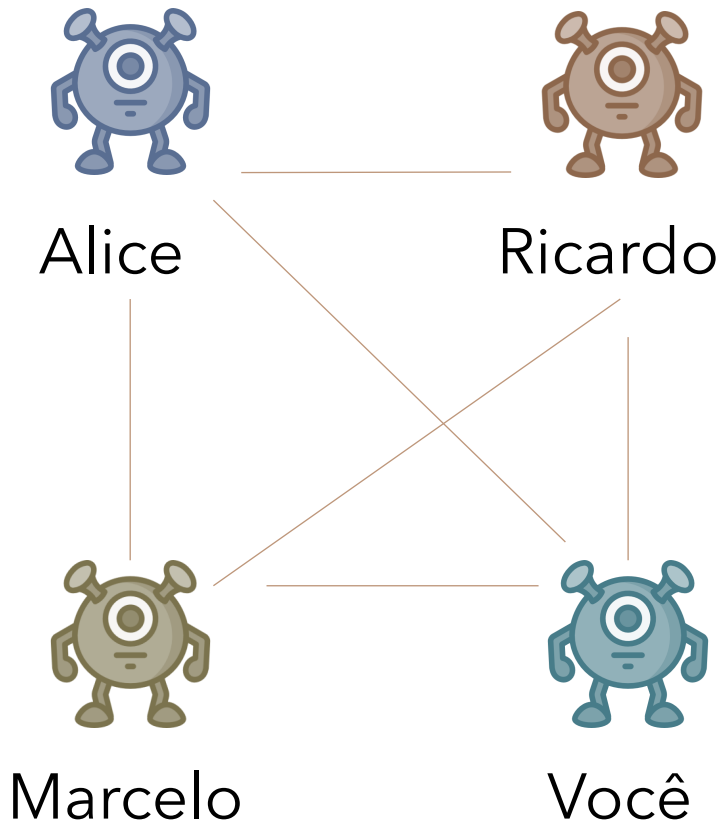
Bom, mas...



Razão

0 **Alice** paga **Ricardo** R$ 20 00110001...
1 **Alice** paga **Ricardo** R$ 20 00111001...
2 **Alice** paga **Ricardo** R$ 20 00110011...
3 **Alice** paga **Ricardo** R$ 20 10110001...
4 **Alice** paga **Ricardo** R$ 20 01100001...

Bom, mas...



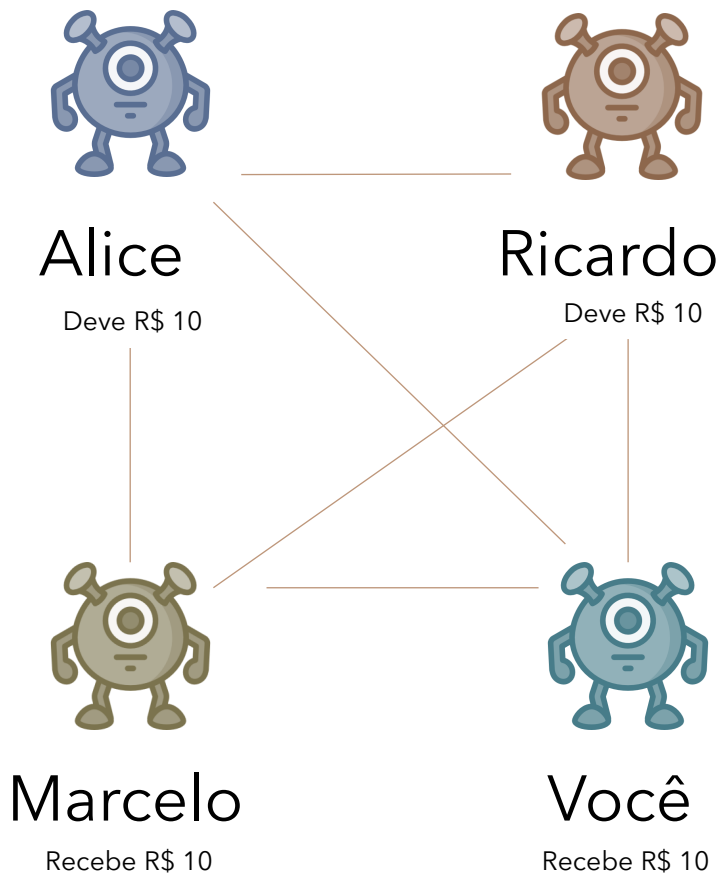
Protocolo para fazer parte desse sistema

- Qualquer **pessoa** pode **adicionar** uma **nova linha** ao razão
- Ao final de cada mês, as pessoas devem se juntar e **contabilizar** os **valores a receber** e a **pagar** (com dinheiro real)
- Somente **transações assinadas** são válidas

Razão

Alice paga **Ricardo** R$ 20
Ricardo paga **Marcelo** R$ 40
Marcelo paga **você** R$ 30
Você paga **Alice** R$ 10
...

Fechamento



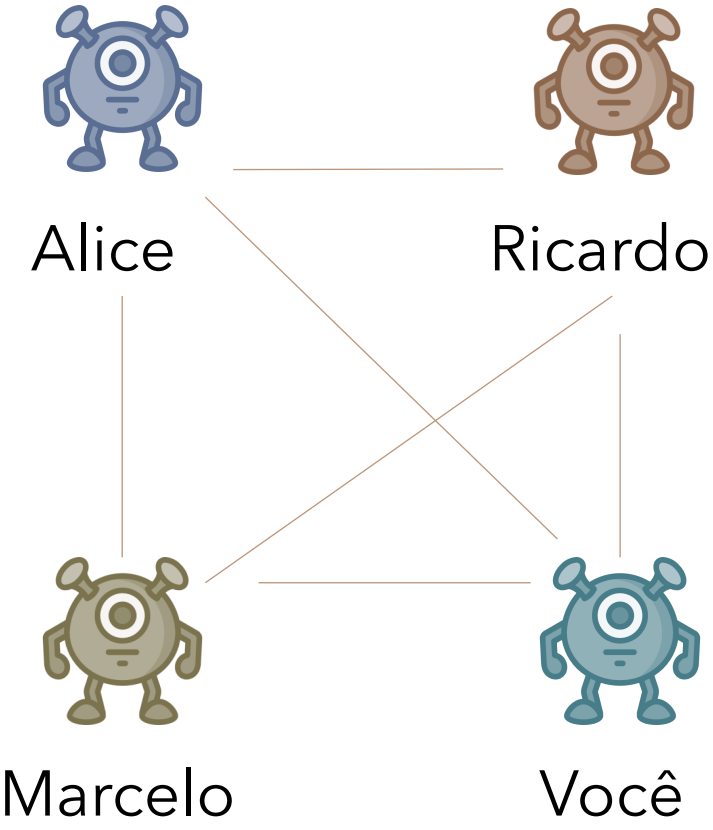
Ainda assim, **exige** um sistema de confiança de que as **pessoas vão pagar** o que **devem ao final**

Razão

1. **Marcelo** paga **Alice** R$ 100 0011001...
2. **Marcelo** paga **Ricardo** R$ 200 1010001...
3. **Marcelo** paga **Ricardo** R$ 100 1011101...
4. **Marcelo** paga **você** R$ 250 1011100...
5. **Marcelo** paga **Alice** R$ 300 1000100...

Ainda assim, **exige** um sistema de confiança de que as **pessoas vão pagar** o que **devem ao final**

Vamos supor que alguém **acumule** milhares de reais em dívida e... **desapareça**



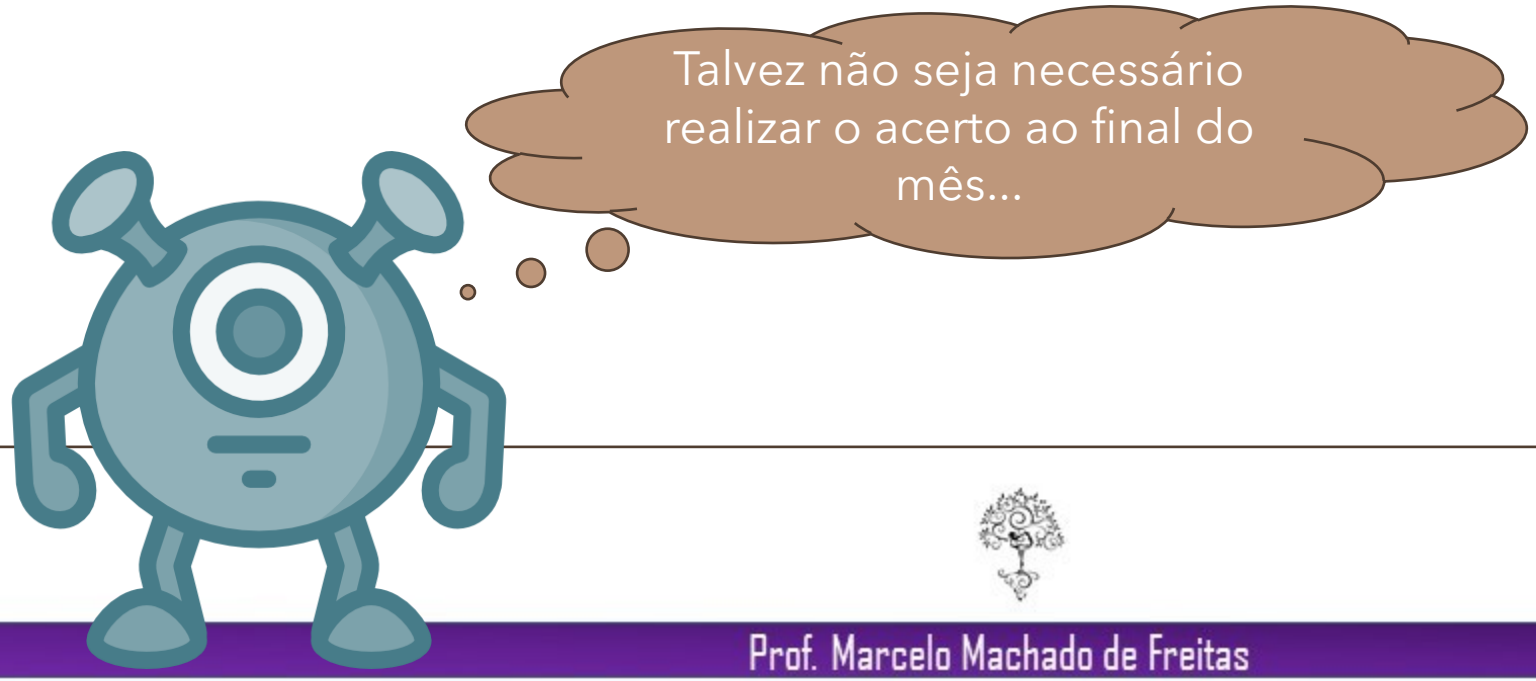
Protocolo para fazer parte desse sistema

- Qualquer **pessoa** pode **adicionar** uma **nova linha** ao razão
- Ao final de cada mês, as pessoas devem se juntar e **contabilizar** os **valores a receber** e a **pagar** (com dinheiro real)
- Somente **transações assinadas** são válidas

A única razão para o "acerto" ao final do mês é porque alguém **deve dinheiro**..

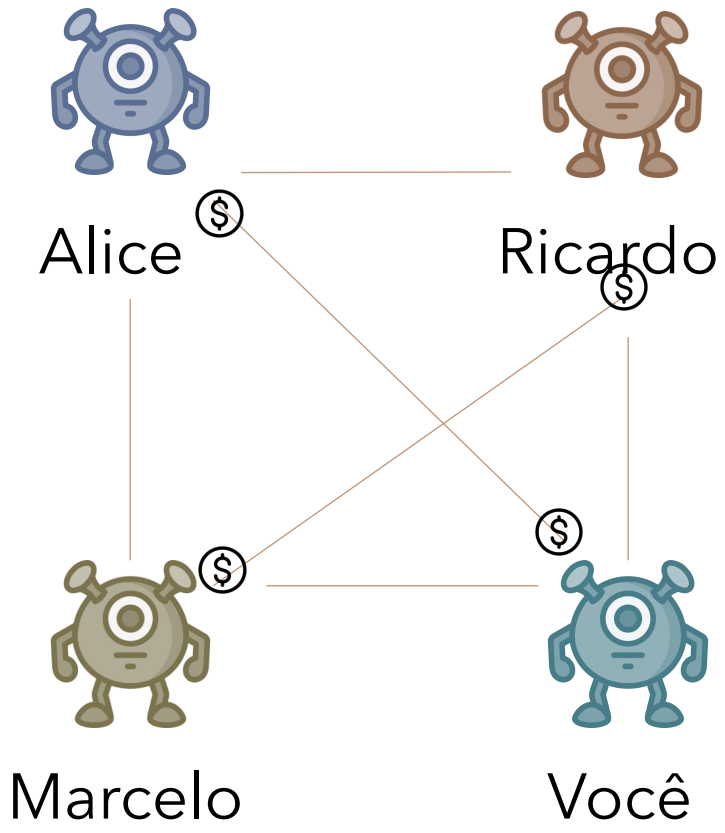
Protocolo para fazer parte desse sistema

- Qualquer **pessoa** pode **adicionar** uma **nova linha** ao razão
- Ao final de cada mês, as pessoas devem se juntar e **contabilizar** os **valores a receber** e a **pagar** (com dinheiro real)
- Somente **transações assinadas** são válidas



Razão

1. **Alice** ganha R$ 100
2. **Ricardo** ganha R$ 100
3. **Marcelo** ganha R$ 100
4. **Você** ganha R$ 100



