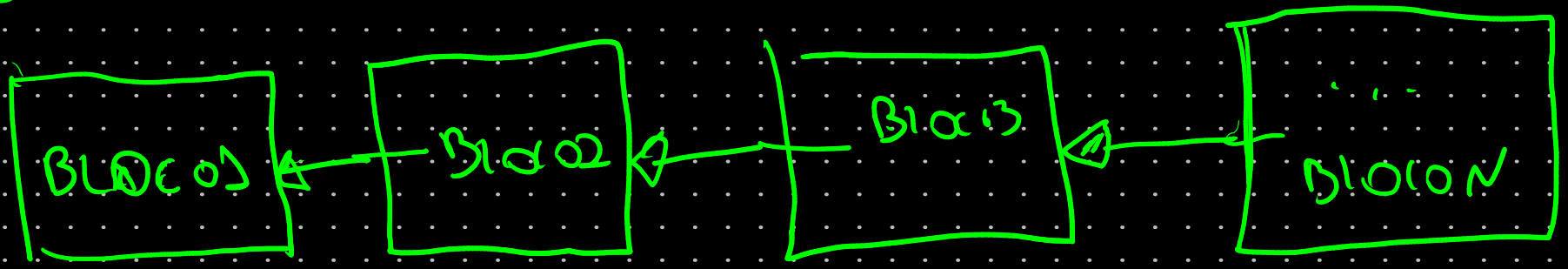
BLOCKCHAIN

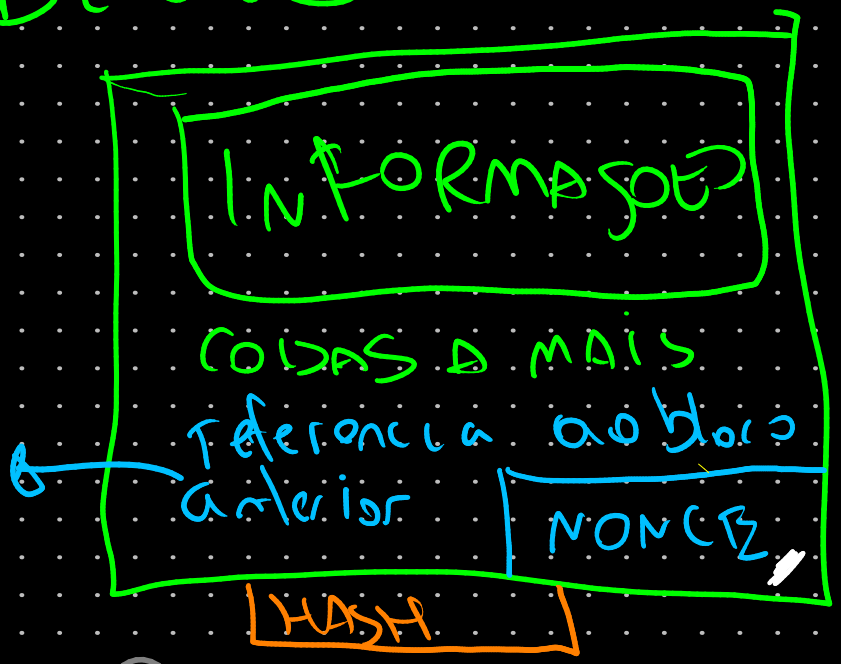
blockchain ≠ bitcoin / criptomoeda

Cadeia de Blocos



A ideia é uma cadeia de blocos distribuída e invidável

BLOCO

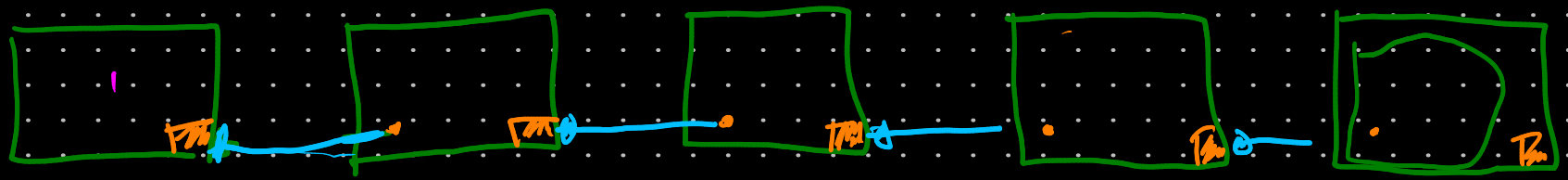


- Parece com uma lista encadeada, mas onde ela está.
- O que essa referência

Pegamos os bytes do bloco e geramos um hash

SHA256 → extremamente sensível a alterações

Se um bit apenas for alterado, o hash muda completamente

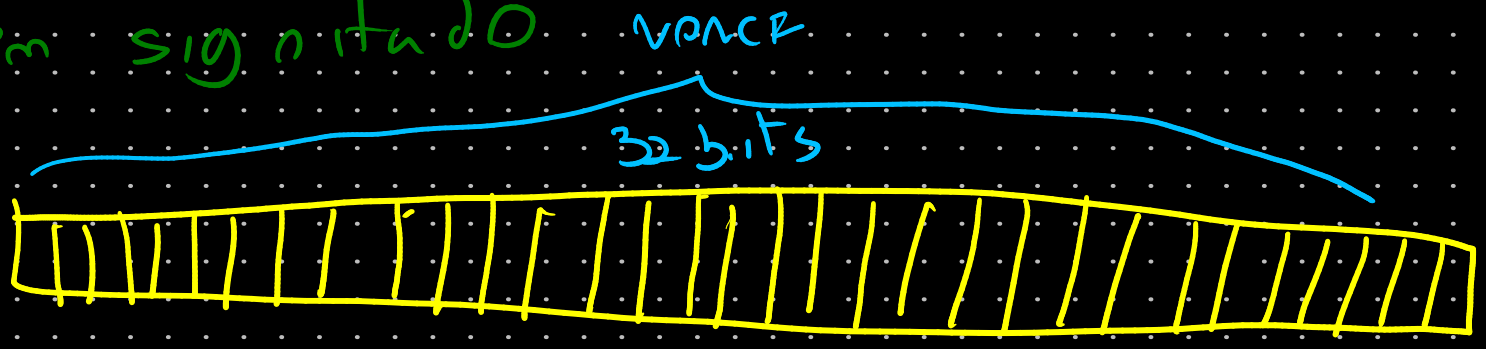


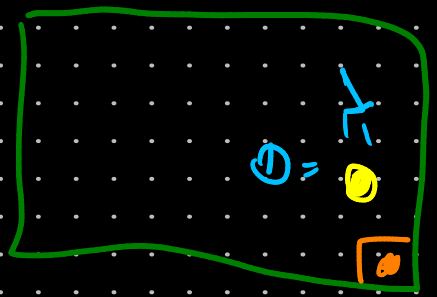
A blockchain é distribuída

