

The background of the slide features a stylized illustration of a blockchain network. Several blocks are depicted as rounded rectangles with a blue border and a yellow base. Each block is labeled with a unique hash, such as 'Block 0x77a6b34f', 'Block 0xf9017a34', 'Block 0x37a1e556', 'Block 0x10e6c7a9', 'Block 0x13a5fc78', and 'Block 0xaf013c45'. The blocks are interconnected by dashed blue lines, representing the chain's structure. The interior of each block is filled with a pattern of binary code (0s and 1s). The overall aesthetic is digital and technological, with a dark blue background and glowing yellow and blue elements.

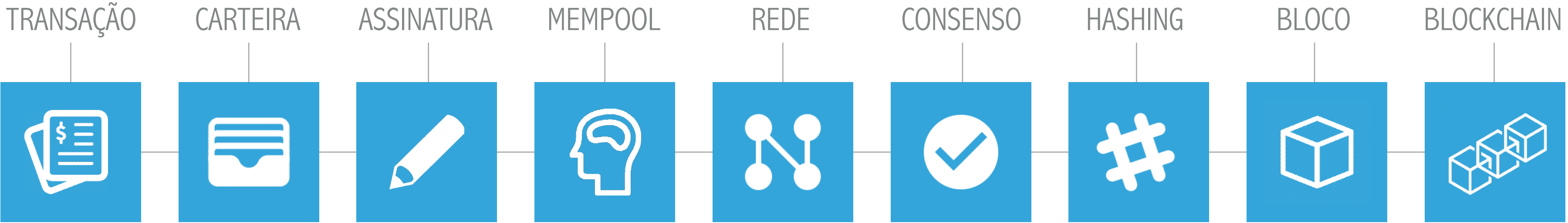
IMD0293

# ARQUITETURA DE UM BLOCKCHAIN

BLOCO

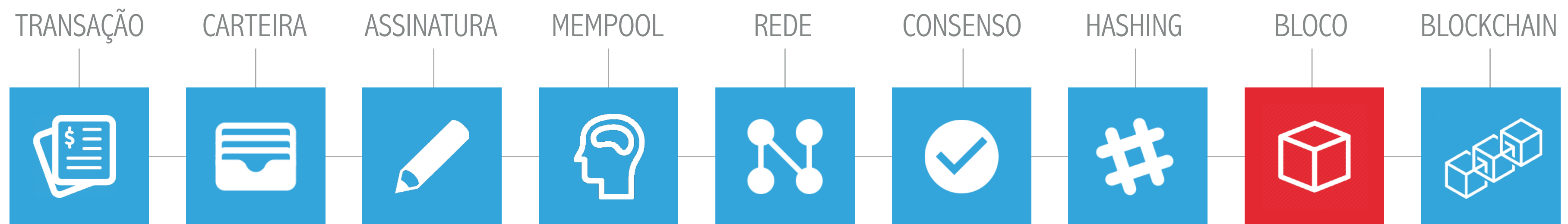


# ARQUITETURA DE UM **BLOCKCHAIN**



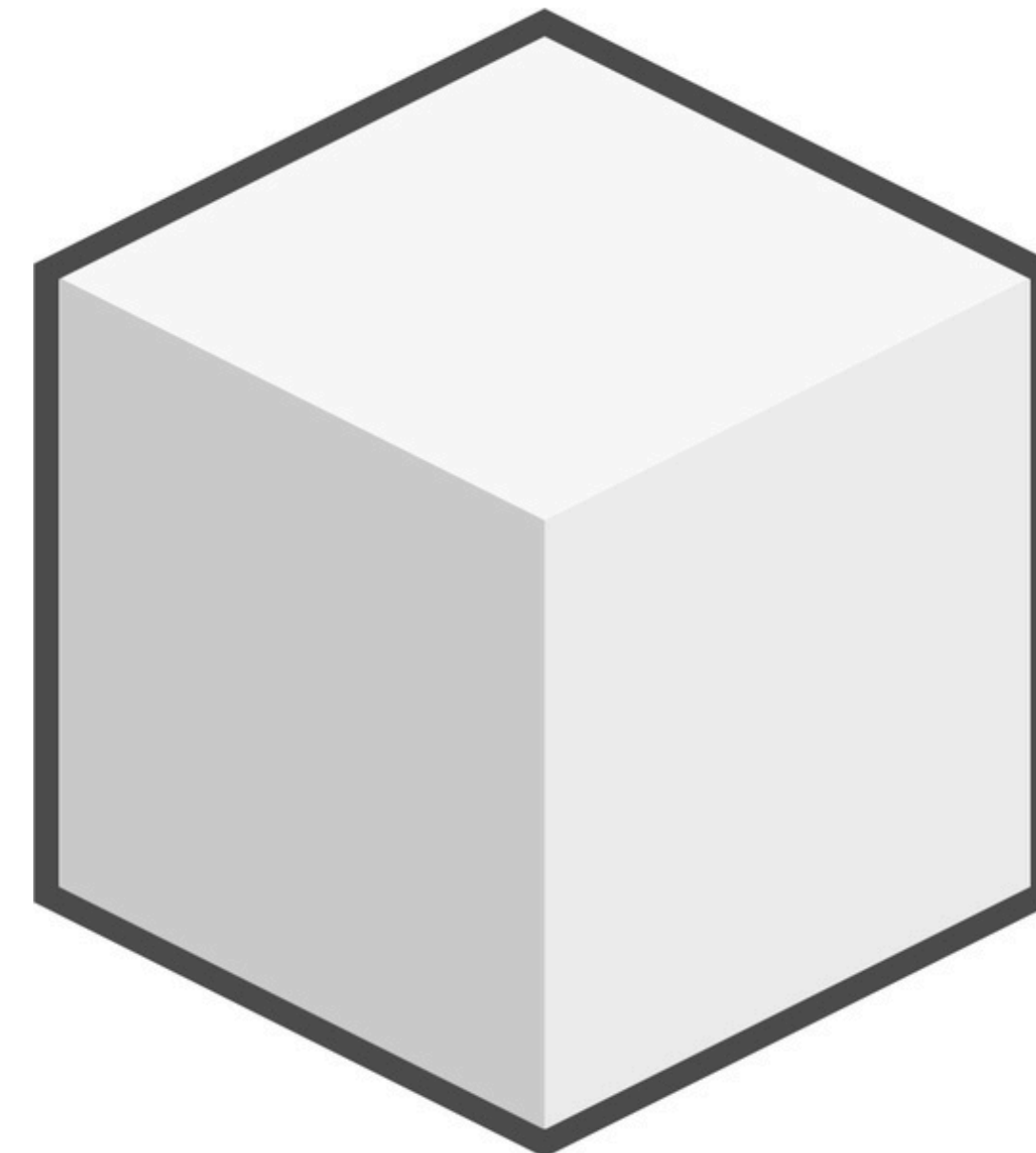
## ARQUITETURA DE UM **BLOCKCHAIN**

---



# BLOCOS

- ▶ Componente fundamental do *blockchain*
- ▶ Segmentação do *blockchain* em unidades mais elementares
- ▶ Eficiência!



