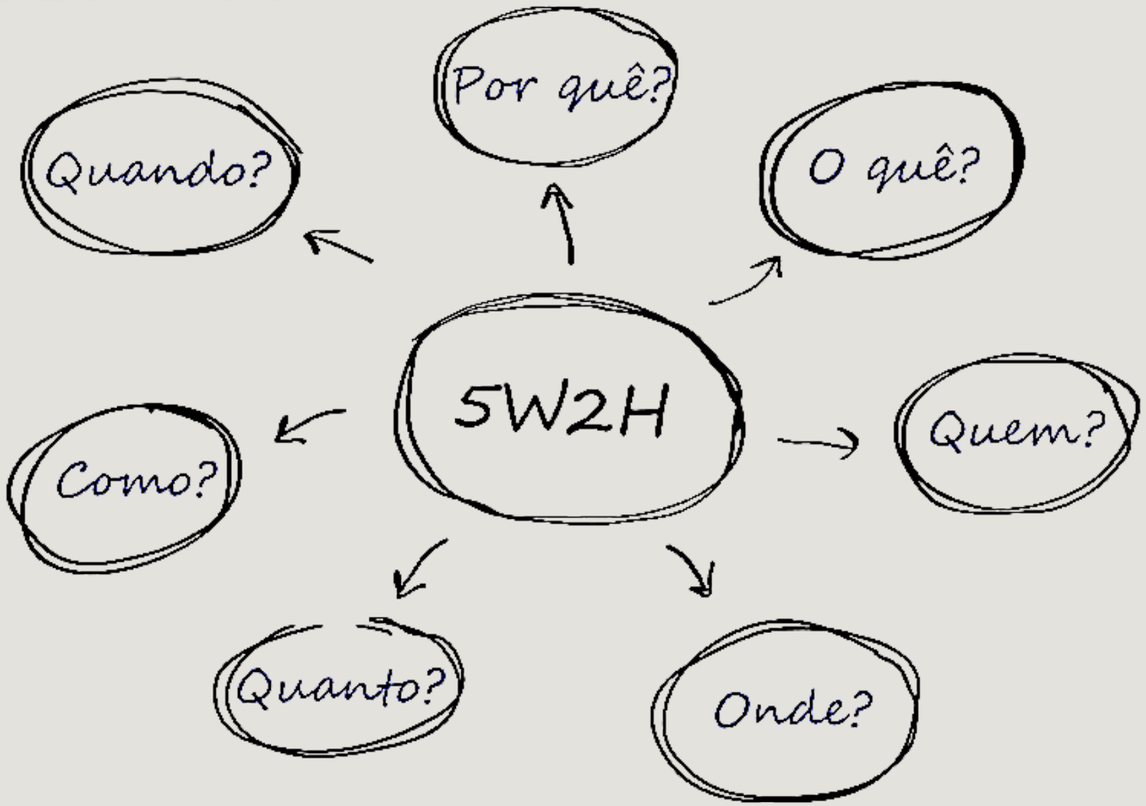
bitups

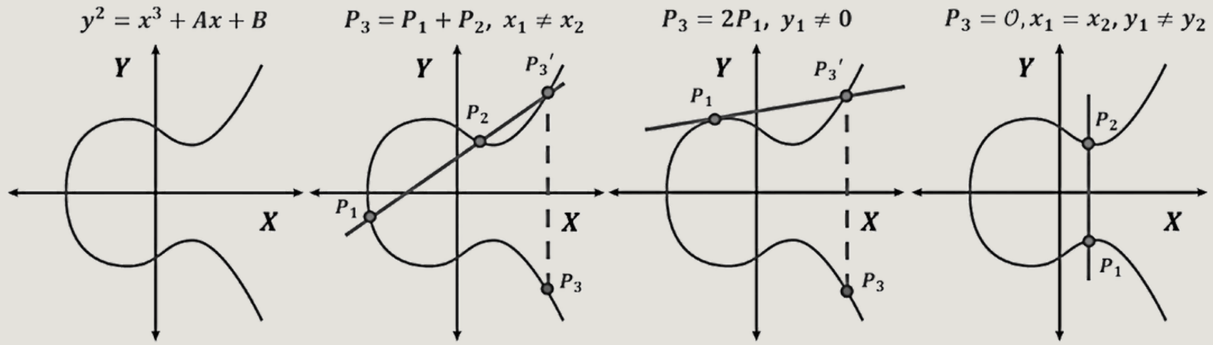
O que realmente é o Bitcoin (e o que não te contaram sobre a tecnologia por trás dele)

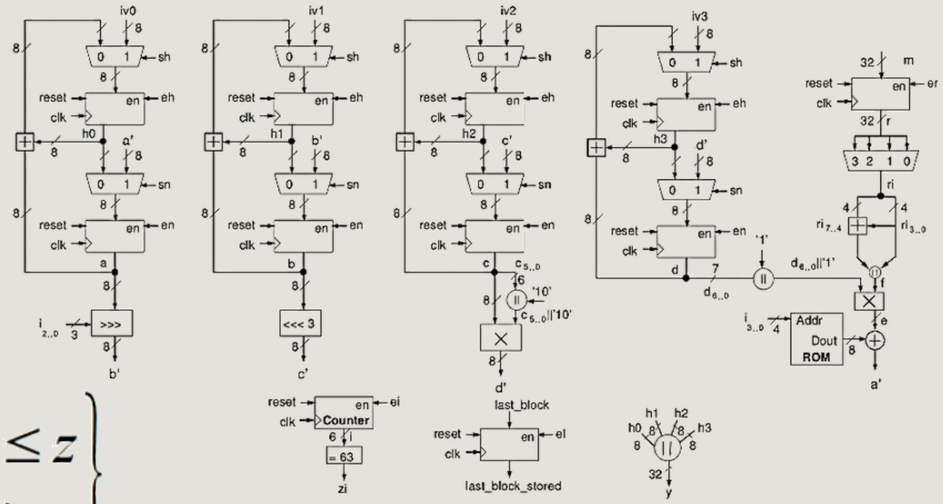
Disclaimer 1 : 5W 2H

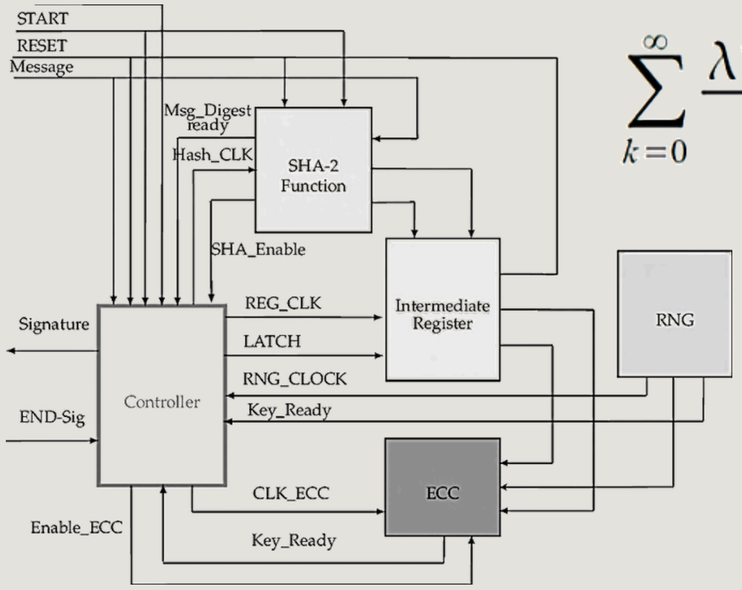
O foco será apenas no “o quê” (*What?*) e no “como” (*How*?) da tecnologia Bitcoin