Protocolo para fazer parte desse sistema

- Qualquer **pessoa** pode **adicionar** uma **nova linha** ao razão
- ~~Ao final de cada mês, as pessoas devem se juntar e **contabilizar** os **valores a receber** e a **pagar** (com dinheiro real)~~
- Somente **transações assinadas** são válidas
- Nenhum transação será aceita quando uma pessoa **gasta mais do que tem** naquele **livro razão**

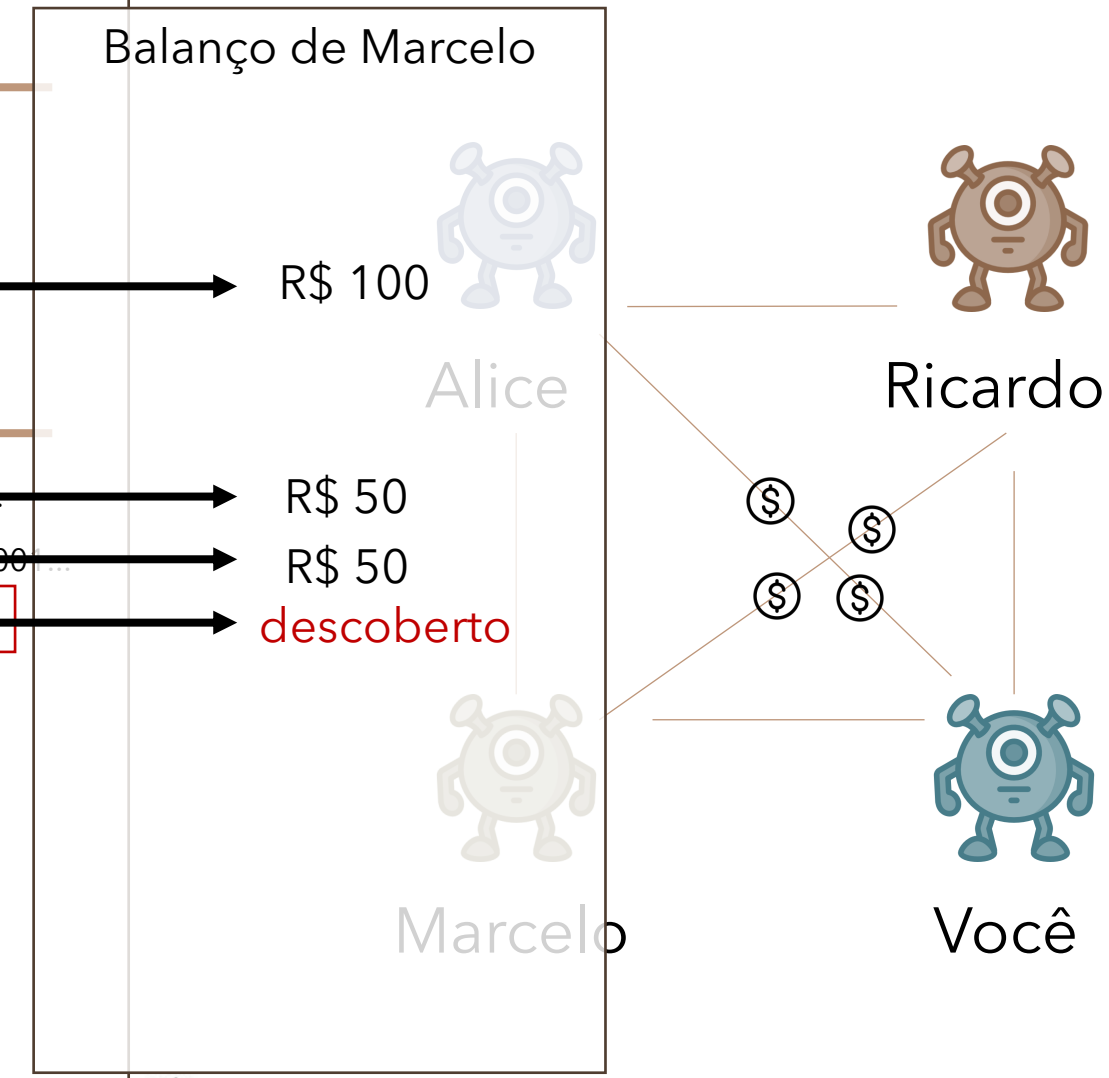
Razão

1. **Alice** ganha R$ 100
2. **Ricardo** ganha R$ 100
3. **Marcelo** ganha R$ 100
4. **Você** ganha R$ 100

5. **Marcelo** paga **Alice** R$ 50 0011001...
6. **Marcelo** paga **Ricardo** R$ 50 1001000...
7. **Marcelo** paga **você** R$ 20 1010101...

Inválido

Para verificar uma **transação** você precisa saber o **histórico completo** até aquele ponto



Razão

---

111. **Alice** paga **Marcelo** R$ 100 1011101...
112. **Ricardo** paga **Alice** R$ 120 1010101...
113. **Marcelo** paga **Alice** R$ 200 1110001...
114. **Você** paga **Marcelo** R$ 100 1010101..
115. **Marcelo** paga **Alice** R$ 50 1000001...
116. **Marcelo** paga **Ricardo** R$ 50 1010001...
117. **Marcelo** paga **você** R$ 20 1010101...
....

Para enfatizar, vamos começar a chamar o dinheiro dentro do livro razão de

Real do Livro Razão "RR"

E se **TODOS** usassem?

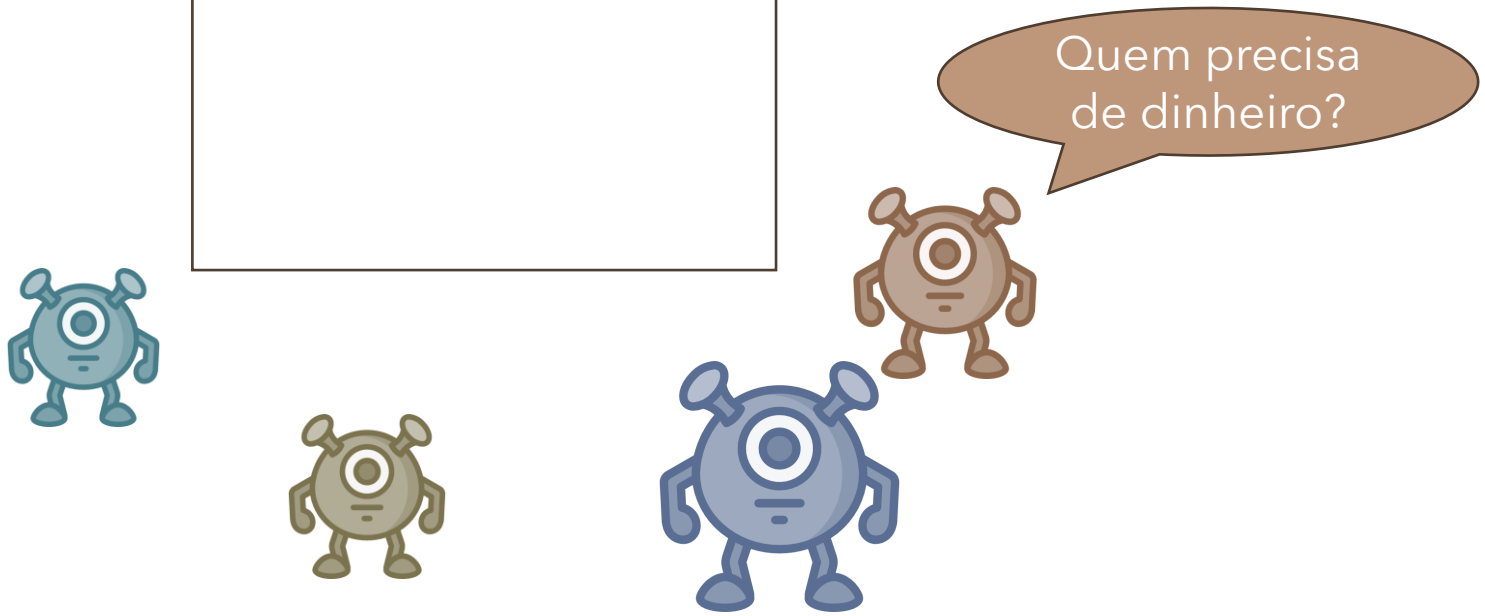
Razão

---

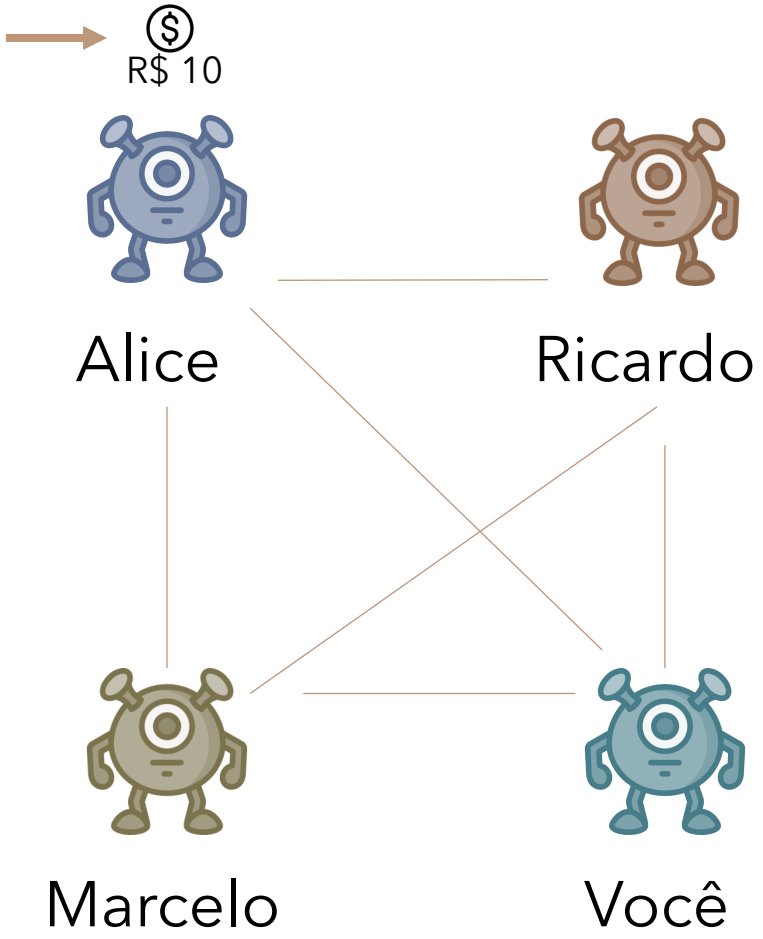
111. **Alice** paga **Marcelo** **RR** 100 1011101...
112. **Ricardo** paga **Alice** **RR** 120 1010101...
113. **Marcelo** paga **Alice** **RR** 200 1110001...
114. **Você** paga **Marcelo** **RR** 100 1010101..
115. **Marcelo** paga **Alice** **RR** 50 1000001...
116. **Marcelo** paga **Ricardo** **RR** 50 1010001...
117. **Marcelo** paga **você** **RR** 20 1010101...
....

Para enfatizar, vamos começar a chamar o dinheiro dentro do livro razão de

Real do Livro Razão "RR"



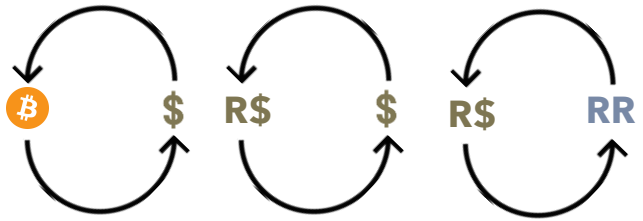
Claro que é possível trocar **RR por R$**



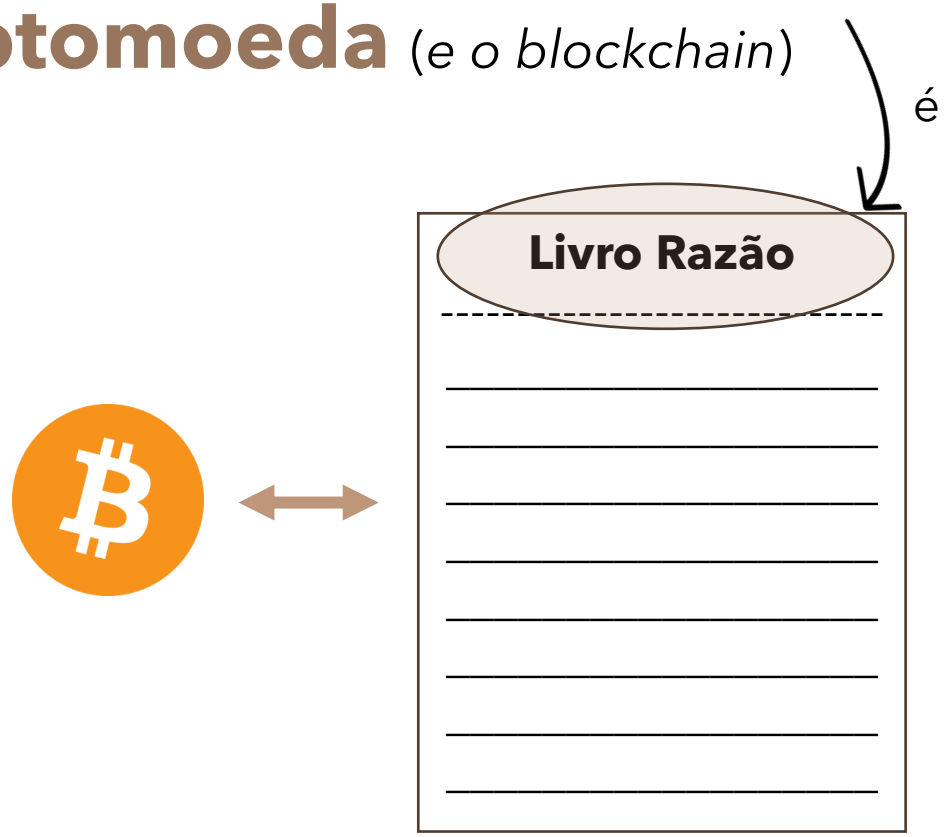
Razão

...
140. **Ricardo** paga **Alice** **RR** 10 1010101...
....