## Bloco

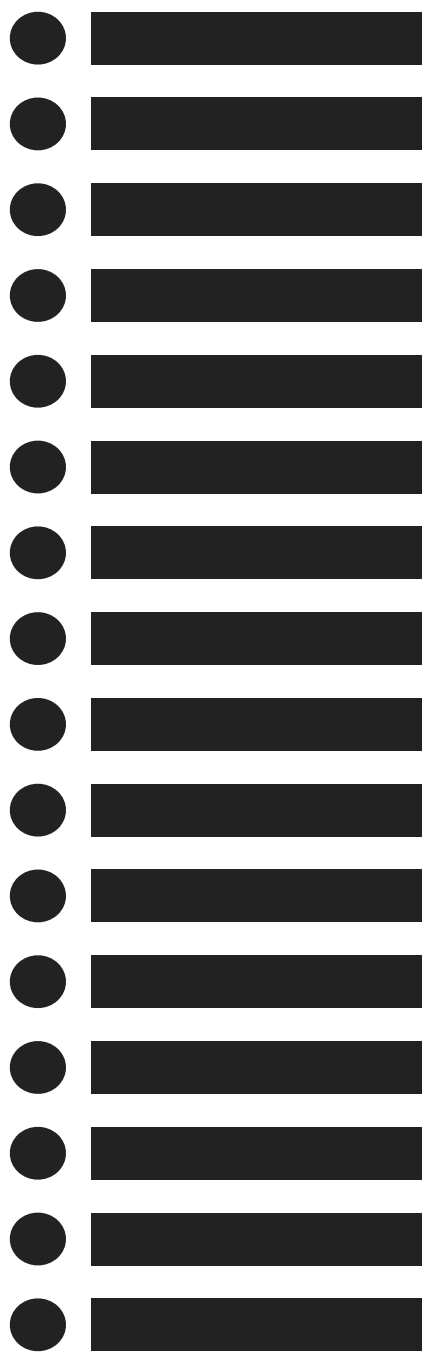
Um *container* que armazena uma lista de transações para serem adicionadas ao *blockchain*.

## Blockchain

Um livro-razão digital e compartilhado que registra uma lista de transações no formato de uma sequência de blocos.

# BLOCOS

transações



# BLOCOS

transações

- ██████████
- ██████████
- ██████████
- ██████████

- ██████████
- ██████████
- ██████████
- ██████████

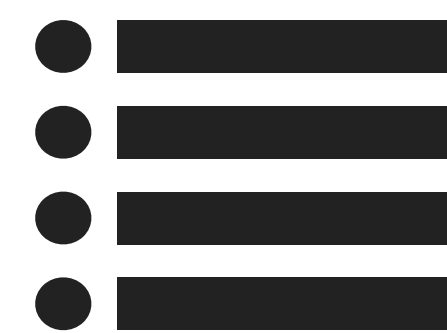
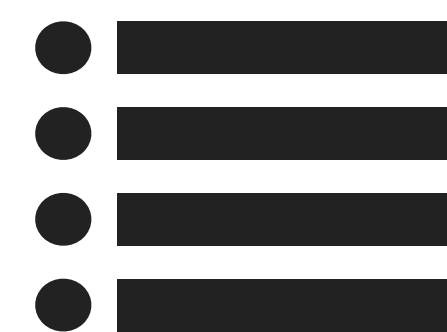
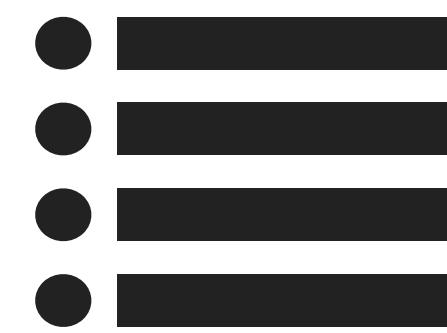
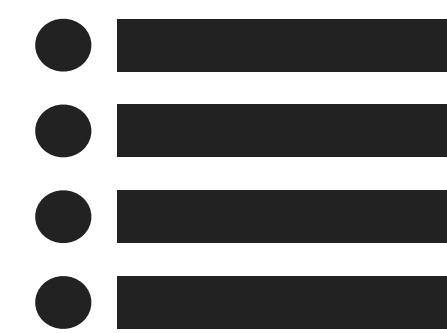
- ██████████
- ██████████
- ██████████
- ██████████

- ██████████
- ██████████
- ██████████
- ██████████

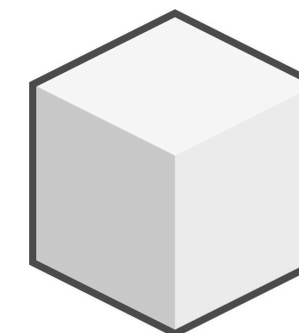
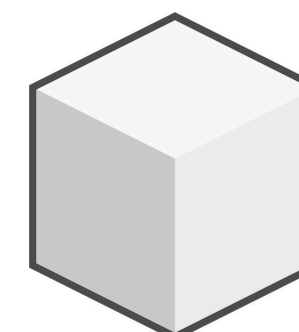
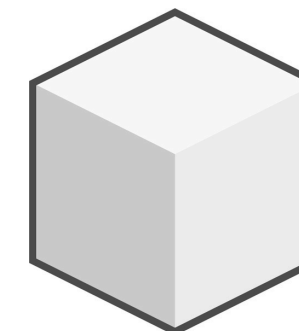
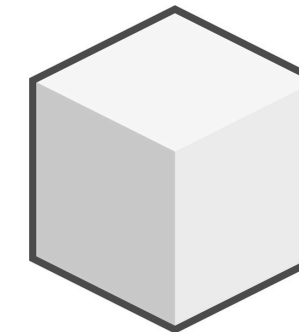