Disclaimer 2 : O que não veremos







$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

$$\sum_{i=0}^{32} 210{,}000 \frac{50}{2^i}$$

Algorithm 6 Split-ECDSA (SECDSA) signature generation
Input: message M, SCE-key $u \in \mathbb{F}_q^*$, PIN-key $\sigma \in \mathbb{F}_q^*$
Output signature (r, s).

1: Compute $\mathcal{H}(M)$ and convert this to an integer e.
2: Compute $e' = \sigma^{-1} \cdot e \bmod q$
3: Select random $k \in \{1, ..., q-1\}$
4: Compute $kG = (x, y)$ and convert x to integer $\bar{x}$
5: Compute $r = \bar{x} \bmod q$. If $r = 0$ go to Line 1
6: If $r \bmod q = 0$ then go to Line 1
7: Compute $s_0 = k^{-1}(e' + u \cdot r) \bmod q$. If $s_0 = 0$ go to Line 1
8: Compute $s = \sigma \cdot s_0 \bmod q$
9: Return (r, s)

Tecnologias Fundamentais

Para entender internamente o BTC, é preciso conhecer duas outras tecnologias das quais derivam as suas estruturas:

- **Função “HASH”**
- **Criptografia Assimétrica.**

Função HASH

Propriedades:

- Resultado de tamanho fixo
- Entradas iguais = HASHes iguais
- Alteração mínima na entrada = HASH completamente diferente
- Resultado da função é unidirecional

SHA256

This SHA256 online tool helps you calculate hashes from strings. You can input UTF-8, UTF-16, Hex, Base64, or other encodings. It also supports HMAC.

Settings

Hash

Auto Update

Remember Input

Input Encoding

UTF-8

Output Encoding

Hex (Lower Case)

Enable HMAC

Input

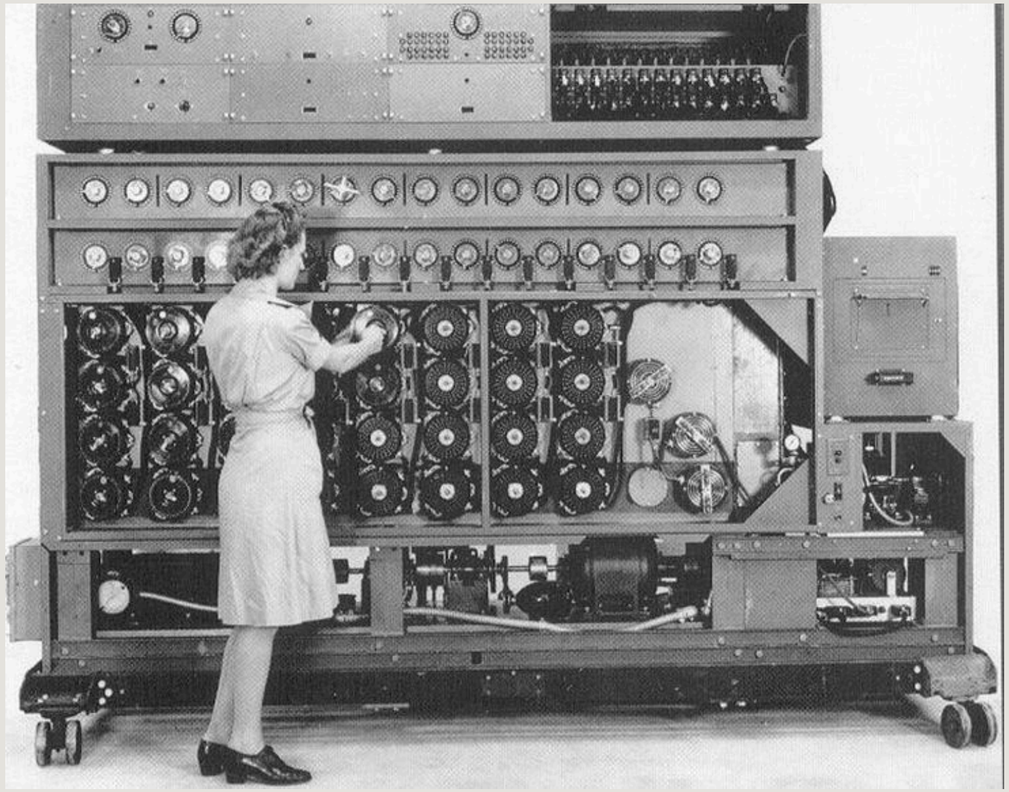
Enter here...

Output

Output here...

Share Link

Criptografia?