Transações como essa **NÃO** estão **garantidas pelo protocolo**



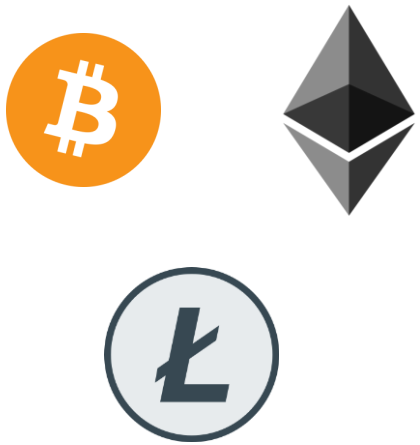
- Isso é a primeira coisa a se entender sobre **Bitcoin**, ou **qualquer outra criptomoeda** (*e o blockchain*)



Moeda = O **histórico** de **Transações**

- Existe uma outra diferença entre o nosso sistema e das **criptomoedas**

Descentralizado



Centralizado

RR

Onde está essa razão?

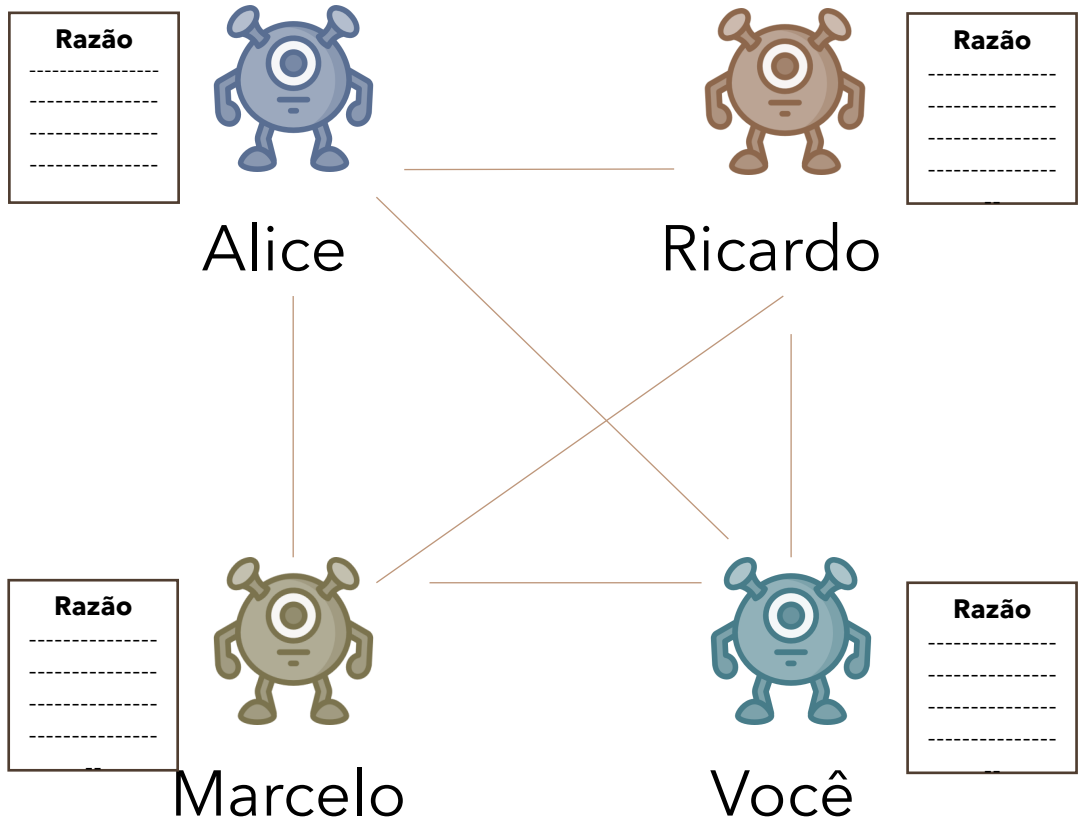
Razão

…. ….

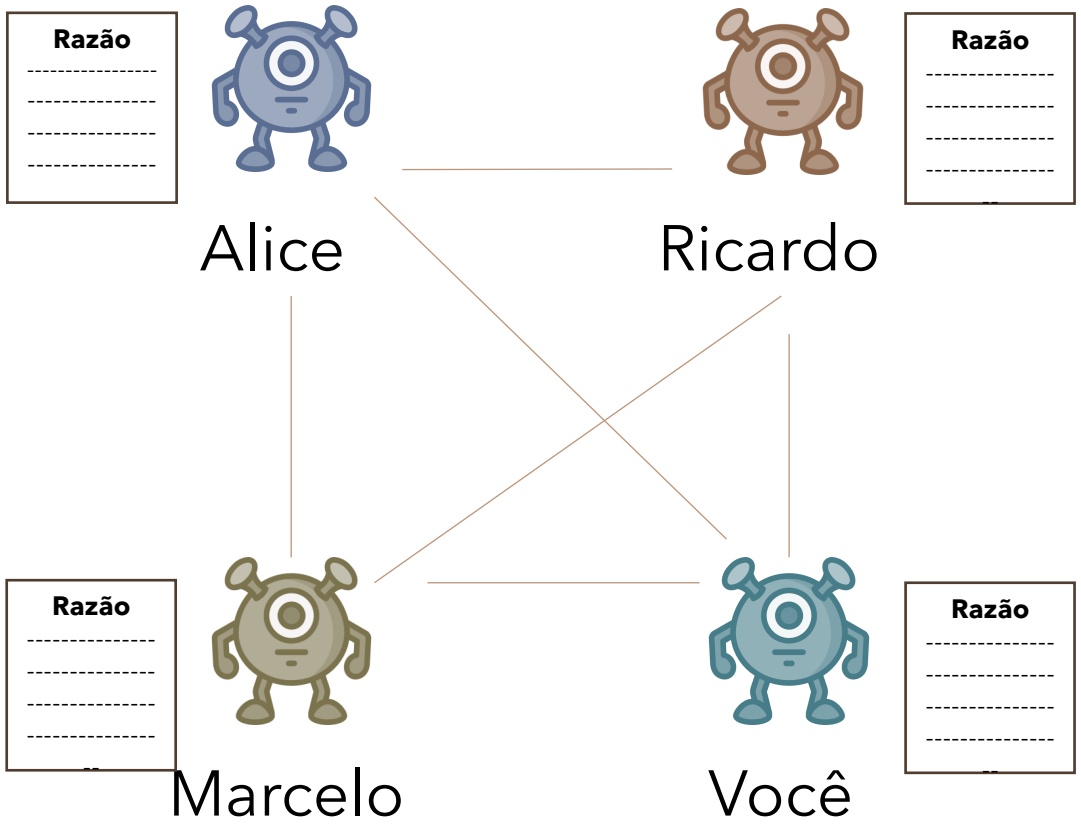
…. ….

…. ….

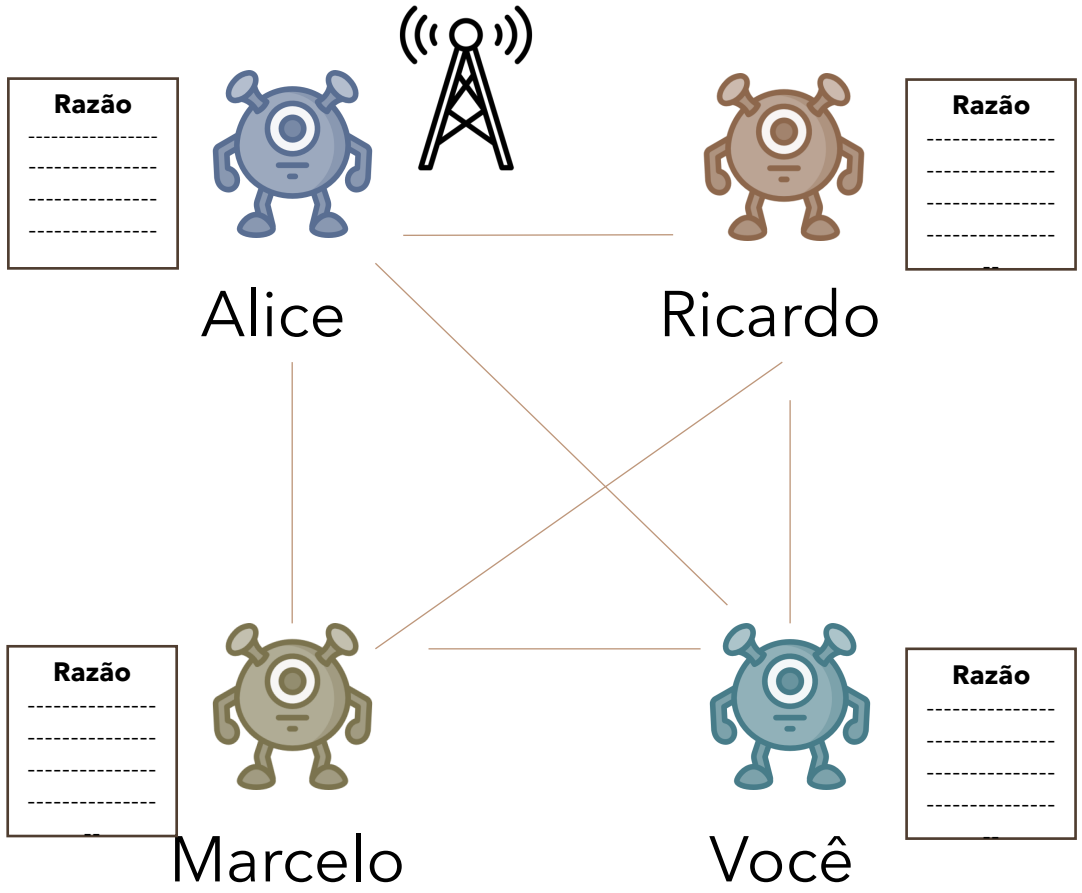
Nesse exemplo, seria preciso **confiar** em uma **localização central**



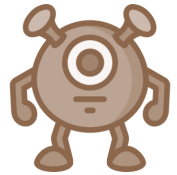
Com isso, **podemos remover** essa necessidade de **confiança** em um **órgão central**



Alice paga Ricardo 100 RR



Vocês **ouviram** isso?



Ricardo

Alice paga **Ricardo** **100**

RR

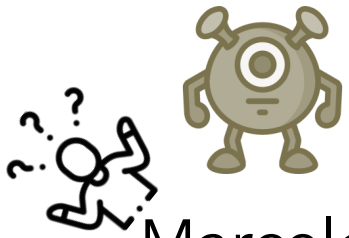
Todos esses são os **mesmos**?

Razão

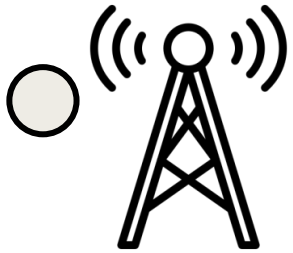
Razão

Razão

Razão



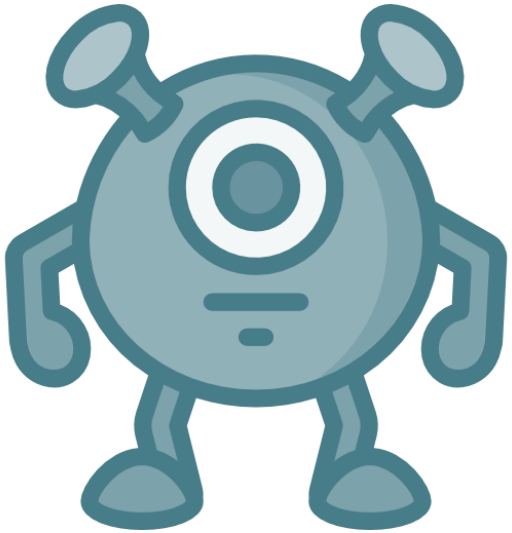
Marcelo



Imagine você **recebendo** essas **transmissões**

Bob paga **você** **50 RR**

Alice paga **você** **100 RR**



Ricardo paga **você** **100 RR**

Protocolo

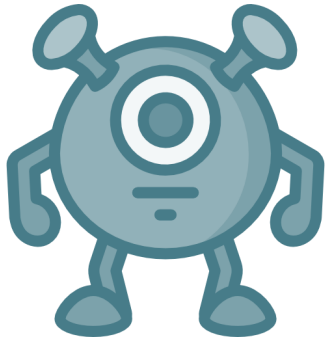
- Qualquer **pessoa** pode **adicionar** uma **nova linha** ao razão
- Somente **transações assinadas** são válidas
- Nenhum transação será aceita quando uma pessoa **gasta mais do que tem** naquele **livro razão**

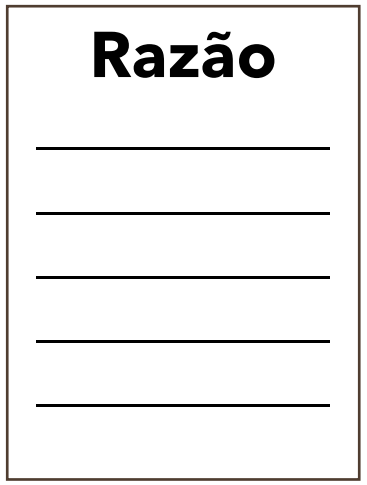
Esse é o **problema** abordado pelo artigo original do Biticoin

O que podemos **adicionar** aqui?