# BLOCOS

transações

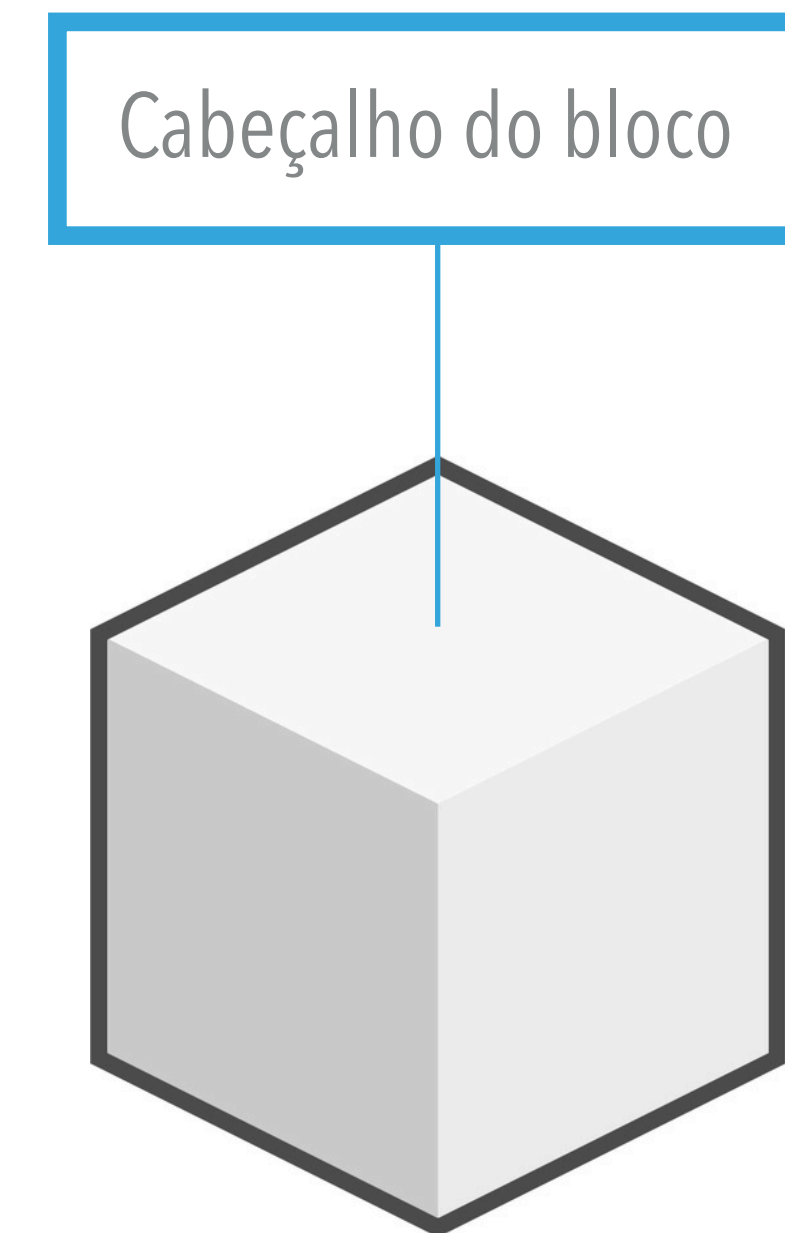


blocos



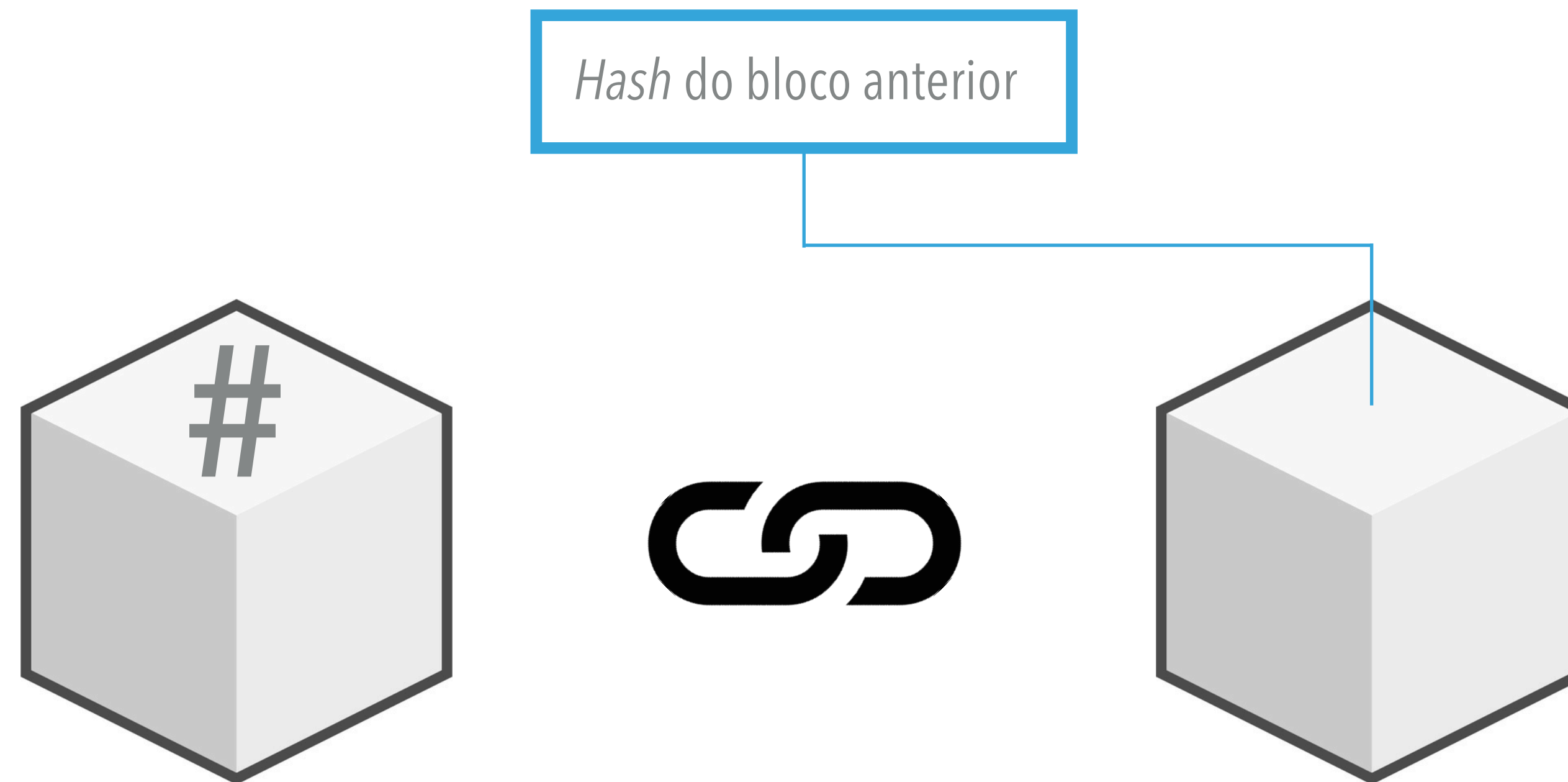
## CABEÇALHO DE UM BLOCO

- ▶ *Hash do bloco anterior (`prevBlockHash`)*
- ▶ *Timestamp*
- ▶ *Merkle Root*
- ▶ *Nonce*
- ▶ ...



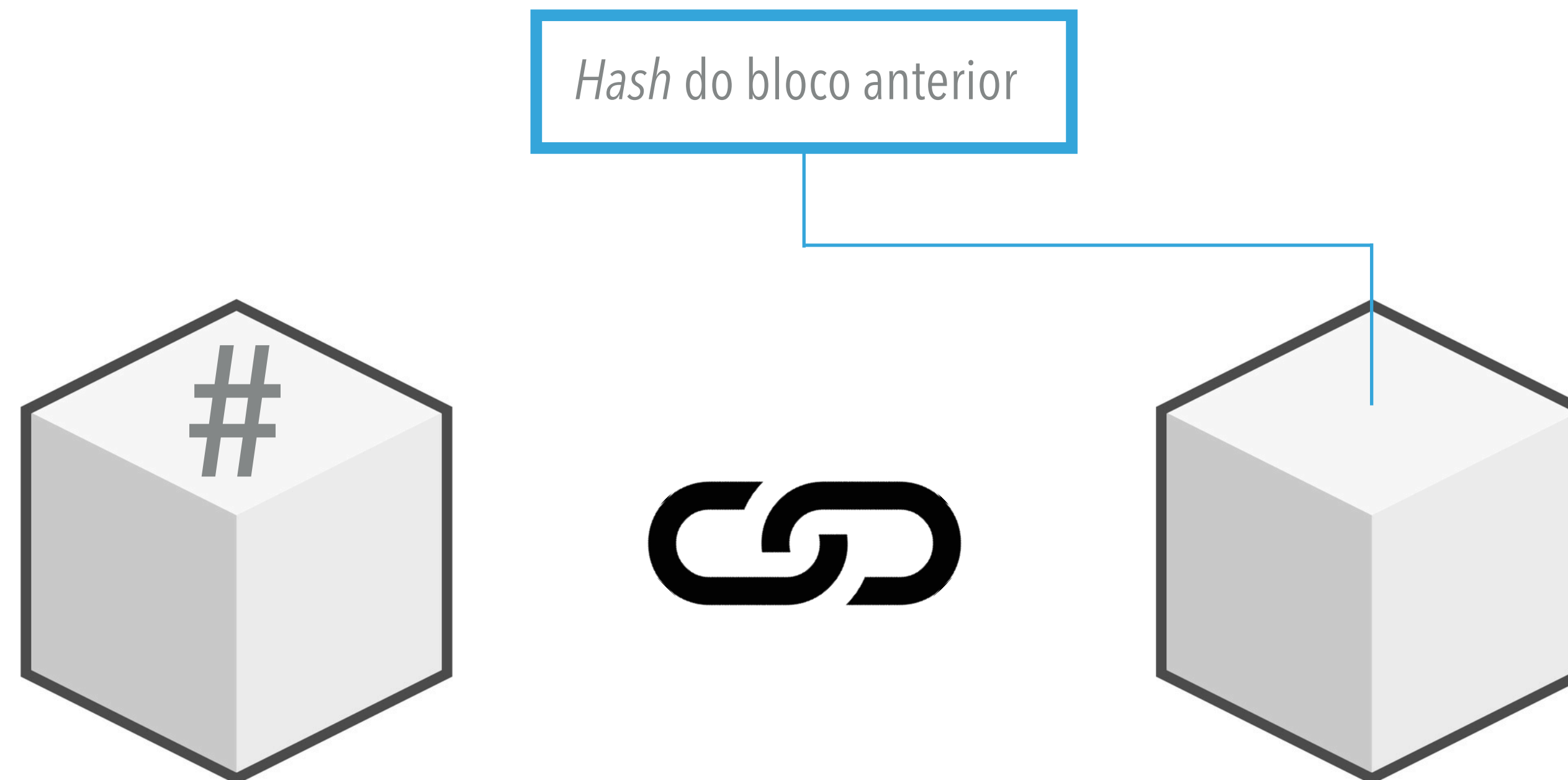


## CABEÇALHO DE UM BLOCO



$\text{blockID} = \mathbf{H(\text{blockHeader})} = H(\text{prevBlockHash} || \text{merkleRoot} || \text{time} || \text{nonce} || \dots)$