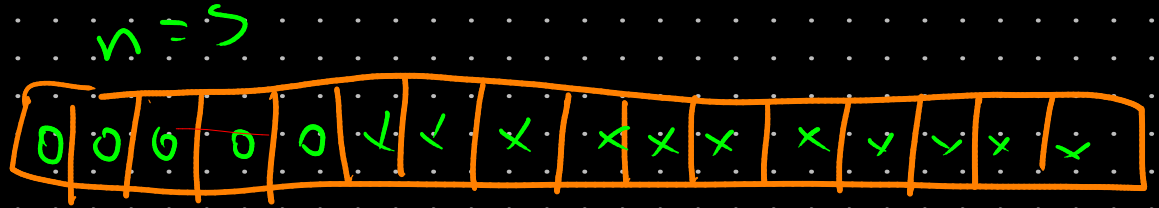
NONCE

É um valor numérico, a princípio sem significado

hash é sensível, mas muito sensível a mudanças







Para um bloco ser considerado válido, o hash precisa ter algumas propriedades

256 bits

→ os primeiros n bits do hash precisam ser 0

Para atingir essa propriedade, altera-se o valor no NONCE

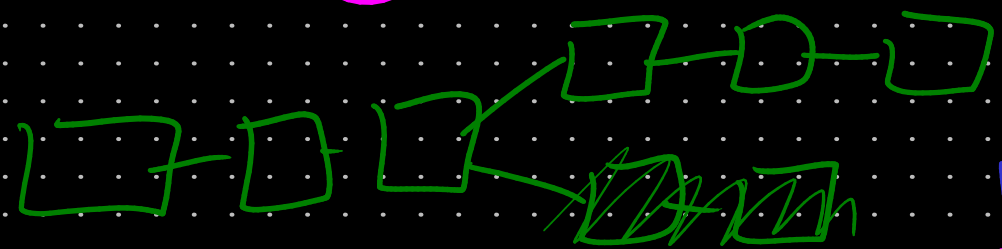
MINERAÇÃO

A REDE DE BLOCKCHAIN

Nó contendo a blockchain

INTERNET

Criação de informação



O que são as informação

Informação é gerada

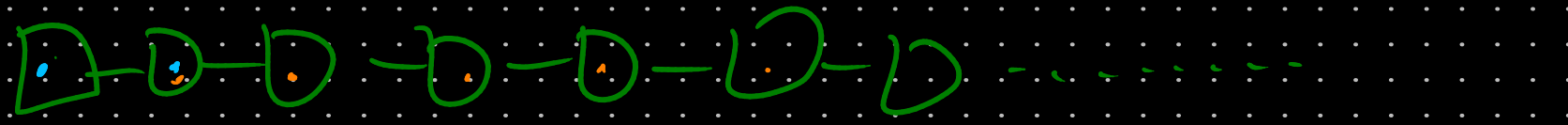