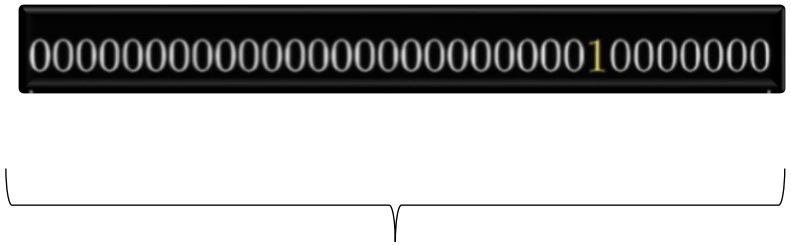
A solução que o **Biticoin** oferece

Proof of work





+



Esforço/Trabalho computacional

Principal ferramenta: funções ***hashs*** criptografadas

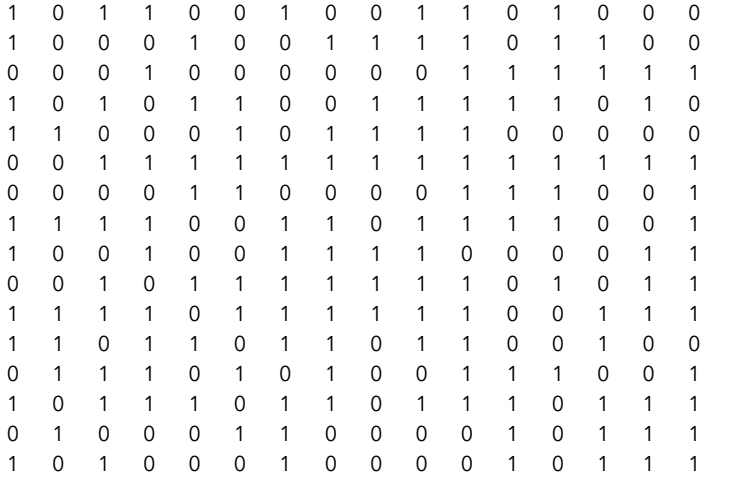
Fraude ⟷ computacionalmente inviável

O que é uma **função *Hash*?**

SHA256 (“**4SeminárioPerícia**”) =

Mensagem ou **arquivo**

Sequência fixa de BITS (256, digamos)



Hash ou “Digest” (*output*)

Parece aleatório... mas não é!

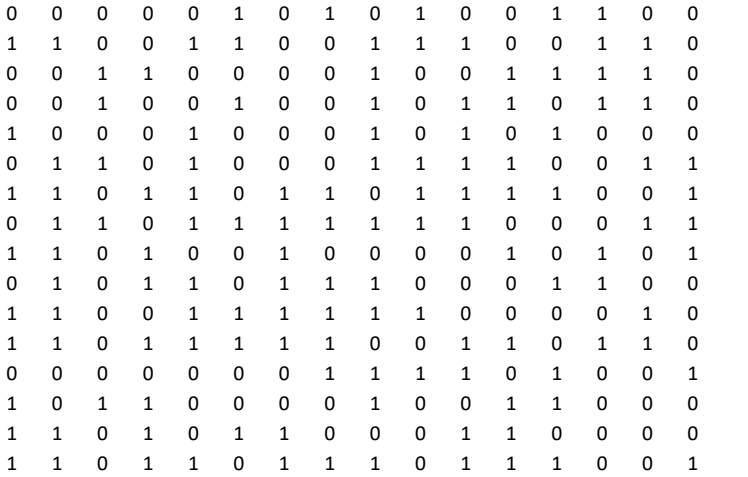
E se você mudar qualquer coisa na mensagem...

O que é uma **função *Hash*?**

SHA256 (“**5SeminárioPerícia**”) =

Mensagem ou **arquivo**

Sequência fixa de BITS (256, digamos)



Hash ou “Digest” (*output*)

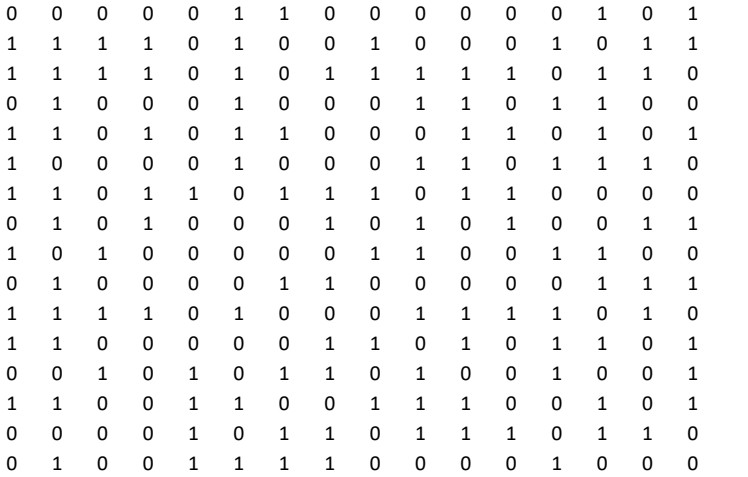
Parece aleatório... mas não é!

O que é uma **função *Hash*?**

SHA256 (“**6SemPerícia**”) =

Mensagem ou **arquivo**

Sequência fixa de BITS (256, digamos)



Hash ou “Digest” (*output*)

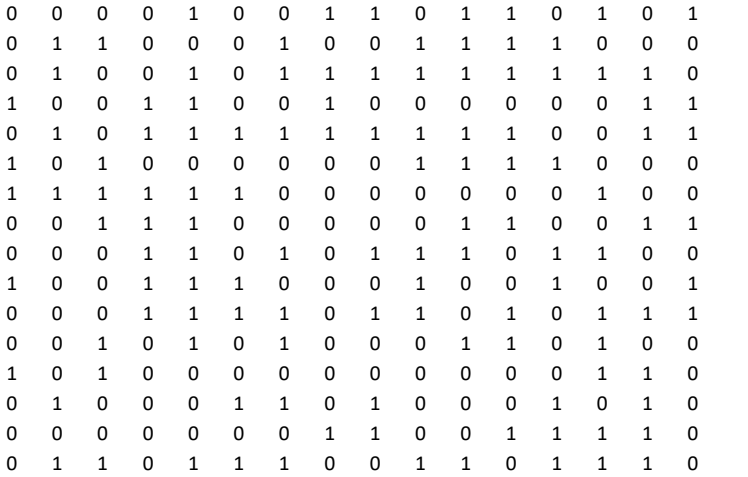
Parece aleatório... mas não é!

O que é uma **função *Hash*?**

SHA256 (“**7SemPerícia**”) =

Mensagem ou **arquivo**

Sequência fixa de BITS (256, digamos)



Hash ou “Digest” (*output*)

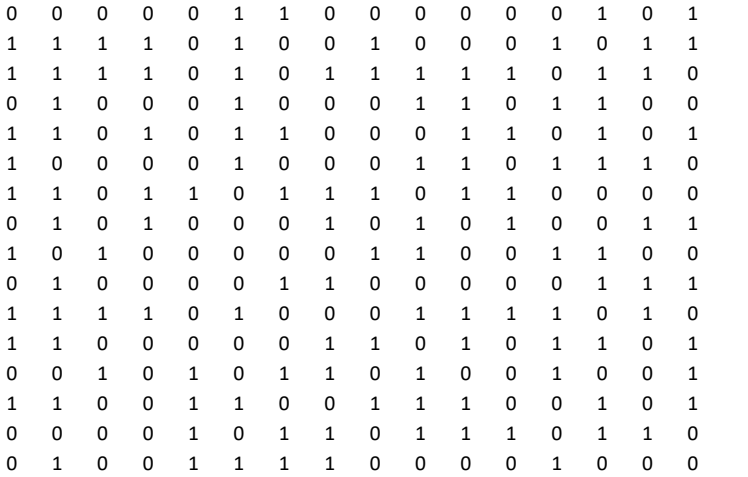
Não é aleatório... mas é imprevisível!

É **inviável** computar na **direção reversa**

O que é uma **função *Hash*?**

SHA256 (“**??????????????????**”) =

Mensagem ou **arquivo**

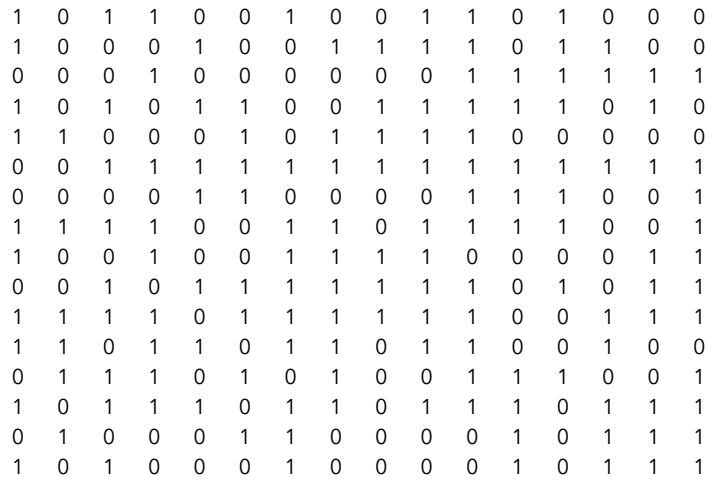


Output Desejado

Não é aleatório... mas é imprevisível!

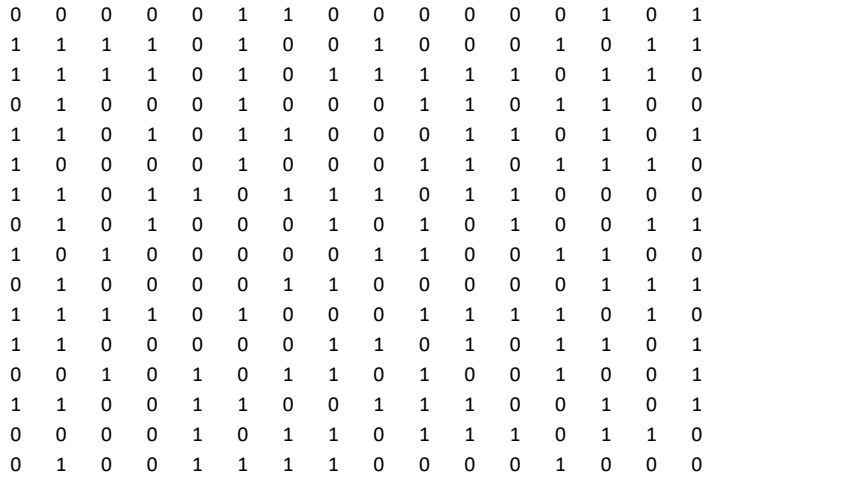
É **inviável** computar na **direção reversa**

SHA256 (“**Chute#1**”) =



SHA256 (“**??????????????**”) =

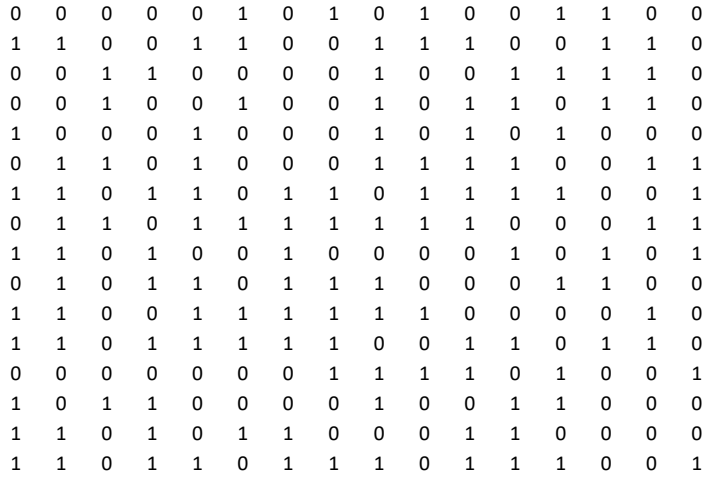
???



Output Desejado

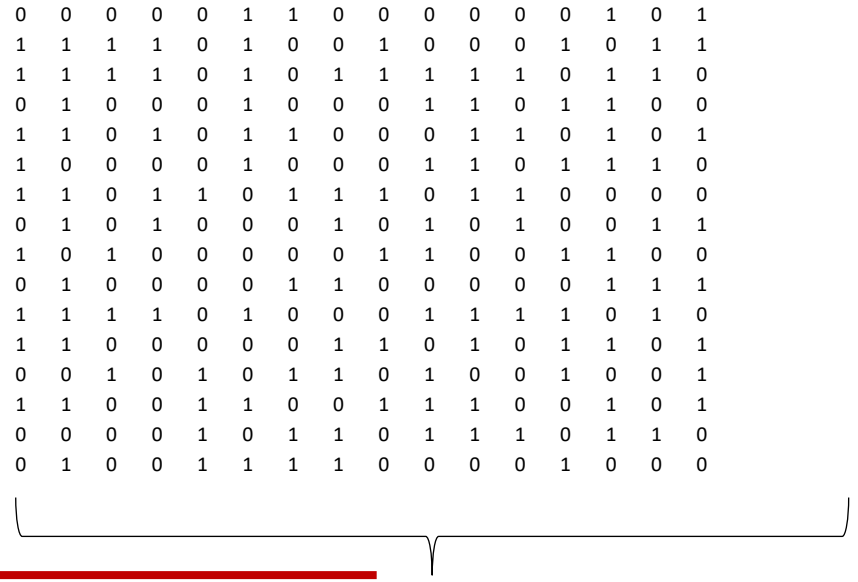
É **inviável** computar na **direção reversa**

SHA256 (“**Chute#2**”) =



SHA256 (“**??????????????**”) =

???