## CABEÇALHO DE UM BLOCO



Bloco 123.456 do Bitcoin:

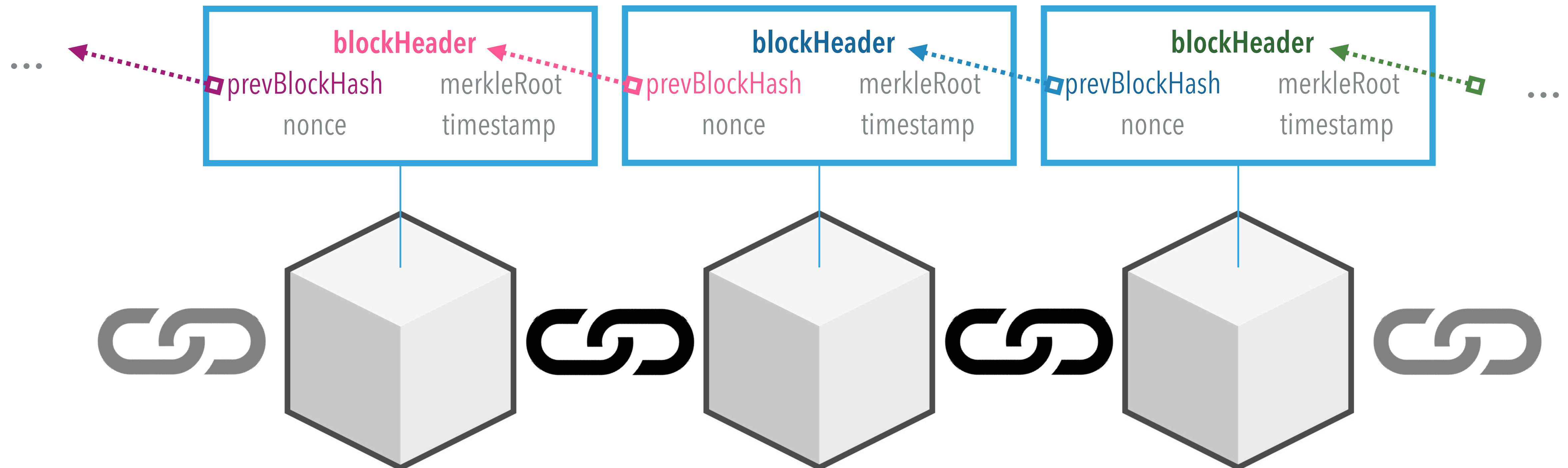
blockID = **SHA256(SHA256(** 010000009500c43a25c624520b5100adf82cb9f9da72fd2447a496bc600b000000000006cd86237 0395dedf1da2841ccda0fc489e3039de5f1ccddef0e834991a65600ea6c8cb4db3936a1ae3143991 **))**

=

0000000000002917ED80650C6174AAC8DFC46F5FE36480AAEF682FF6CD83C3CA



## CABEÇALHO DE UM BLOCO

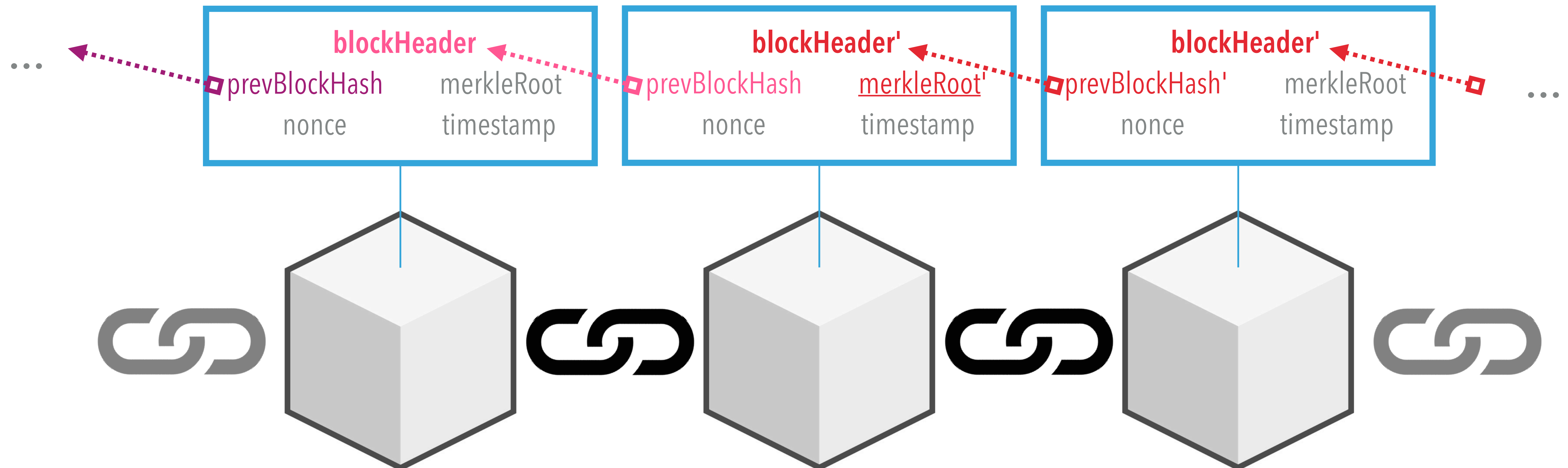


SHA256(SHA256(x))



$$\text{prevBlockHash} = H(\text{prevBlockHash} || \text{merkleRoot} || \text{time} || \text{nonce})$$

## CABEÇALHO DE UM BLOCO



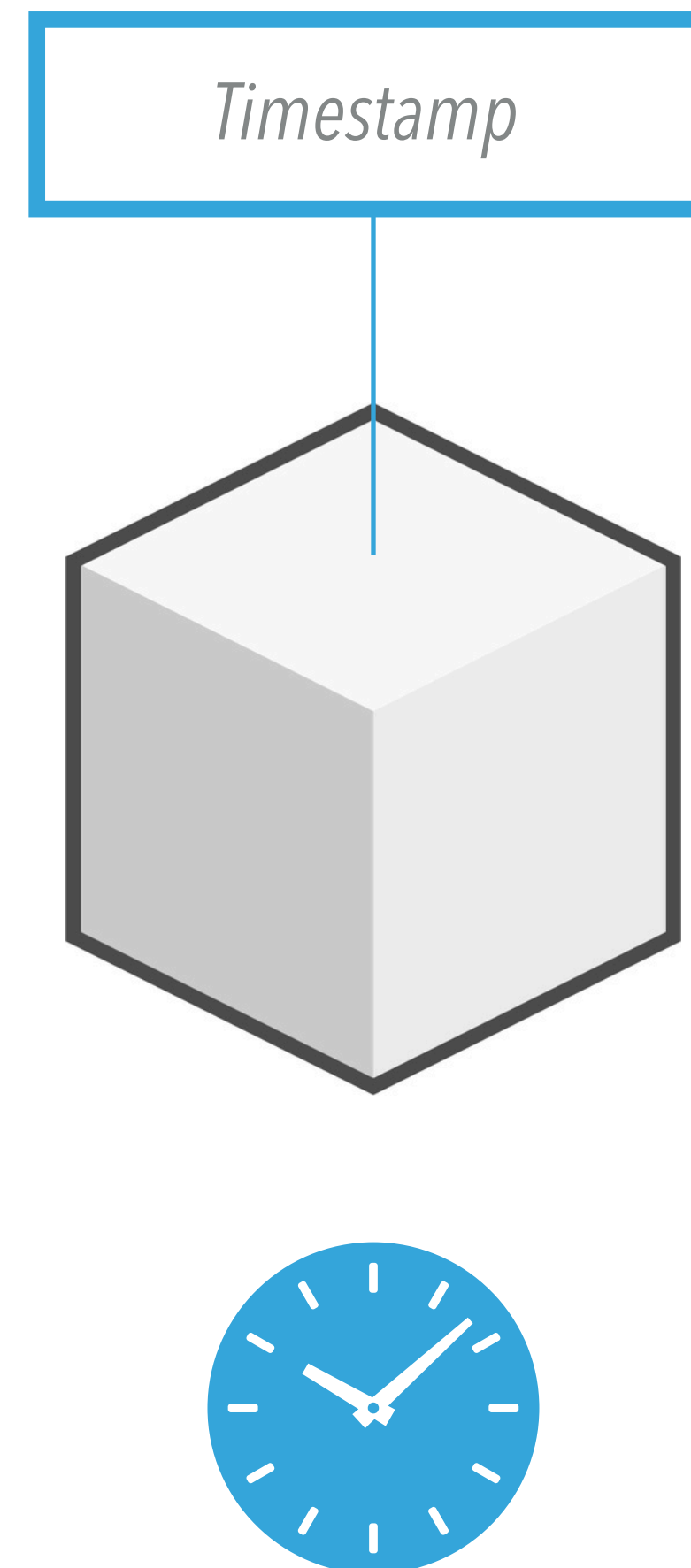
SHA256(SHA256(x))