Os nós pegam as informações pra gerar os blocos

Os blocos são criado

O nonce valida

O hash válido é o endereço do novo bloco

Para adulterar a blockchain é necessário um poder computacional gigantesco



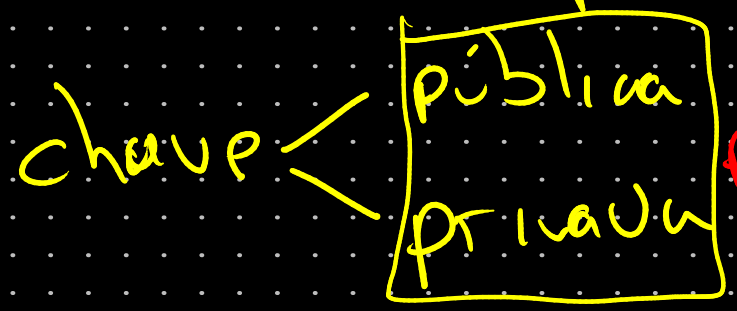
PROVA DE TRABALHO → proof of work

Criptomoeda - Bitcoin

Bitcoin não, não, não é um conjunto de bytes que por exemplo, poderia ser copiado

Chave - única e representa uma carteira simples

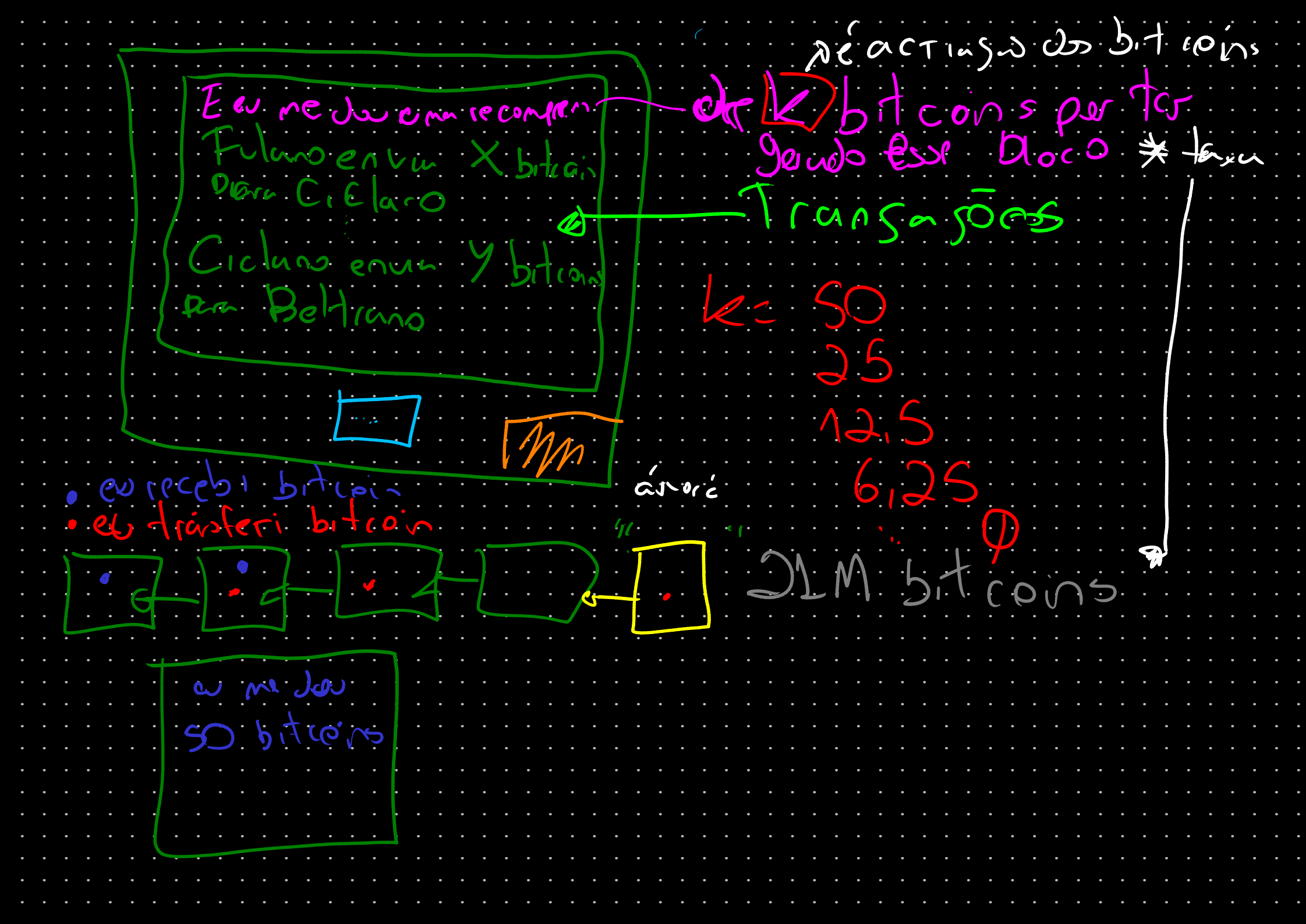
a blockchain do bitcoin é um grande livro contábil uma posição é representada na blockchain pela chave