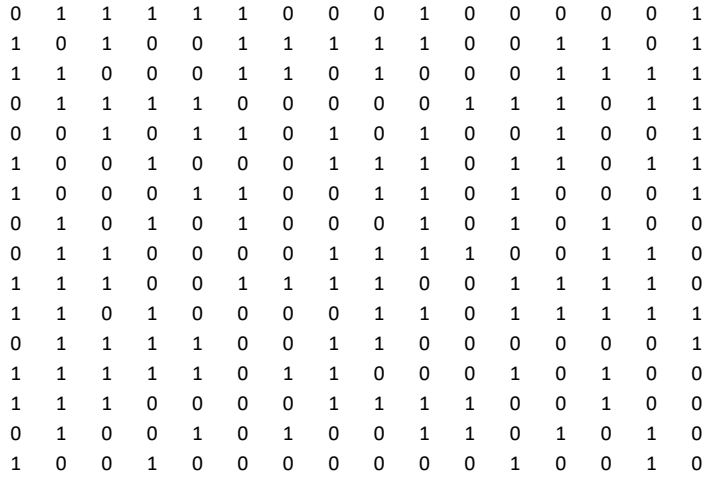


Output Desejado

É **inviável** computar na **direção reversa**

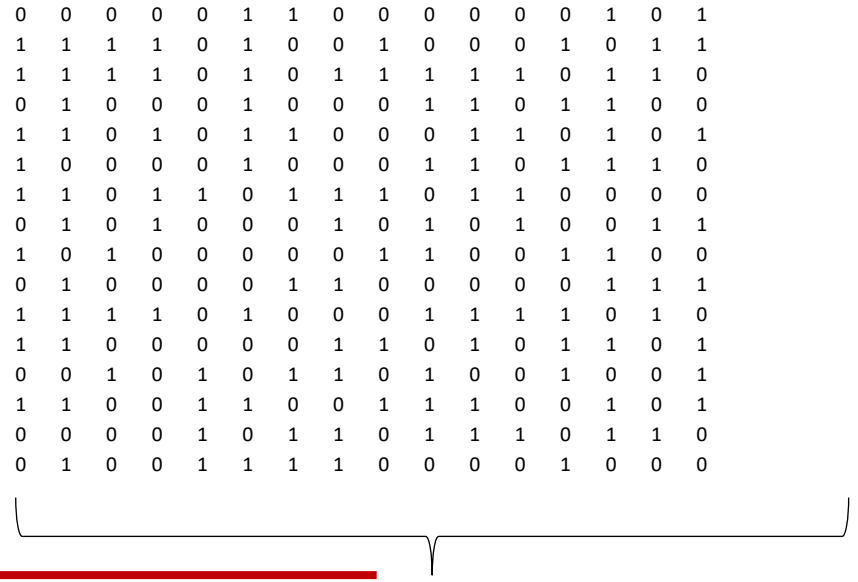
SHA256 (“**Chute#3**”) =

2^{256} palpites...



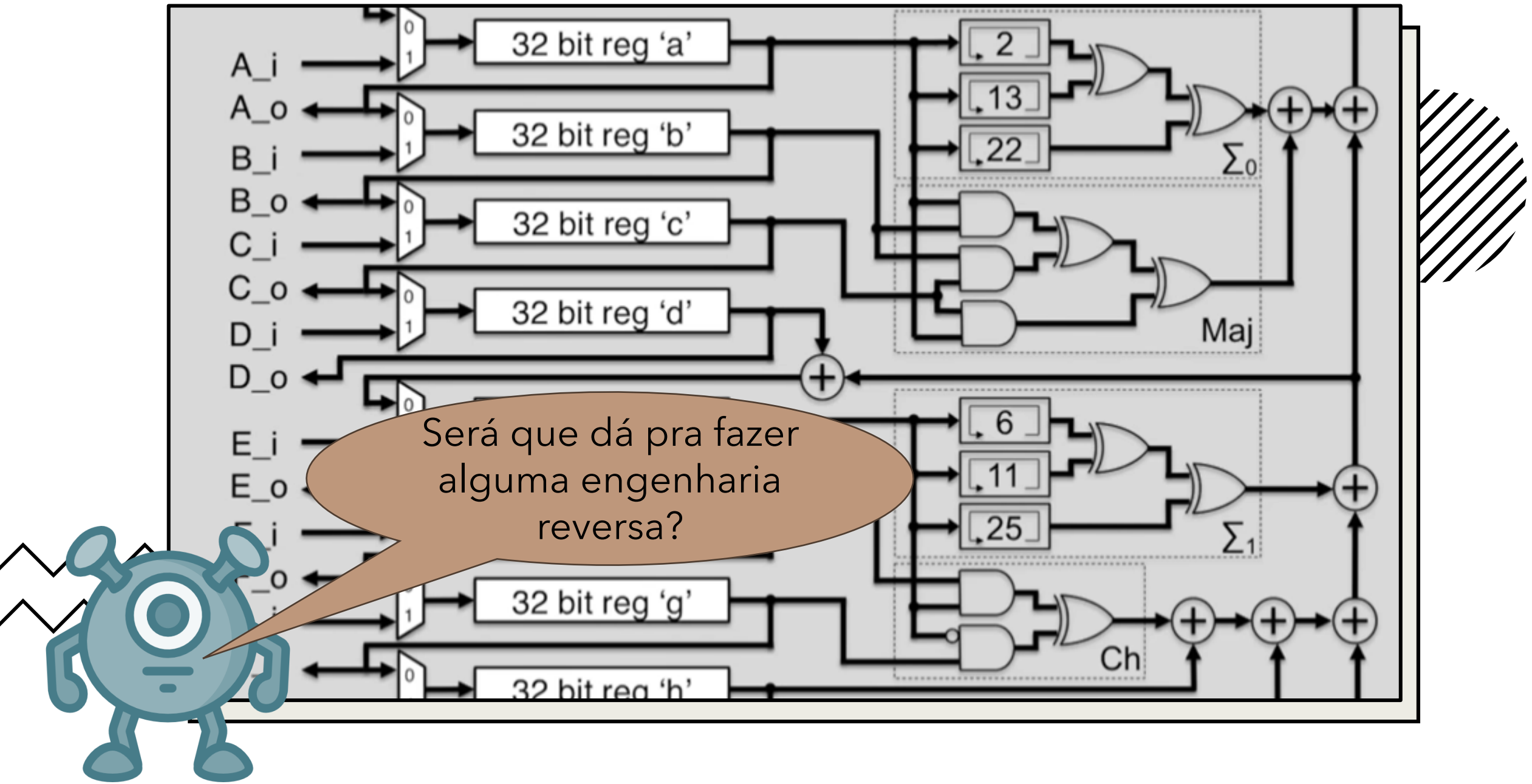
SHA256 (“**??????????????**”) =

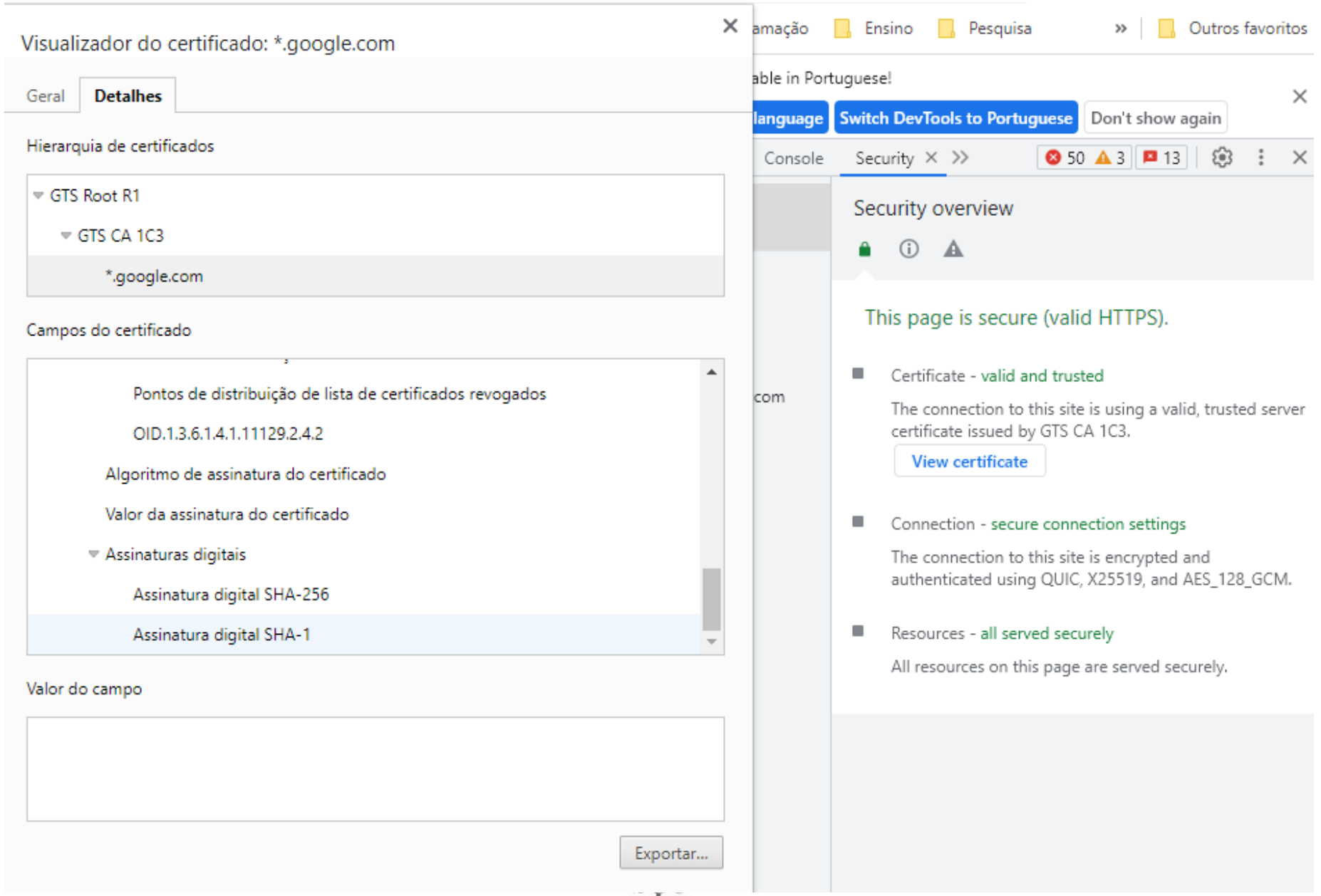
???



Output Desejado

É **inviável** computar na **direção reversa**

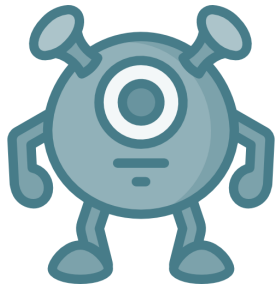

A_i
A_o
B_i
B_o
C_i
C_o
D_i
D_o
E_i
E_o
32 bit reg 'a'
32 bit reg 'b'
32 bit reg 'c'
32 bit reg 'd'
32 bit reg 'g'
32 bit reg 'h'
2
13
22
6
11
25
Σ_0
Σ_1
Maj
Ch
Será que dá pra fazer alguma engenharia reversa?


Visualizador do certificado: *.google.com
Geral
Detalhes
Hierarquia de certificados
GTS Root R1
GTS CA 1C3
*.google.com
Campos do certificado
Pontos de distribuição de lista de certificados revogados
OID.1.3.6.1.4.1.11129.2.4.2
Algoritmo de assinatura do certificado
Valor da assinatura do certificado
Assinaturas digitais
Assinatura digital SHA-256
Assinatura digital SHA-1
Valor do campo
Exportar...
Ensino
Pesquisa
Outros favoritos
able in Portuguese!
Switch DevTools to Portuguese
Don't show again
Console
Security
Security overview
This page is secure (valid HTTPS).
Certificate - valid and trusted
The connection to this site is using a valid, trusted server certificate issued by GTS CA 1C3.
View certificate
Connection - secure connection settings
The connection to this site is encrypted and authenticated using QUIC, X25519, and AES_128_GCM.
Resources - all served securely
All resources on this page are served securely.

Mas por hora, vamos focar...

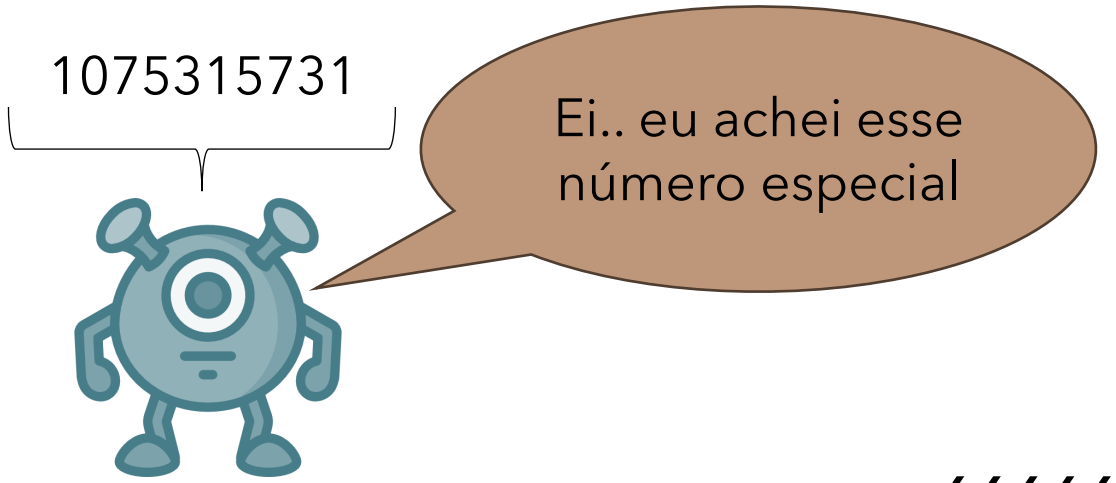
em entender como essa função hash *SHA256* pode provar que uma lista particular de transações está associada com um grande esforço computacional

SHA256 ⟶ Proof of Work



Razão

Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 40
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...