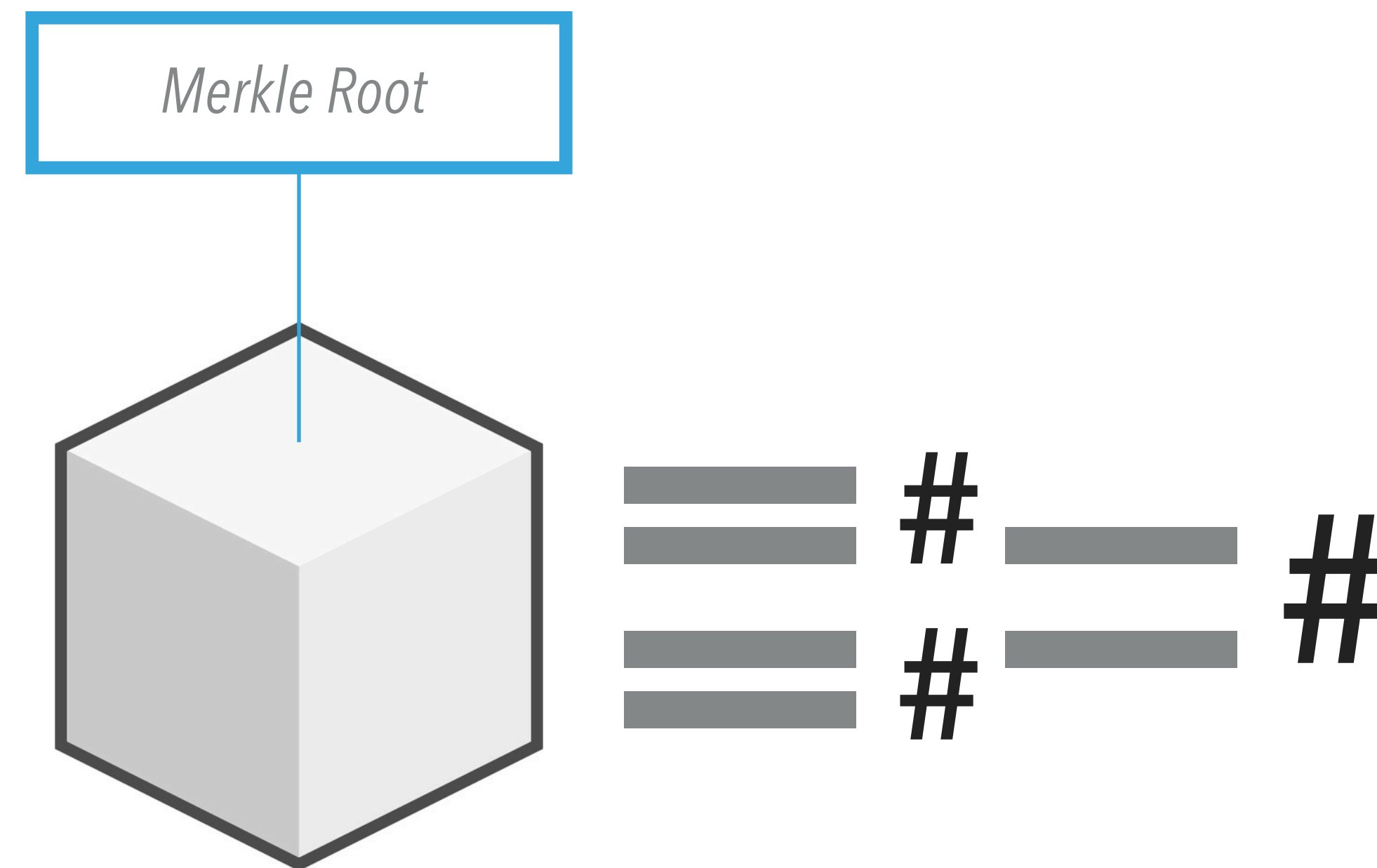
$$\text{prevBlockHash} = H(\text{prevBlockHash} || \text{merkleRoot} || \text{time} || \text{nonce})$$