t e n i s

p o l a r

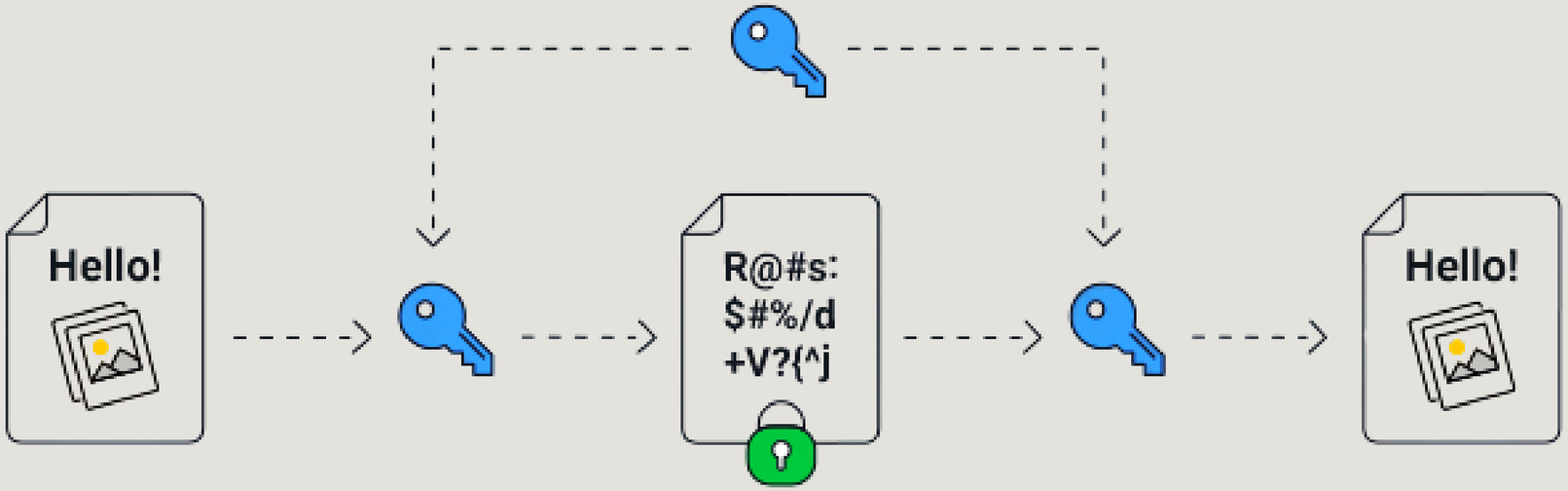
TE ENCONTRO NA PRAÇA DEPOIS DA AULA

PO OLCELPRE LI TSIÇI DOTOAR DI IUNI

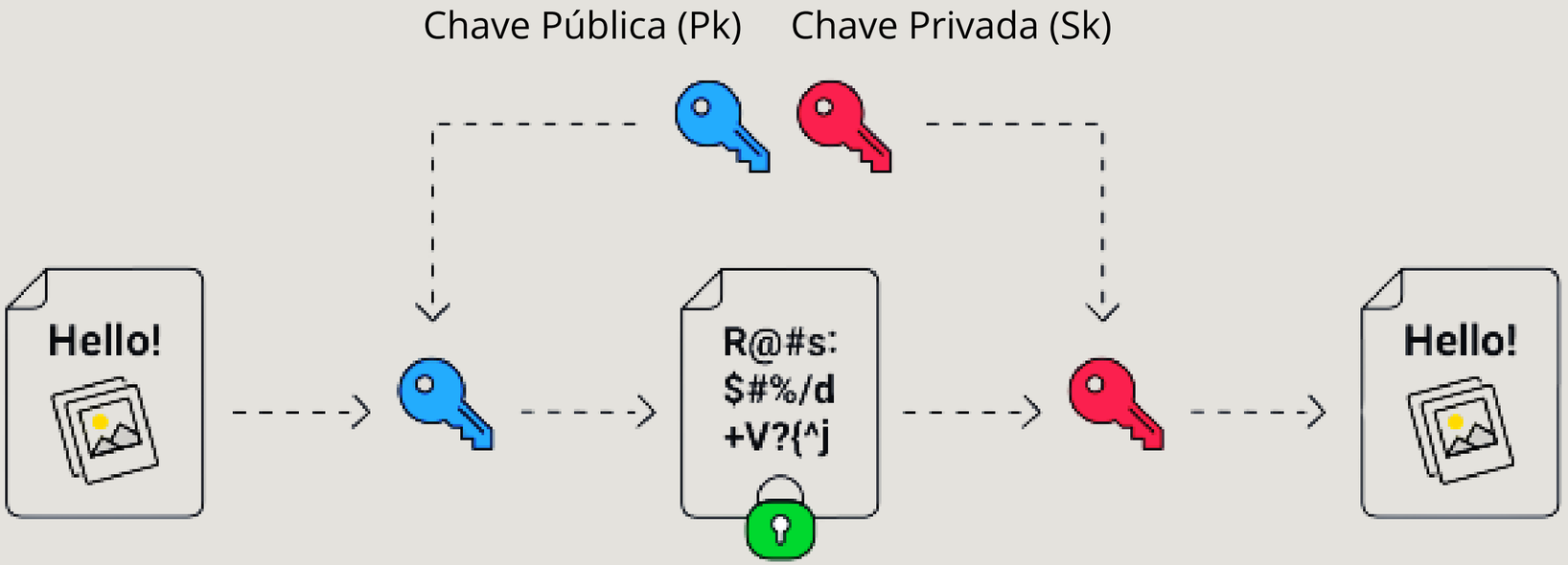
NOSTR

Criptografia Simétrica

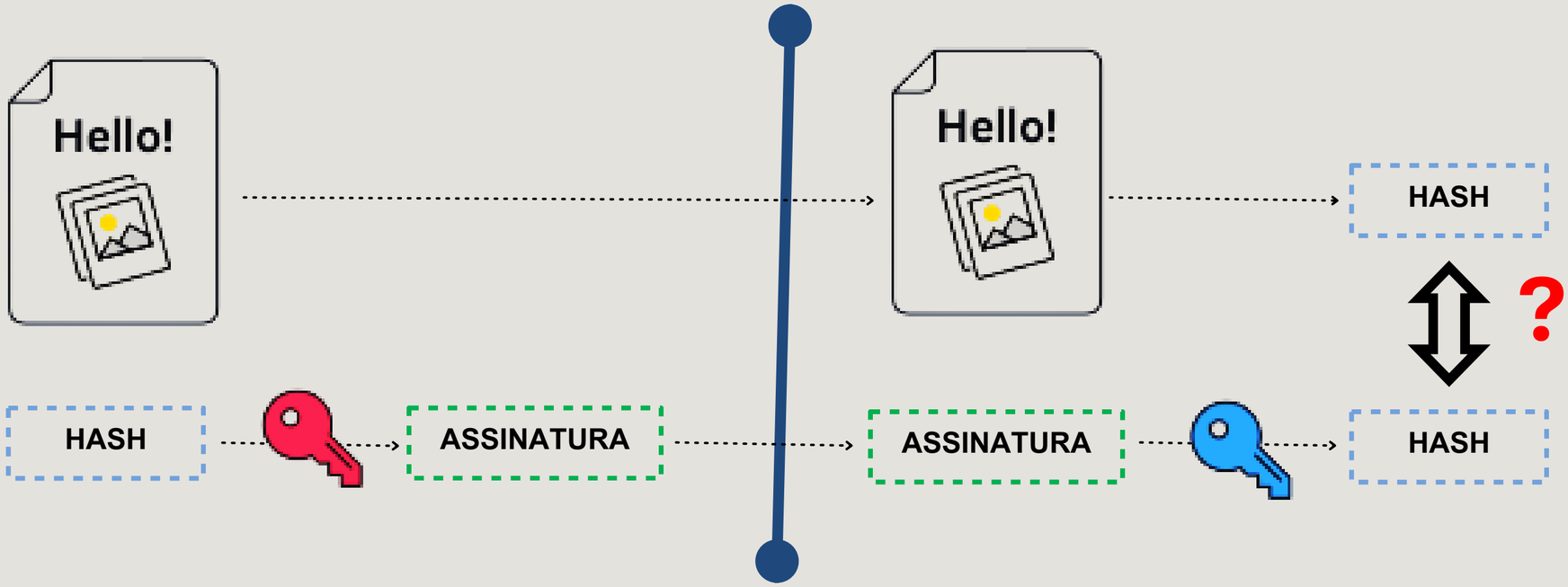
Chave previamente conhecida pelo emissor e pelo receptor da mensagem



Criptografia Assimétrica



Assinatura Digital



ECDSA Key Generator

This online tool helps you generate a pair of ECDSA keys. It supports PEM, HEX, and Base64 formats, as well as various curves. The PEM format supports PKCS#1, PKCS#5, and PKCS#8.