Razão

Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 40
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...

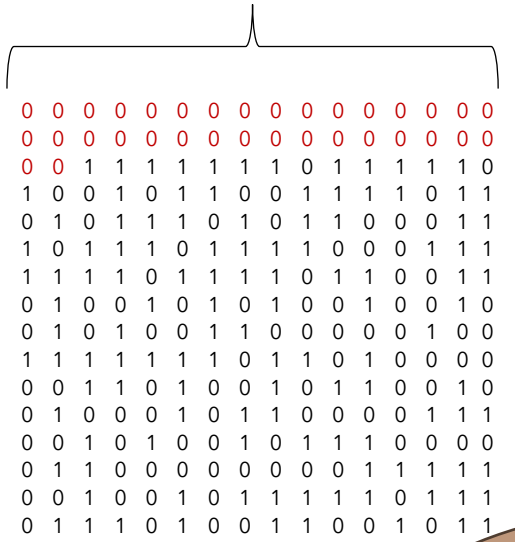
1075315731

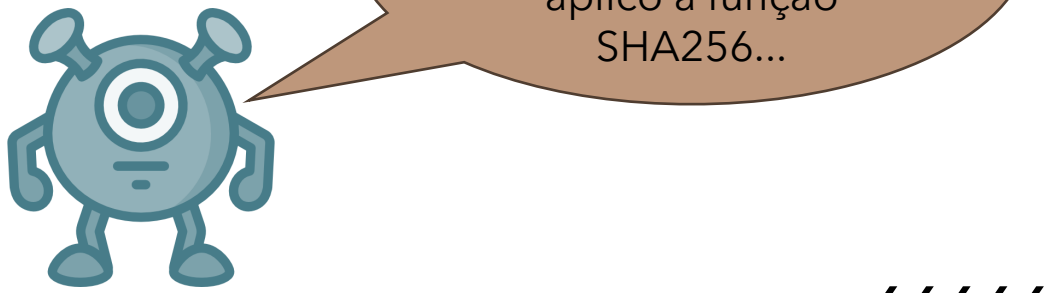
Como SHA256 é uma função hash criptografada, a única maneira é tentativa e erro

Probabilidade: $1/2^{30} \fallingdotseq \frac{1}{1\text{ bilhão}}$

30 primeiros bits = 0

SHA256





Razão

Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 40
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...

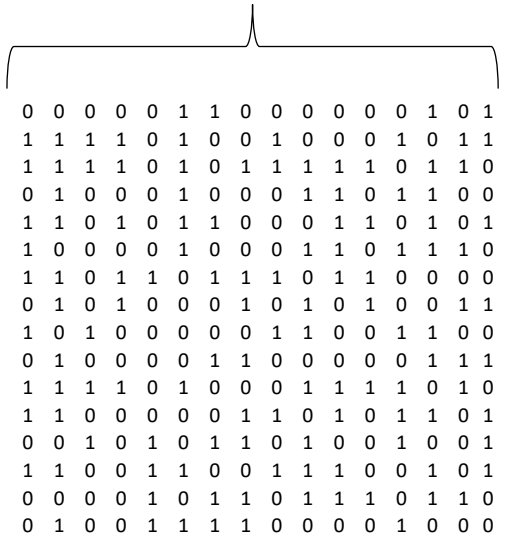
1

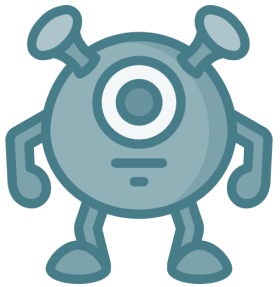
Como SHA256 é uma
função hash criptografada,
a única maneira é tentativa
e erro

Probabilidade: $1/2^{30}$ ≒ **1 / 1 bilhão**

30 primeiros bits = 0

SHA256





Razão

Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 40
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...

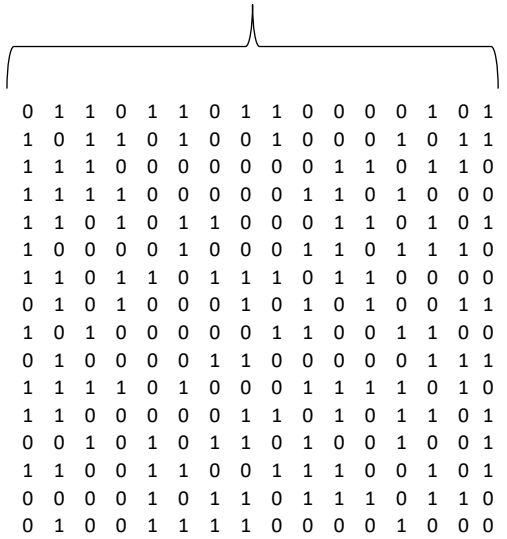
2

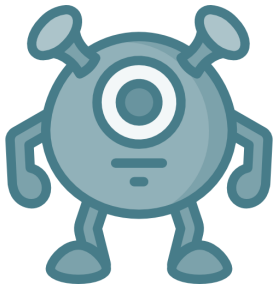
Como SHA256 é uma
função hash criptografada,
a única maneira é tentativa
e erro

SHA256

Probabilidade: $1/2^{30}$ ≒ **1 / 1 bilhão**

30 primeiros bits = 0





Razão

Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 40
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...

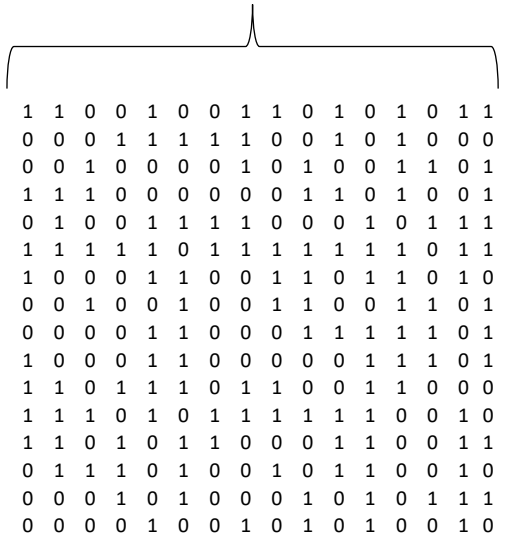
3

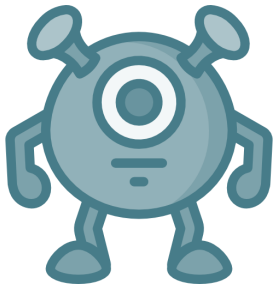
Como SHA256 é uma
função hash criptografada,
a única maneira é tentativa
e erro

SHA256

Probabilidade: $1/2^{30}$ ≒ $\frac{1}{\text{1 bilhão}}$

30 primeiros bits = 0





Razão

Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 40
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...

1075315731

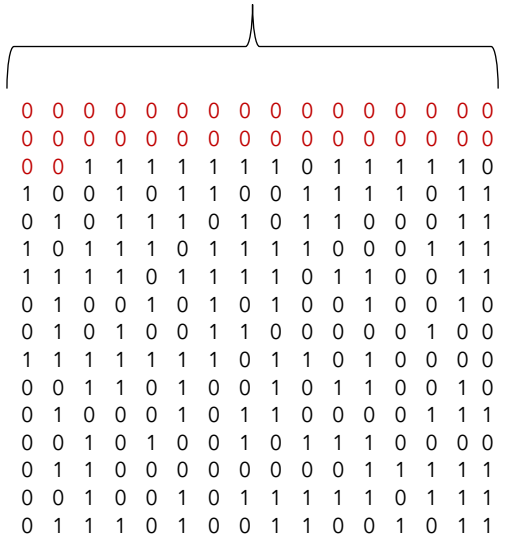
Todo esse esforço está intrinsicamente conectado com a lista de transaçoes

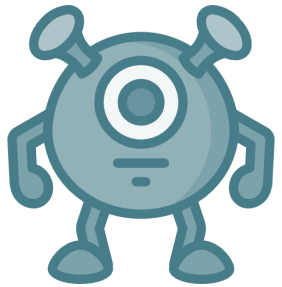
Isso se chama "**Proof of Work**"

Probabilidade: $1/2^{30} \fallingdotseq \frac{1}{1\text{ bilhão}}$

30 zeros?

SHA256





Razão

Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** **RR 4000**
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...

~~1075315731~~

1...

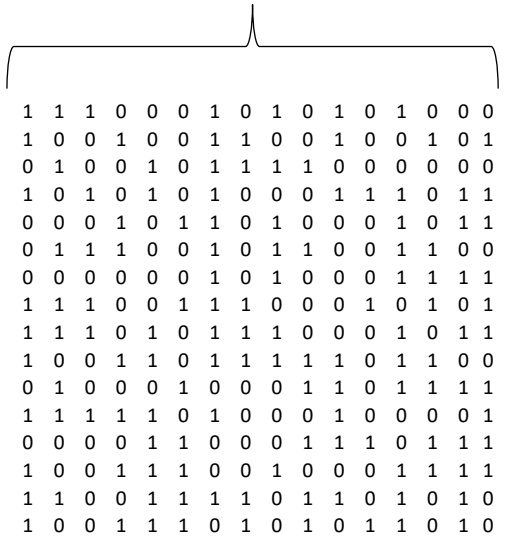
Todo esse esforço está intrinsicamente conectado com a lista de transaçoes

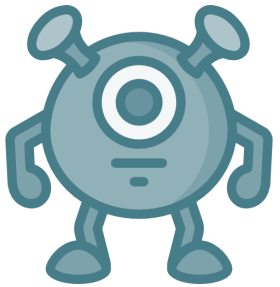
Isso se chama "**Proof of Work**"

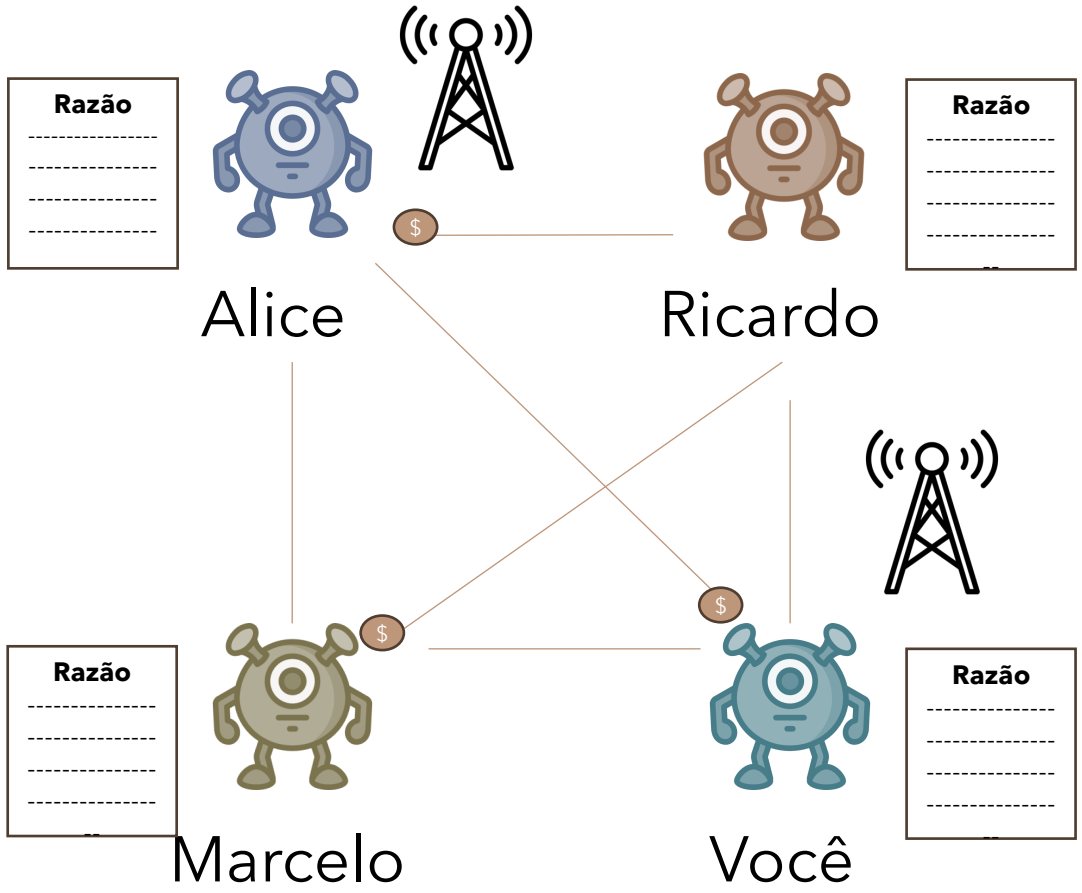
Probabilidade: $1/2^{30} \fallingdotseq \frac{1}{1 \text{ bilhão}}$

~~**30 zeros?**~~

SHA256






Razão
Razão
Alice
Ricardo
Razão
Razão
Marcelo
Você

Blocos

Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 40
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...