# CABEÇALHO DE UM BLOCO

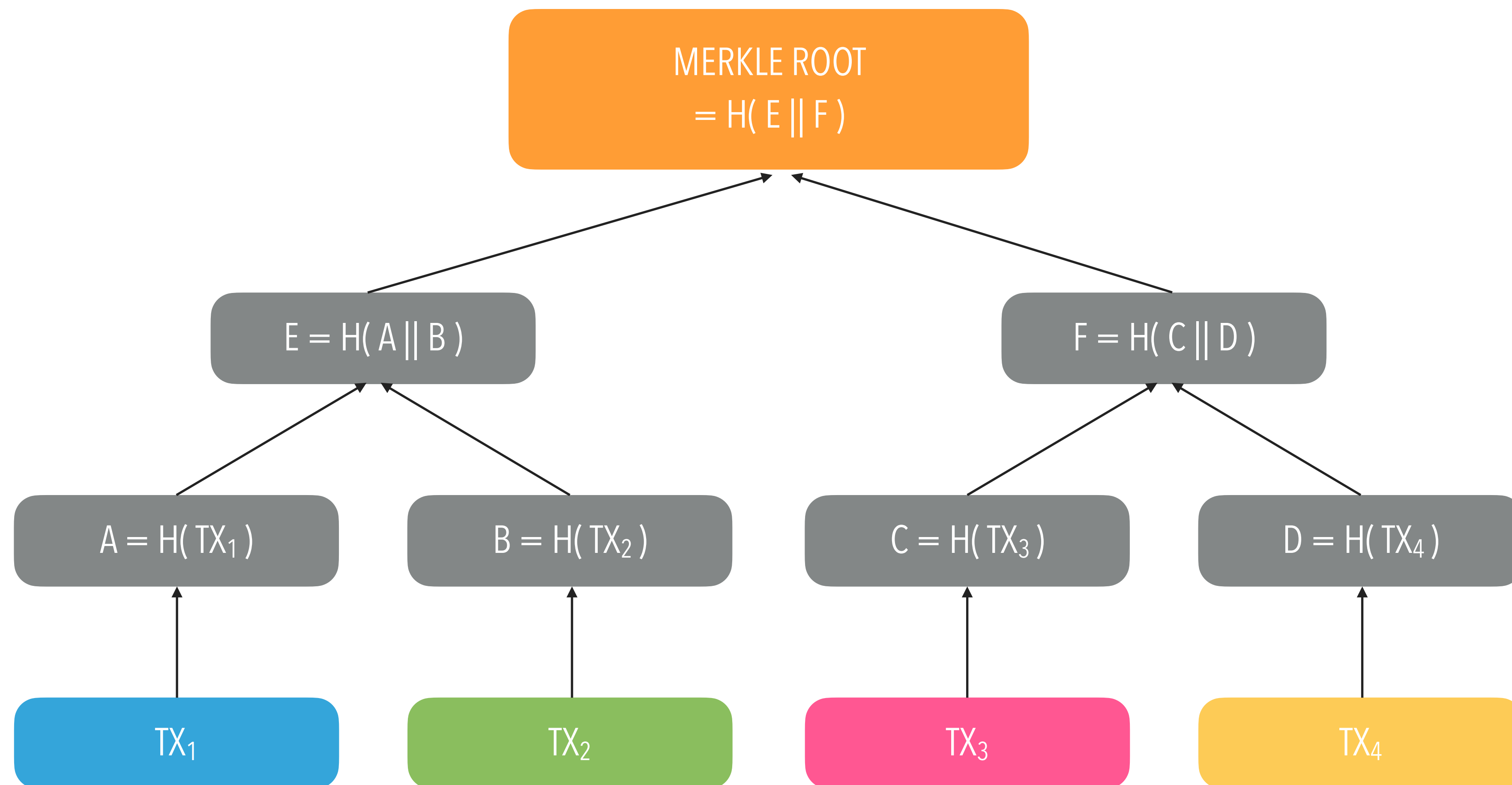


## CABEÇALHO DE UM BLOCO

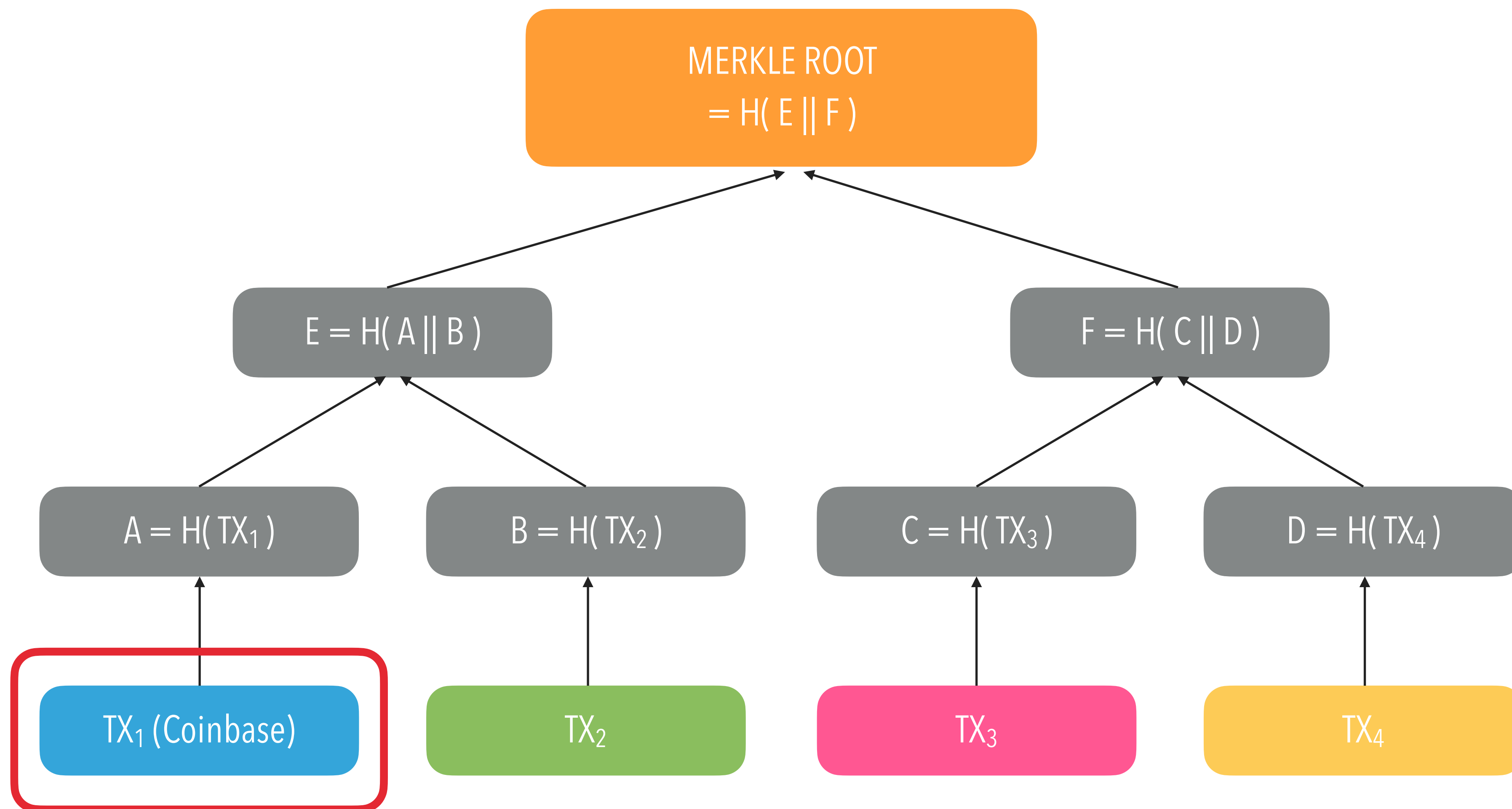