representa

enviar bitcoin para alguém assinar com a chave privada

Criptografia de Curvas Elípticas


Reactions de bitcoins
Eu me dou uma recompensa de k bitcoins por ter gerado esse bloco
Transações
Fulano envia X bitcoin para Ciclano
Ciclano envia Y bitcoins para Beltrano
k = 50
25
12,5
6,25
0
21M bitcoins
árvore
eu recebi bitcoin
eu transferi bitcoin
eu me dou 50 bitcoins

Outros usos

- NFT → non fungible token

"Tokens" não fungíveis

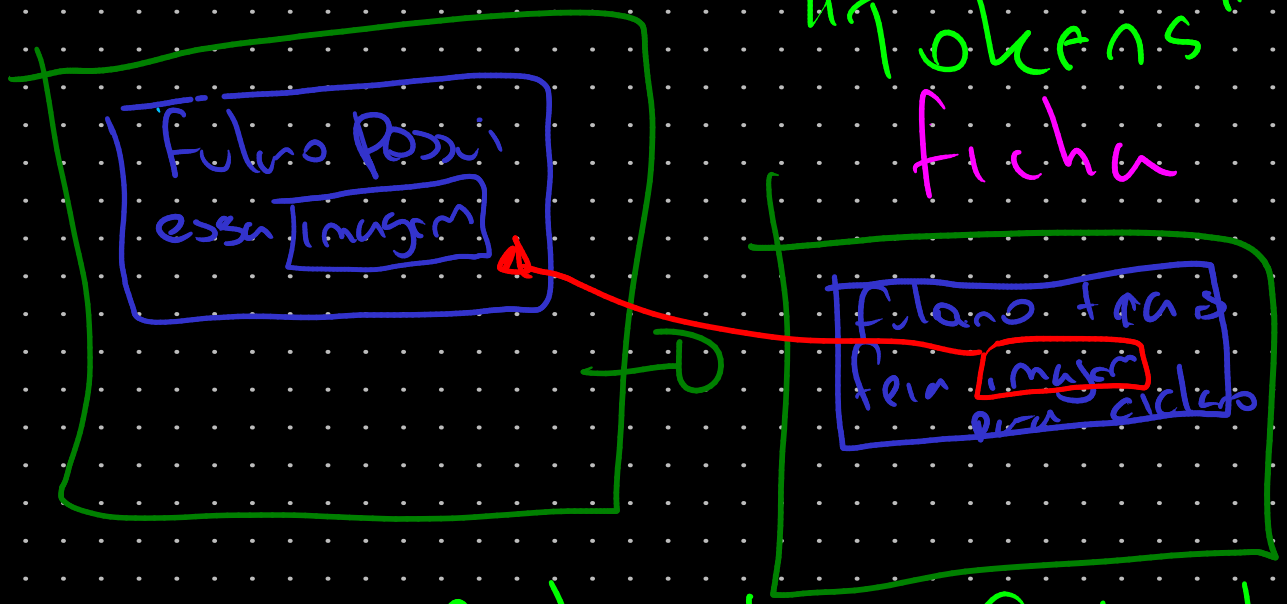


Imagem é única ou pelo menos rara

- Smart Contract = Contrato inteligente

Código executável - contratos automáticos

- Livro Contábil - Além disso?
- Rastreio de Produtos