Proof of Work

Blocos

Alice paga **Ricardo** RR 30
Ricardo paga **Marcelo** RR 50
Marcelo paga **você** RR 80
Você paga **Alice** RR 20
...

Proof of Work

Blocos

Ricardo paga **Marcelo** RR 30
Você paga **Alice** RR 100
Alice paga **Ricardo** RR 300
Marcelo paga **você** RR 20
...

Proof of Work

Blocos

Alice paga **Ricardo** RR 20
(Assinatura)
Marcelo paga **você** RR 30
(Assinatura)
...

6415156123468

Só é **válida** quando assinada

SHA256

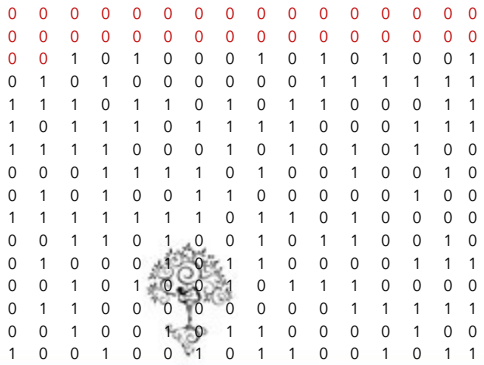
Bloco só é **válido** quando possui um *Proof of Work*

Blocos

Alice paga **Ricardo** RR 30
(Assinatura)
Marcelo paga **você** RR 80
(Assinatura)
...

11111561453468

SHA256



Blocos

Ricardo paga **Marcelo** RR 30
(Assinatura)
Alice paga **Ricardo** RR 300
(Assinatura)
...

6511212312313

SHA256

Blocos

Hash do bloco anterior

Alice paga **Ricardo** RR 20
(Assinatura)
Marcelo paga **você** RR 30
(Assinatura)
...

Proof of Work

SHA256

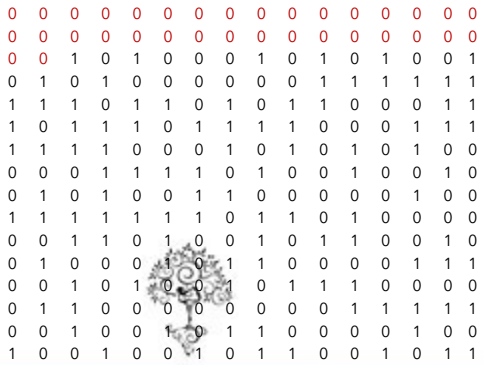
Blocos

Hash do bloco anterior

Alice paga **Ricardo** RR 30
(Assinatura)
Marcelo paga **você** RR 30
(Assinatura)
...

Proof of Work

SHA256



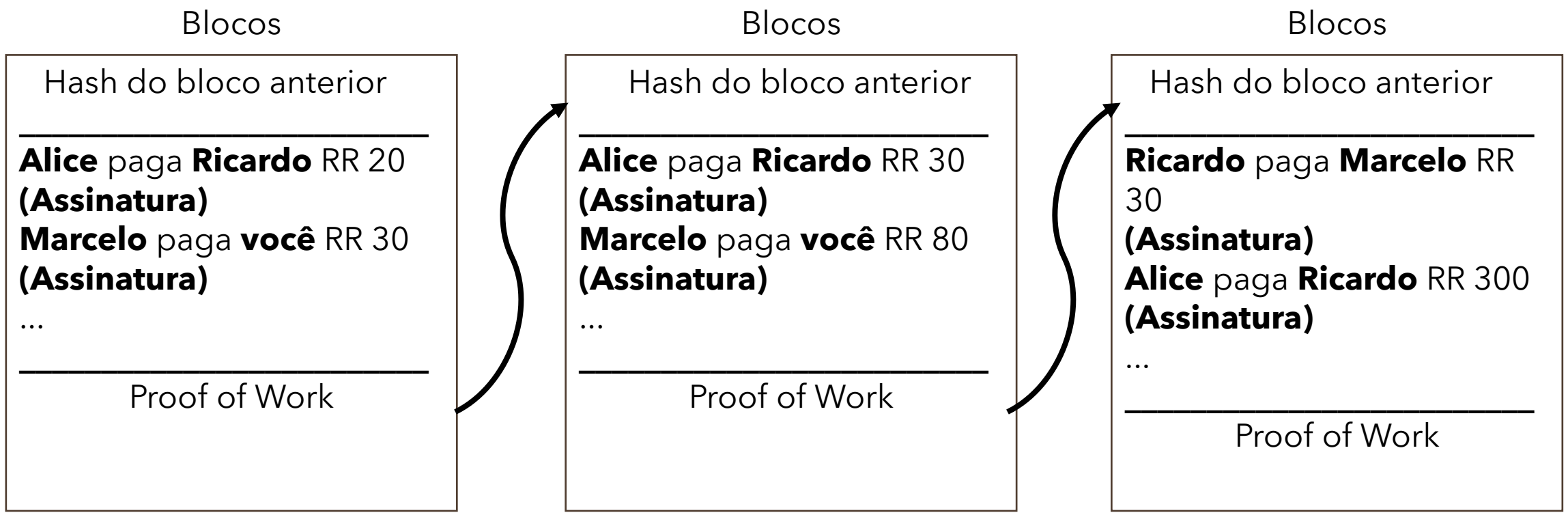
Blocos

Hash do bloco anterior

Ricardo paga **Marcelo** RR 30
(Assinatura)
Alice paga **Ricardo** RR 300
(Assinatura)
...

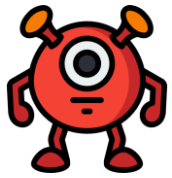
Proof of Work

SHA256

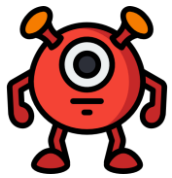


~~**Razão**~~

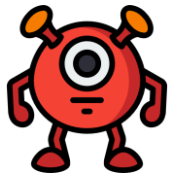
"Block Chain" (Rede/Cadeia de Blocos)



Criador de Bloco 1



Criador de Bloco 2

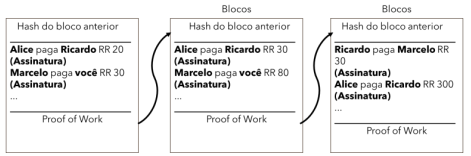


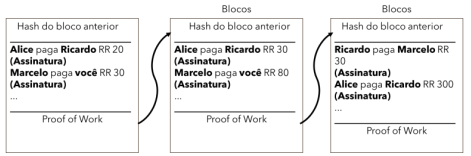
Criador de Bloco 3

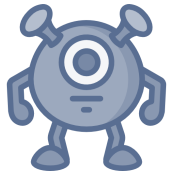
Hash do Bloco Anterior

546121235

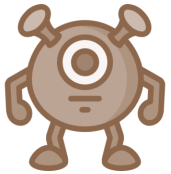
SHA256





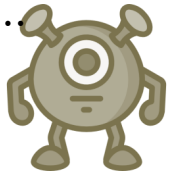


Alice

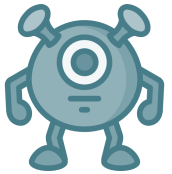


Ricardo

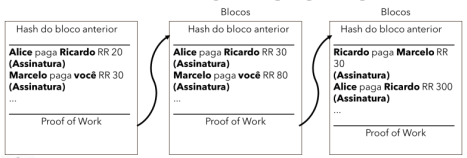
Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 200
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...

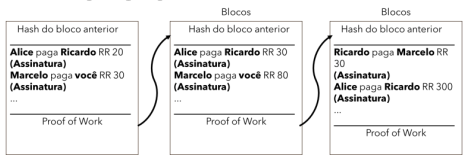


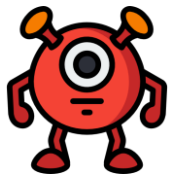
Marcelo



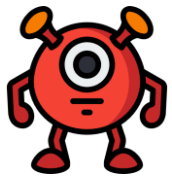
Você



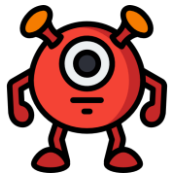




Criador de Bloco 1



Criador de Bloco 2

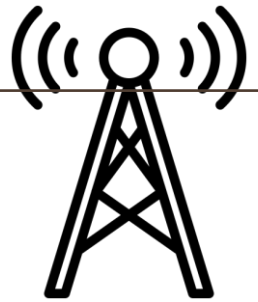


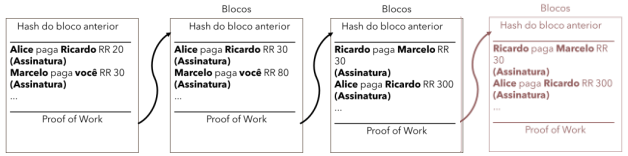
Criador de Bloco 3

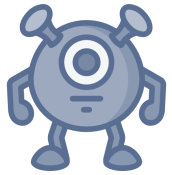
Hash do Bloco Anterior

Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 200
Marcelo paga **você** RR 30
Você paga **Alice** RR 10
...

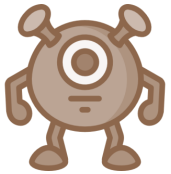
546121235



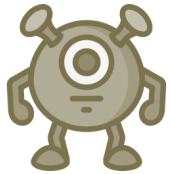




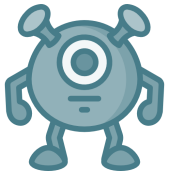
Alice



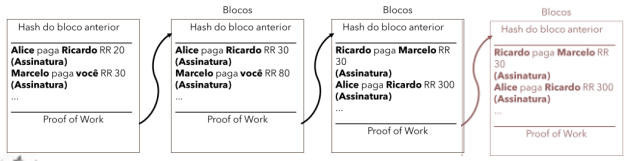
Ricardo

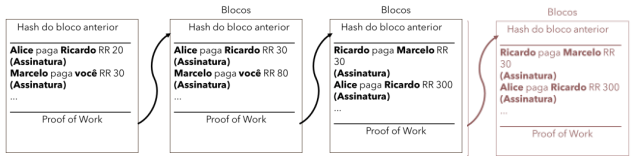


Marcelo



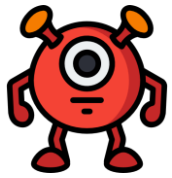
Você



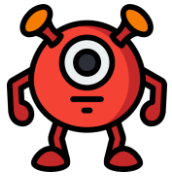


Requer muito trabalho e novos bits de moeda na economia

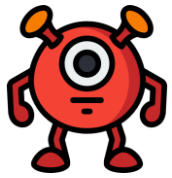
Mineração



Criador de Bloco 1



Criador de Bloco 2



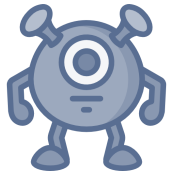
Criador de Bloco 3

Recompensa:

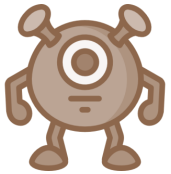
Hash do Bloco Anterior

Criador 1 ganha 10 RR
Alice paga **Ricardo** RR 20
Ricardo paga **Marcelo** RR 200
Marcelo paga **você** RR 30
Você paga **Alice** RR 10

546121235

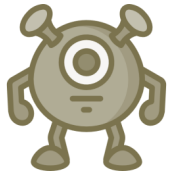


Alice

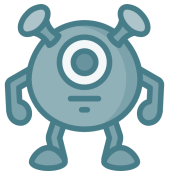


Ricardo

- Não é necessário assinatura ou destinatário
- Aumenta o total de dinheiro no sistema



Marcelo

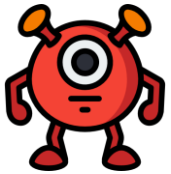


Você

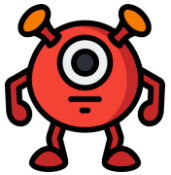
- Dessa forma, quando você escutar sobre mineração, relembre:

1. Eles estão escutando por transações;
2. Criando blocos (com *proof of work*);
3. Transmitindo novos blocos;
4. E sendo recompensados por isso!