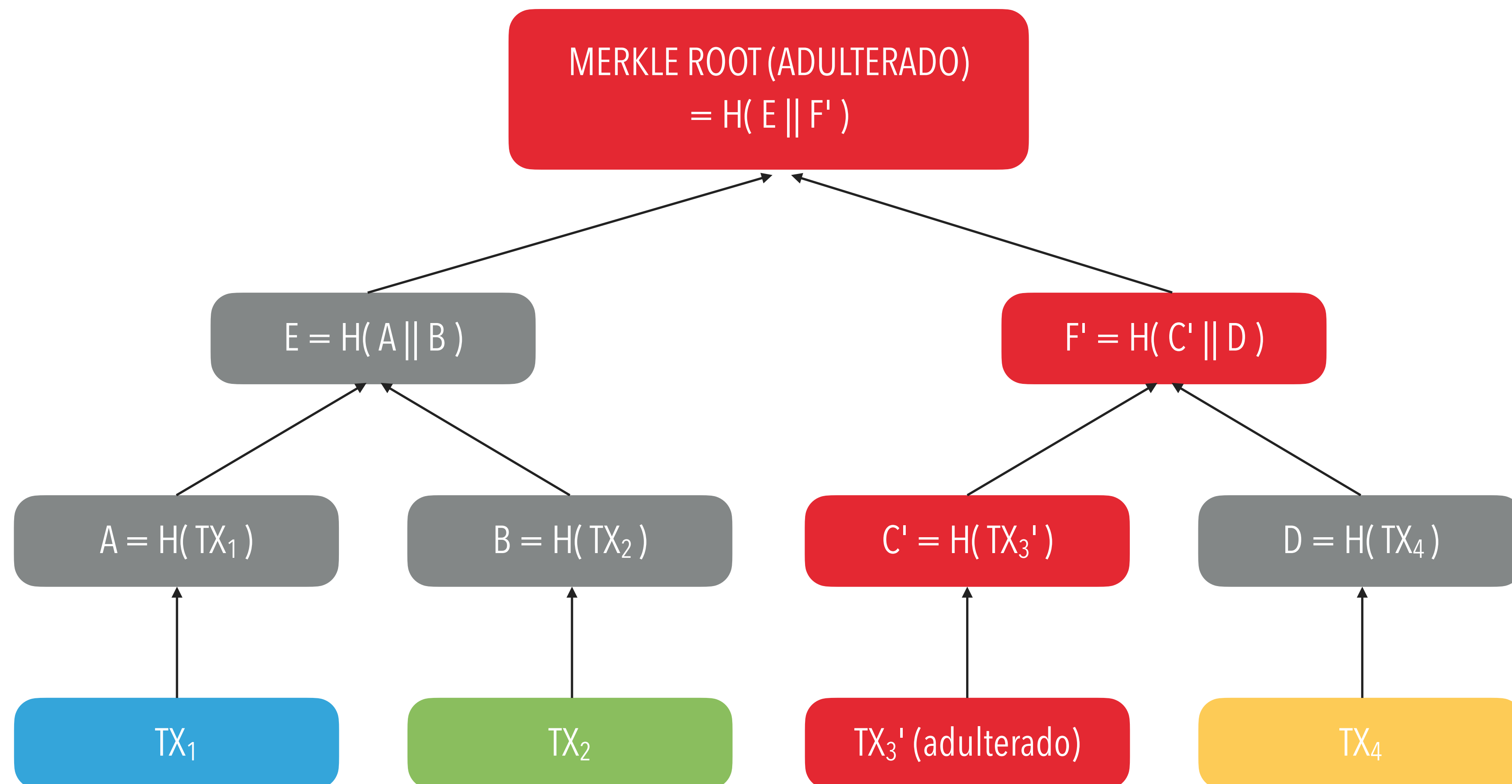
# MERKLE ROOT



# MERKLE ROOT

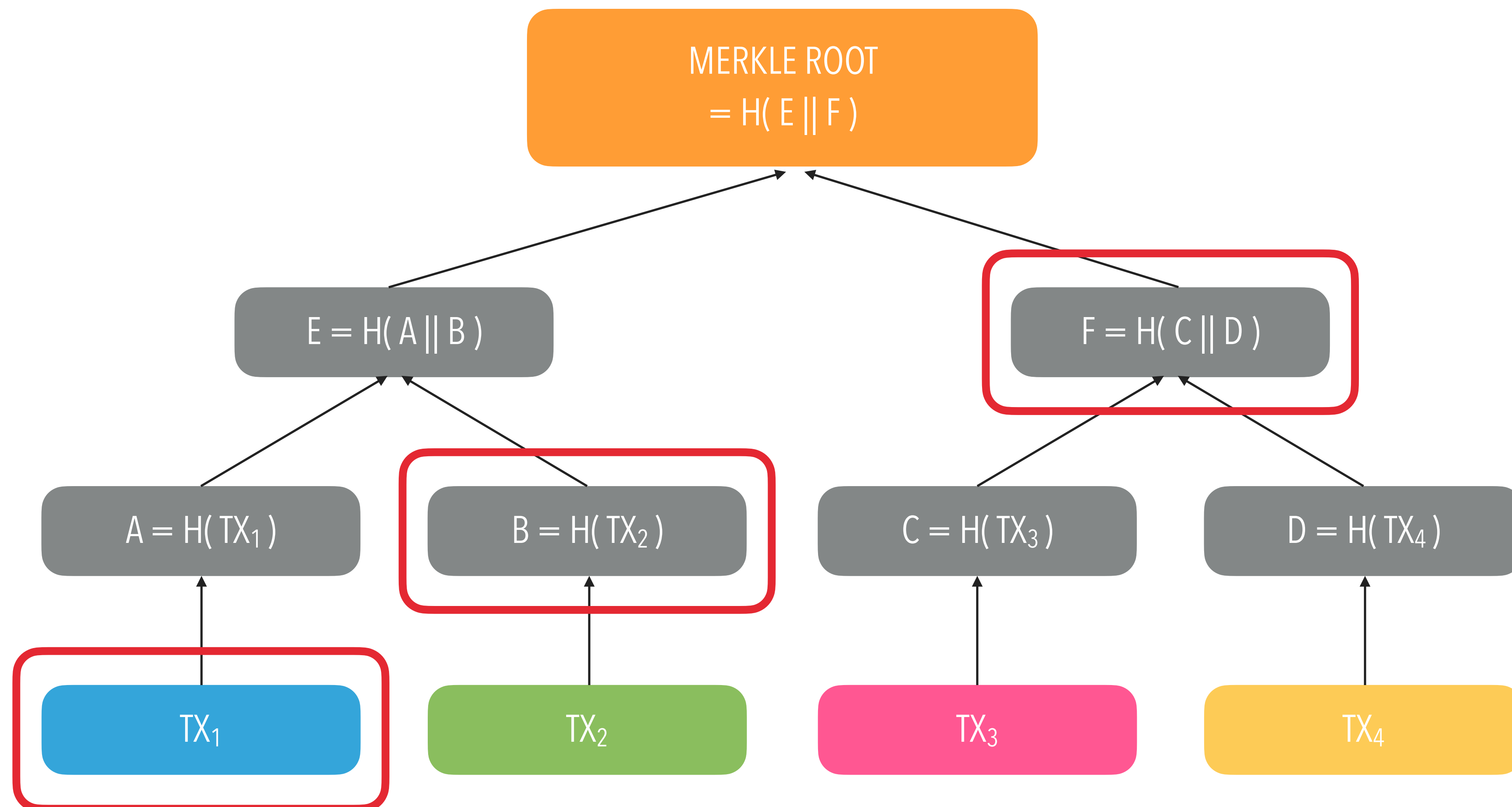


# MERKLE ROOT

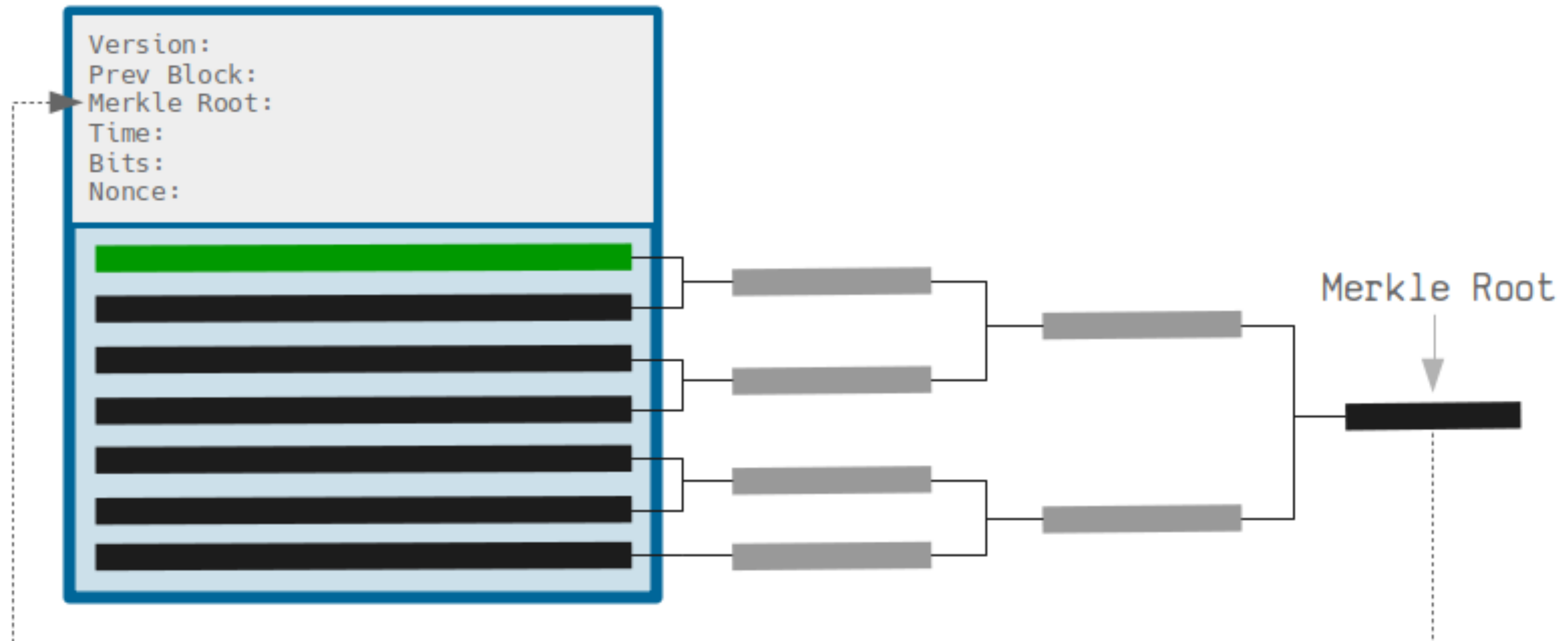