Settings

Generate

Auto Update

Remember Input

Curve

SECG secp256k1 / X9.63 ansip256k1

Output Type

Hex

Private Key

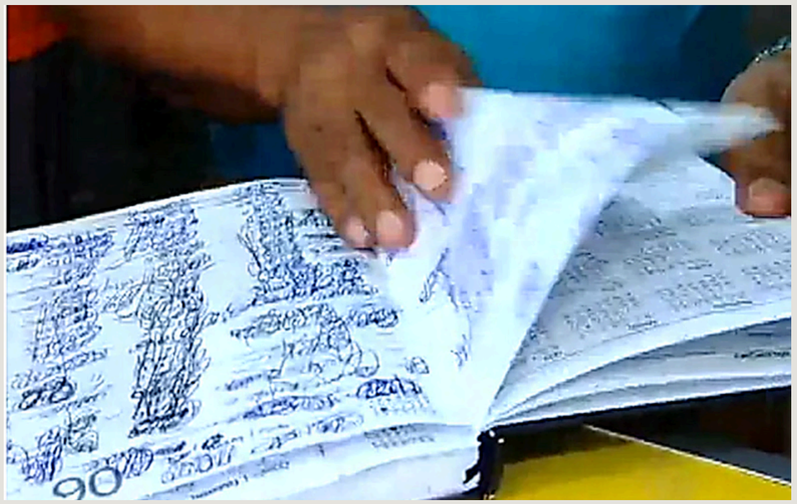
2441245f54d7a7b8693c813fbd2163d76fcccb7081943445530fdc8f6ef9ec55

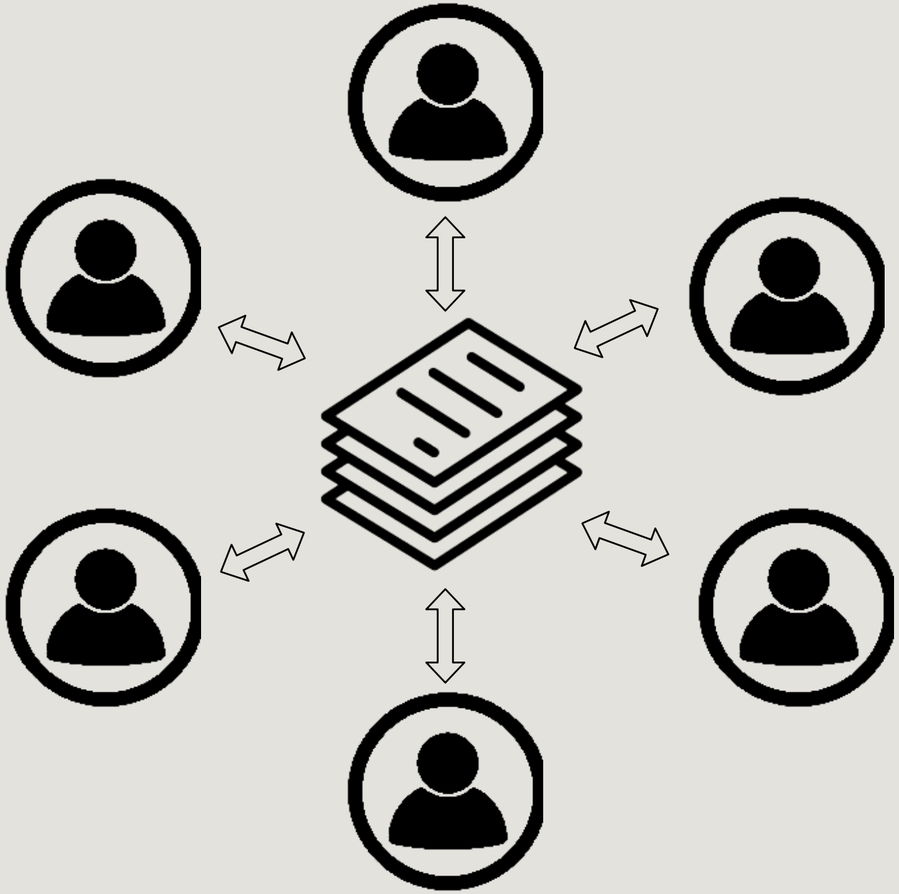
Public Key

042c26f839763268722729d303aadddf8591aeef0412aca9129e628718d5863298262862cd38334564413c94abe480bb68ddbc2584b7f187d533f5bc60303dc2e0