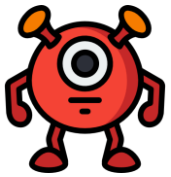
Mineração



Minerador 1



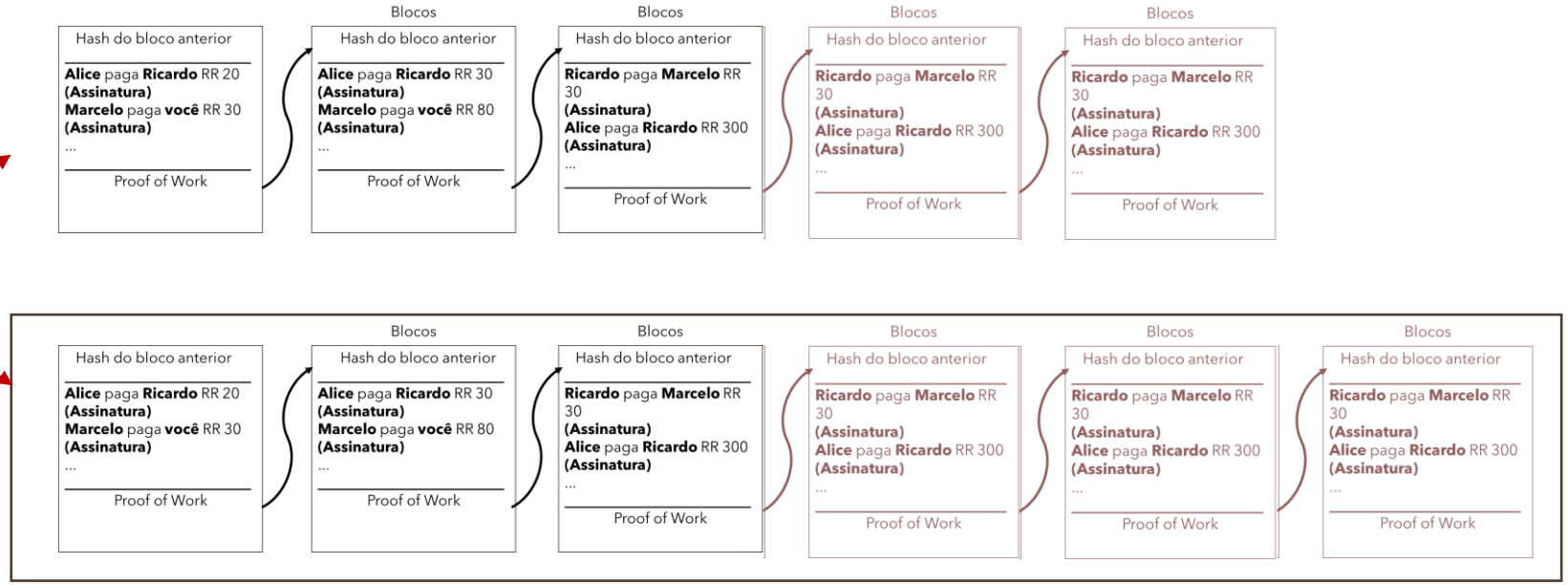
Minerador 2

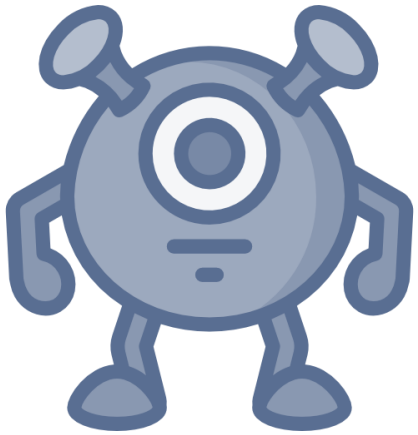


Minerador 3

- Dessa forma, ao invés de escutar transações, as pessoas escutam **a transmissão dos blocos**

Conflito?

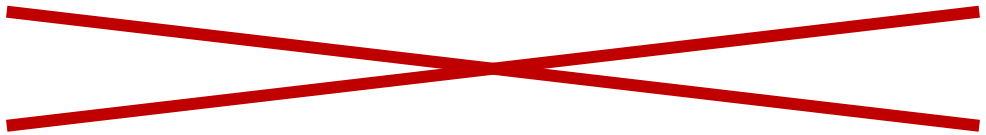




Confiar naquela que foi colocado mais **esforço computacional!**

Então ainda que não exista uma **autoridade central** e se todos estão mantendo sua própria cópia do *blockchain* e se todos concordarem em **dar preferência** para **qualquer bloco** que tem o **maior trabalho colocado nele**, nós chegamos a um **consenso descentralizado**

Confiar no esforço computacional



Vamos imaginar se alguém quisesse fraudar

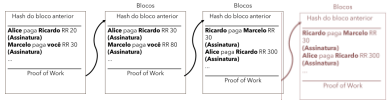
Hash do Bloco Anterior

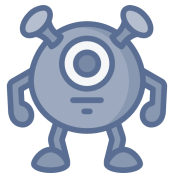
....

Alice pagou **Ricardo** **100 RR**

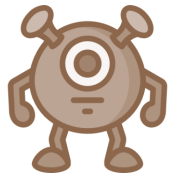
....

121564562318

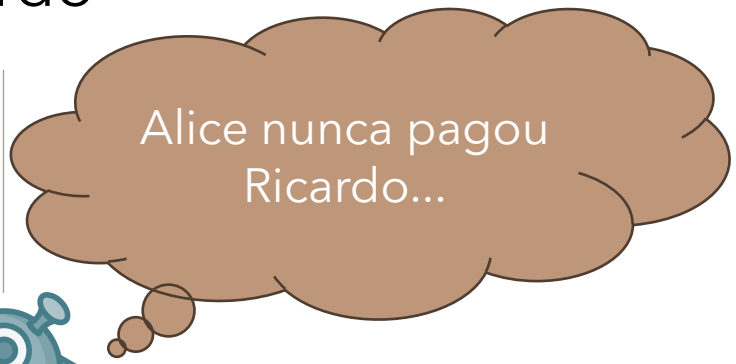


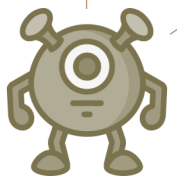


Alice

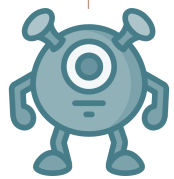


Ricardo

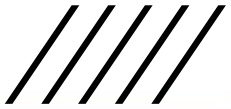




Marcelo

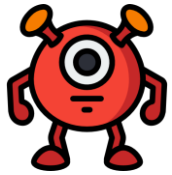


Você

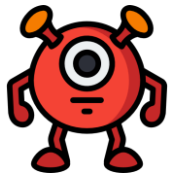


Vamos imaginar se alguém quisesse fraudar

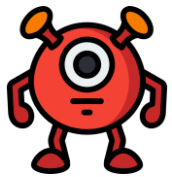
Mineração



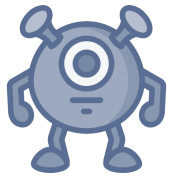
Minerador 1



Minerador 2

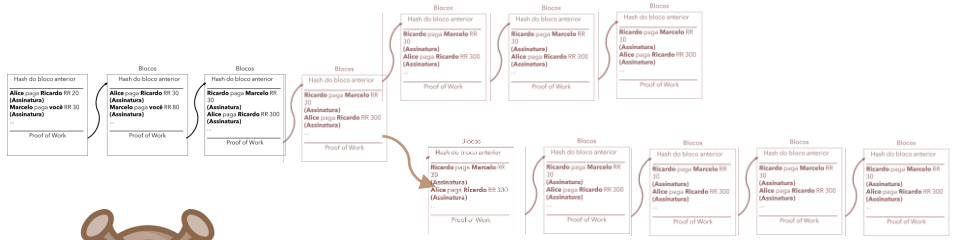


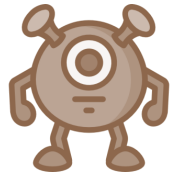
Minerador 3



Alice

Alice precisaria colocar todo esforço sozinha





Ricardo

Confiamos no mais longo

Porém, Ricardo ainda continuaria ouvindo a transmissão dos **outros mineradores**...

Ideias principais

- Assinaturas Digitais
- O livro razão **É A MOEDA**
- Descentralizado
- *Proof of Work*
- *Block chain*

Média de Criação de Blocos

10 minutos

12 segundos

Recompensas pela mineração

- Jan 2009 – Nov 2012: 50 BTC
- Nov 2012 – Jul 2016: 25 BTC
- Jul 2016 – Fev 2020: 12,5 BTC
- Fev 2020 – Set 2023: 6,25 BTC

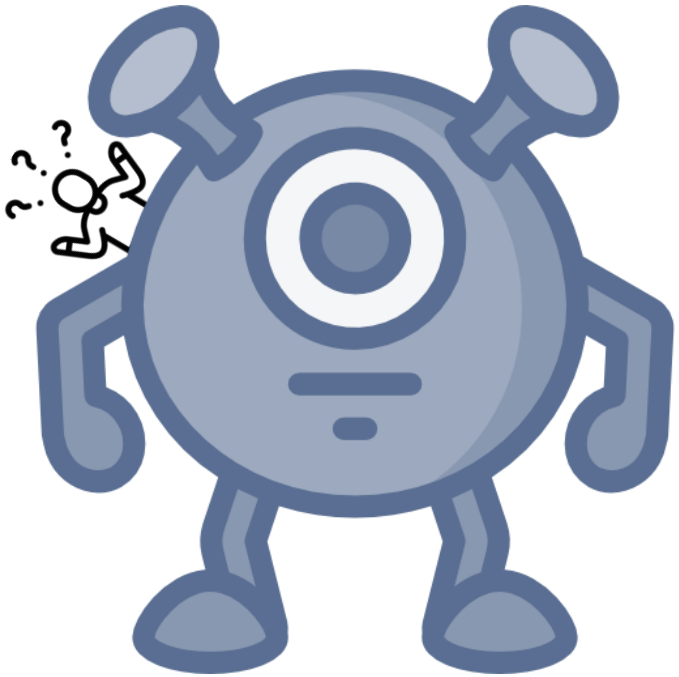
½ a cada 4 anos....

Total: 21 milhões de BTCs ao final...

No Biticoin...

Limitado a mais ou menos 2400 transações

Deu pra ter uma **noção geral**?



Vamos explorar

https://blockexplorer.one/

https://oxt.me/

https://www.coindesk.com

Hacker rouba 7mil *bitcoins* da Binance

Markets

Hackers Steal $40.7 Million in Bitcoin From Crypto Exchange Binance

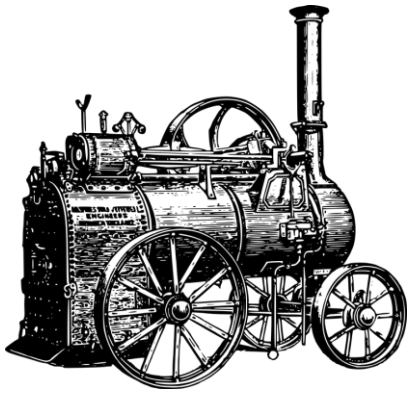
Crypto exchange Binance has disclosed a 7,000 BTC loss following the discovery of what it called a "large scale security breach."

By Nikhilesh De May 7, 2019 at 8:57 p.m. Updated Sep 13, 2021 at 6:09 a.m.

Binance CEO Changpeng Zhao

Vamos refletir...

- 1400s – *Gap* do Conhecimento
- 1800s – *Gap* Energético
- 1900s – *Gap* da Distância



- 2000s – Próximo Gap?

Alguns projetos em Andamento

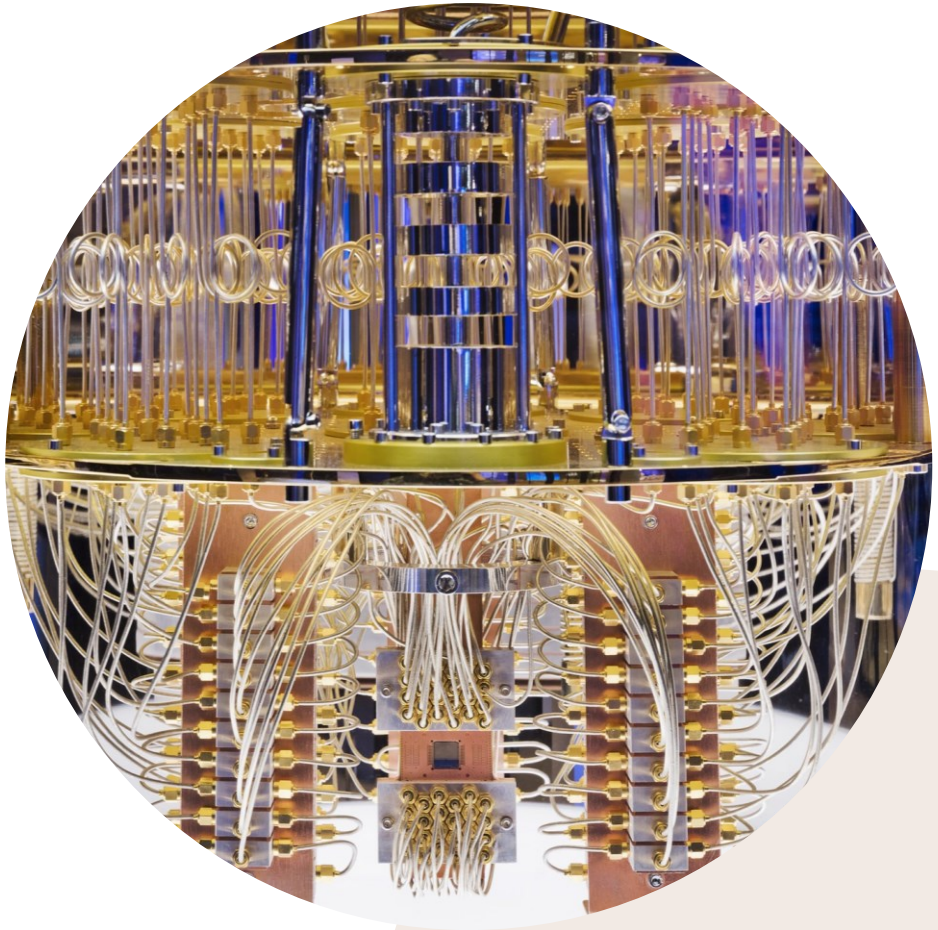
- Real Digital;
- Central Bank Digital Currency dos Estados Unidos;
- Contratos Inteligentes [em compras públicas] (projeto de pesquisa no Estado de SC)

Algumas possíveis aplicações

DETRAN

Quais sãos os desafios **práticos**?

O que esperar do **futuro**?



Referências

As imagens retiradas nessa apresentação foram retiradas de www.flaticon.com

3Blue1Brown (2019). **But how does biticoin actually work?**

Ivan on Tech (2021). **Tracking Bitcoin Transactions (Forensics) - Programmer explains**

Obrigado!

Marcelo Freitas
Pesquisador da FAPESC na área de Auditoria Contínua (CGE-SC) ||...

Contatos
E-mail: mmf.marcelofreitas@gmail.com ou marcelofreitas@cge.sc.gov.br
Lattes: http://lattes.cnpq.br/1621974592687502
Redes: @marcelofreitas_mmf