Share Link

O Caderninho de Fiado





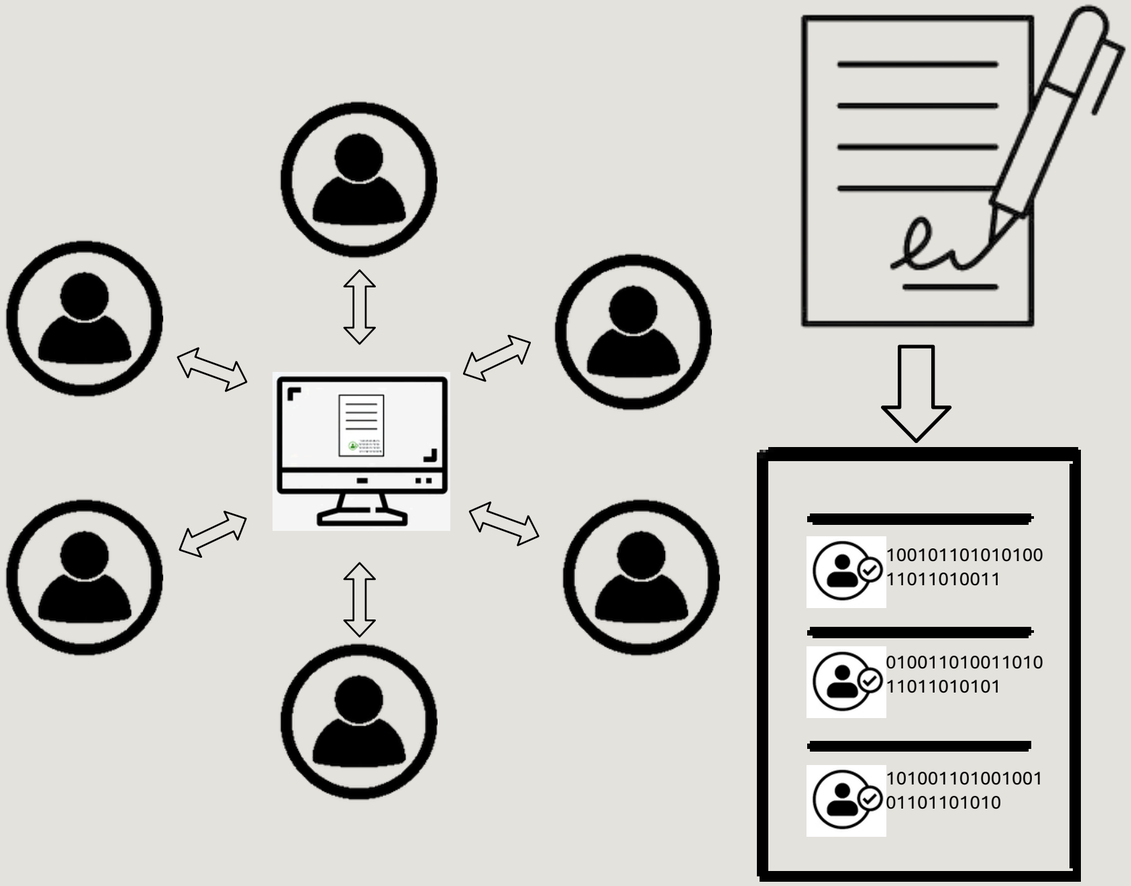
NOSTR

O Livro-Registro

Do uso coletivo, emergiram regras:

- O registro é o próprio dinheiro
- Proibido gastar além dos fundos que já possui
- Cada página deve ser validada e assinada por um conferente
- O conferente ganha 10$ pelo trabalho
- Outro participante interessado assume o controle do Livro

O Livro-registro Digital



Pela sua natureza centralizada, esse sistema voltou aos problemas do bancarismo

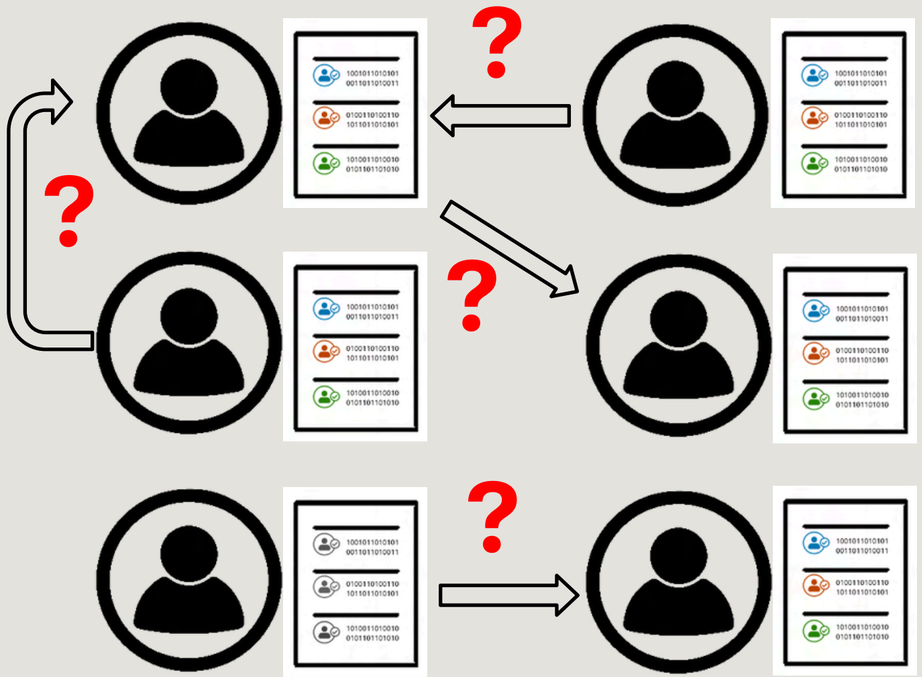
NOSTR

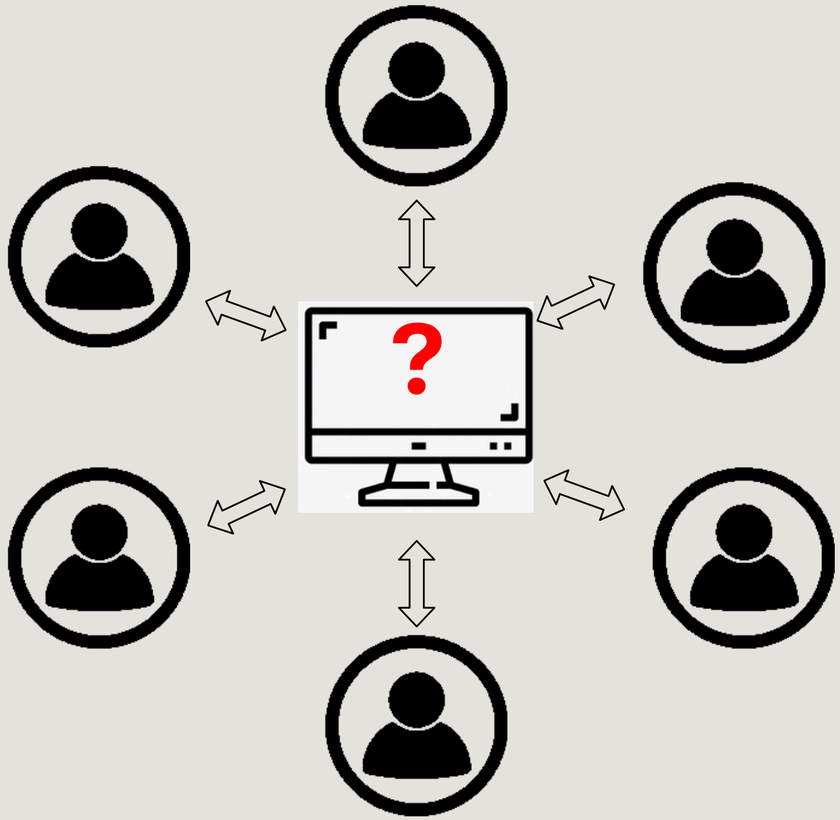
Tentativa de Solução

Já que a centralização é um problema, porque cada participante não poderia ter sua própria cópia do Livro-registro?

NOSTR

Descentralização X Centralização





A Solução de Satoshi Nakamoto

A obra-prima de um gênio: Blockchain

- **Hash**
- **Assinaturas digitais**
- **Prova de trabalho (PoW)**
- **Desempate: maior PoW**
- **Ajuste de dificuldade**

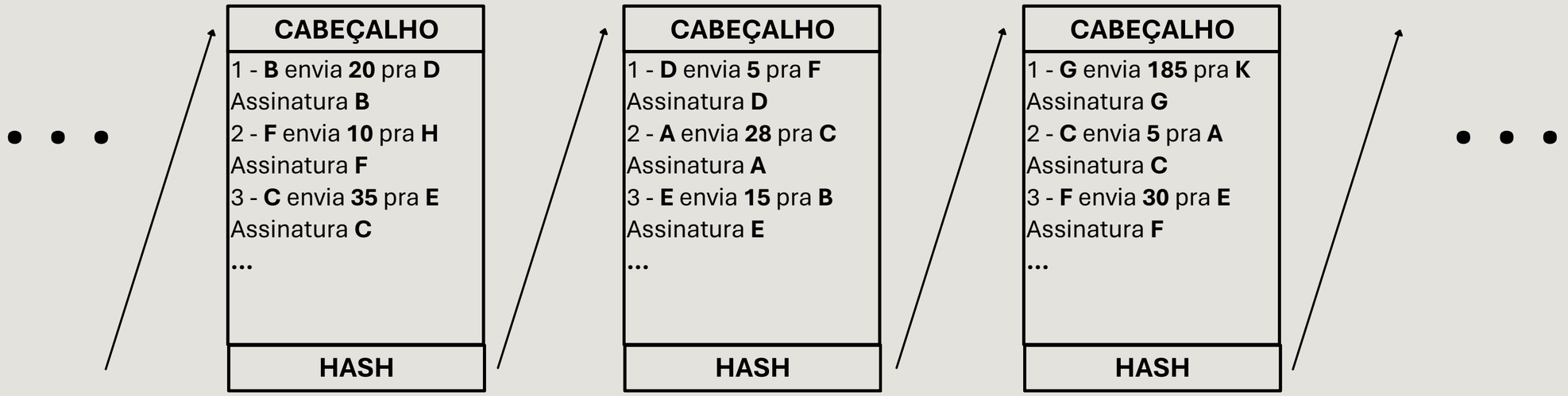
Blockchain

Todo usuário pode guardar uma cópia dinâmica da Blockchain inteira, enquanto ouve/transmite dados das transações para a rede

NOSTR

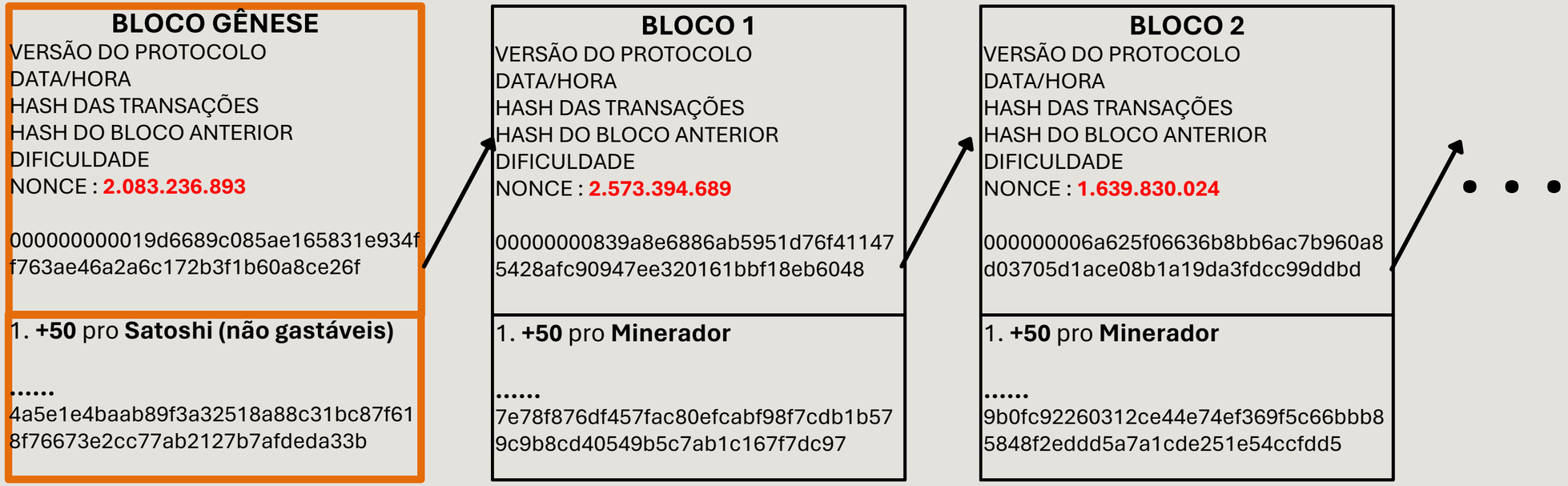
Blockchain

Cada “Bloco” representa uma página do Livro-registro, que se conecta aos outros blocos pelo HASH gerado por cada um



Prova de Trabalho - Encadeamento

Cada bloco só é válido se o seu HASH estiver de acordo com as regras e a dificuldade atuais da rede



Prova de Trabalho - Mineração

“Minerar” é o ato de descobrir (por tentativa e erro) o NONCE, que faz com que o bloco tenha um HASH abaixo da dificuldade atual da rede, validando-o

0000387 

0000387 

0000387 

0000387 

0000387 

0000387 

NOSTR

POWsim

proof of work simulator

# of zeroes

10

Message

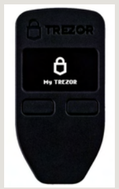
Message

Work!

What is this?

Especialização

No início da rede, todos eram simultaneamente <u>Mineradores</u>, <u>Nós</u> e <u>Usuários.</u> Com o tempo, os diferentes atores do sistema foram se especializando.

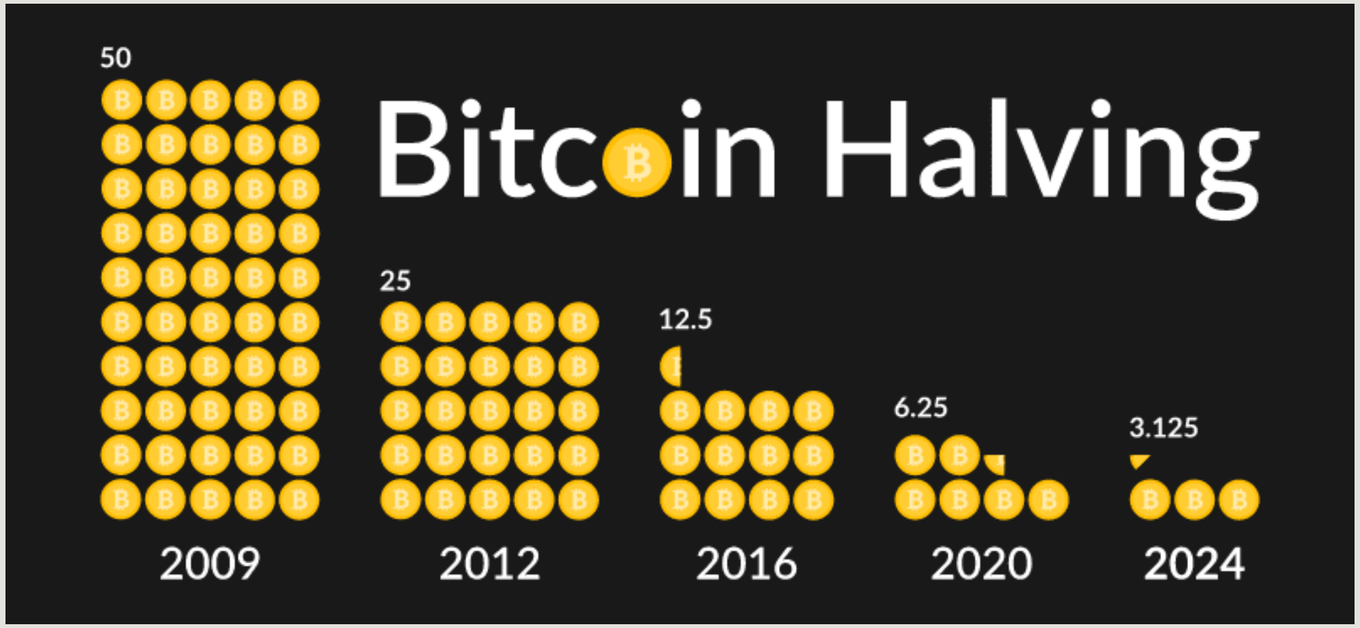


Mineração : Subsídio

Para recompensar aqueles que empregam poder computacional na mineração, quem primeiro encontrar o NONCE que valida o bloco e transmiti-lo para a rede, recebe um Subsídio de 50BTC + taxas

Mineração : Halving

Para que a emissão de novos BTC seguisse uma lógica deflacionária, a recompensa aos mineradores é dividida pela metade a cada 210.000 blocos (~4 anos)

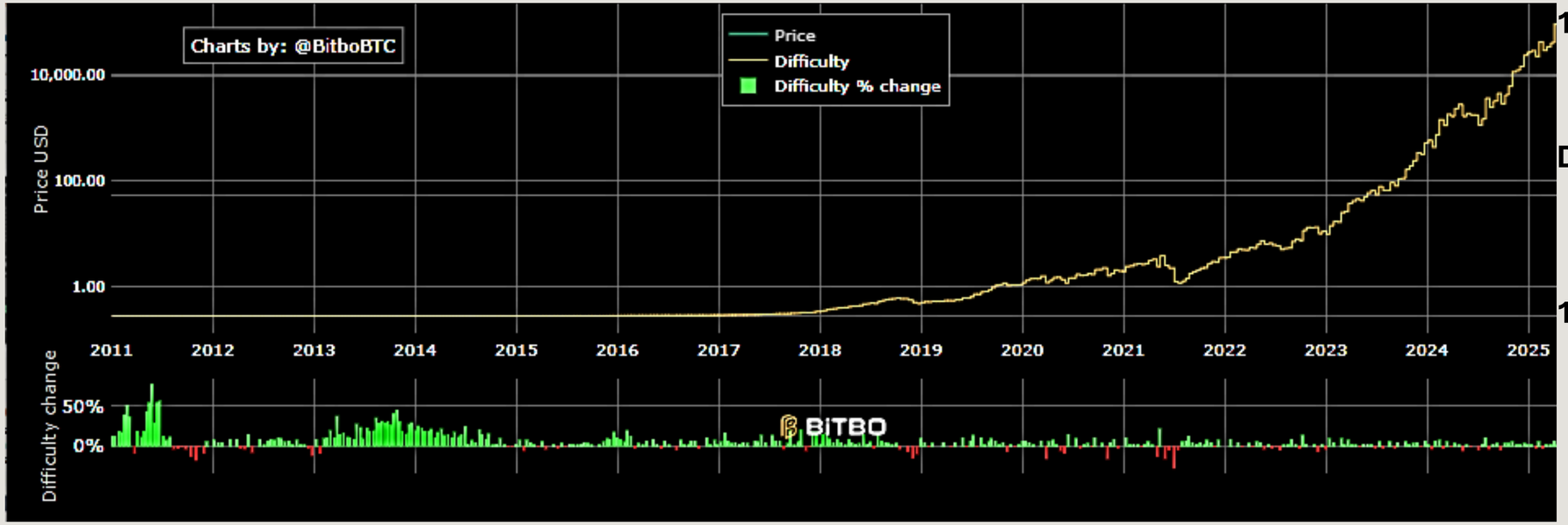


Mineração : Emissão de Novos Tokens

- **Cada um dos tokens existentes de BTC foi criado/emitido na mineração.**
- **Não existe “compensação externa” nem entrada ou saída de novos tokens na Blockchain.**
- **“Ter um BTC” é possuir uma chave privada que contenha tokens associados a ela.**

Ajuste de Dificuldade

A dificuldade é automaticamente ajustada a cada 2016 blocos, para que os próximos 2016 blocos sejam gerados aproximadamente a cada 14 dias



123.234.387.977.050

Dificuldade

1

POWsim

proof of work simulator

# of zeroes

10

Message

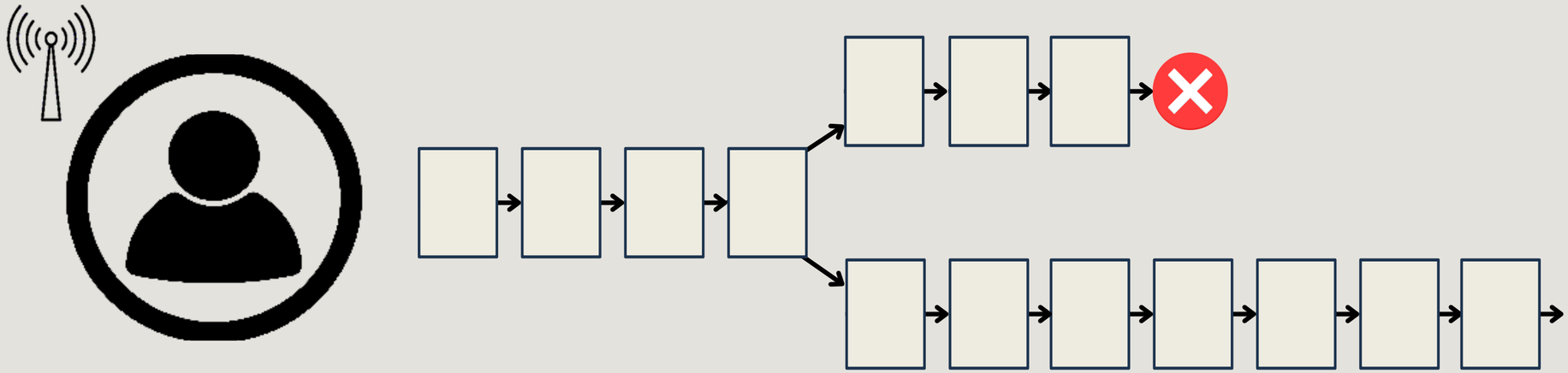
Message

Work!

What is this?

Critério de Desempate: Maior PoW

Em caso de dois blocos serem gerados e transmitidos simultaneamente, deve-se aguardar novos blocos e optar pela cadeia mais longa.

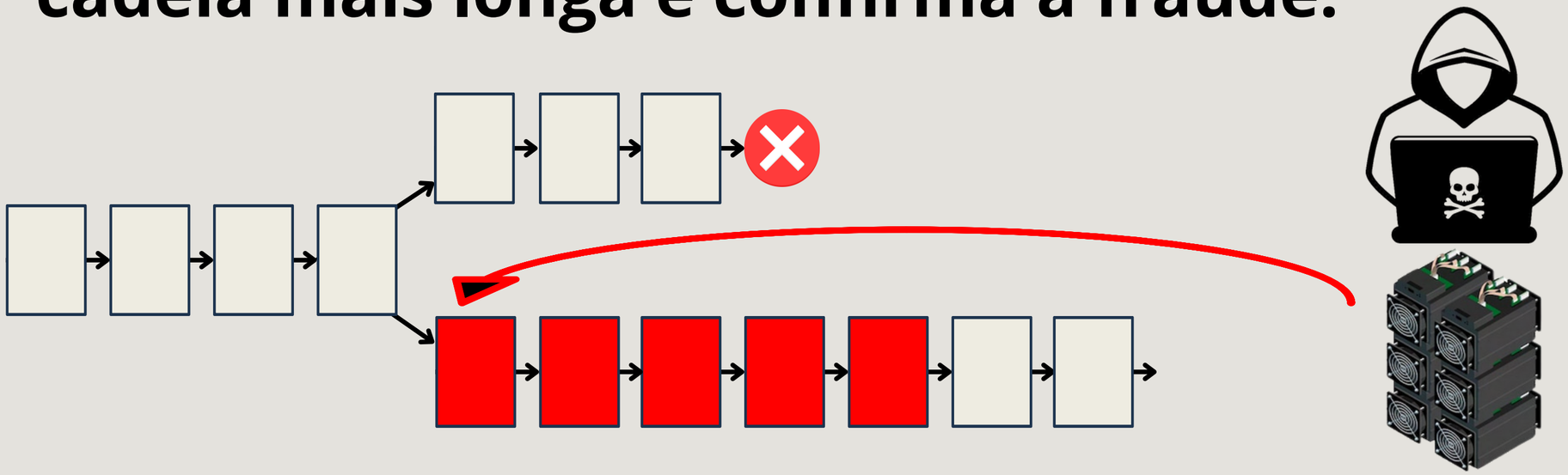


Hashrate

- O *Hashrate* é a medida total da capacidade de geração de HASHes de todos os mineradores, é medido em “Hashes/seg”
- Um termômetro da saúde da rede Bitcoin. Um hashrate maior aponta para um aumento no número de mineradores e, consequentemente um maior interesse e investimento na rede

Hashrate – Ataque de 51%

- O *Ataque de 51%* acontece quando alguém com uma altíssima capacidade computacional cria blocos com transações fraudulentas, vence a disputa pela cadeia mais longa e confirma a fraude.



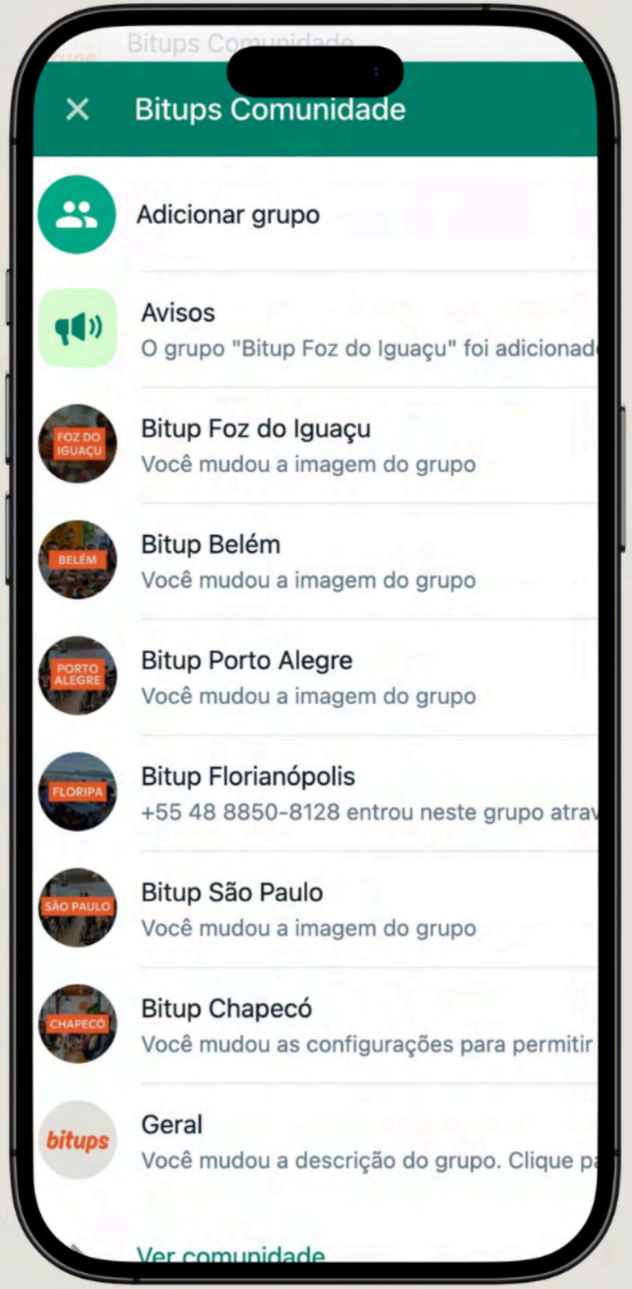
Bitcoin: Bitcoin Hashrate

kilo-	k or K*	10^3
mega-	M	10^6
giga-	G	10^9
tera-	T	10^{12}
peta-	P	10^{15}
exa-	E	10^{18}
zetta-	Z	10^{21}
yotta-	Y	10^{24}

bitups

Mensagem final:

Nada disso é necessário: apenas compre e guarde!



Bitups Comunidade

Comunidade do WhatsApp

bitups