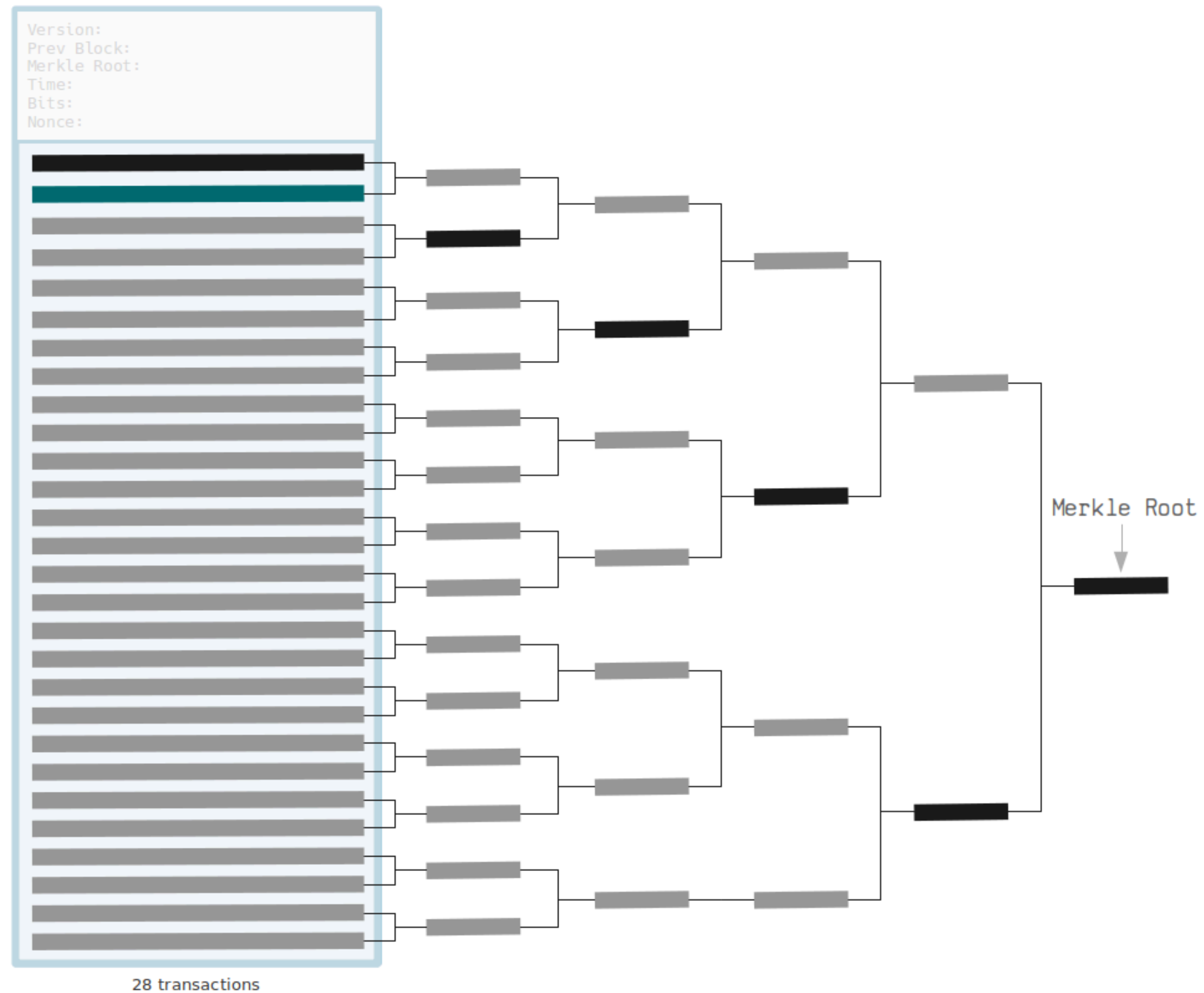


# MERKLE ROOT E PROOF-OF-INCLUSION



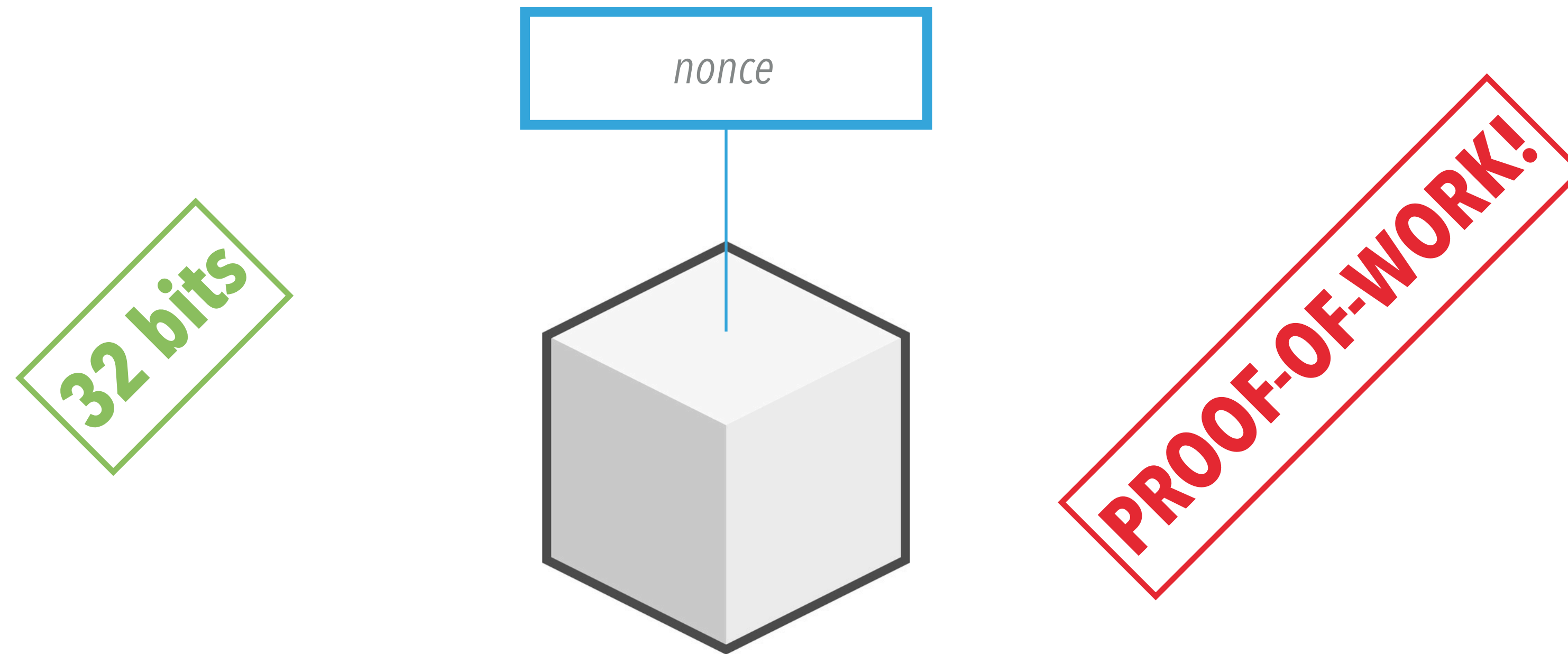
# MERKLE ROOT







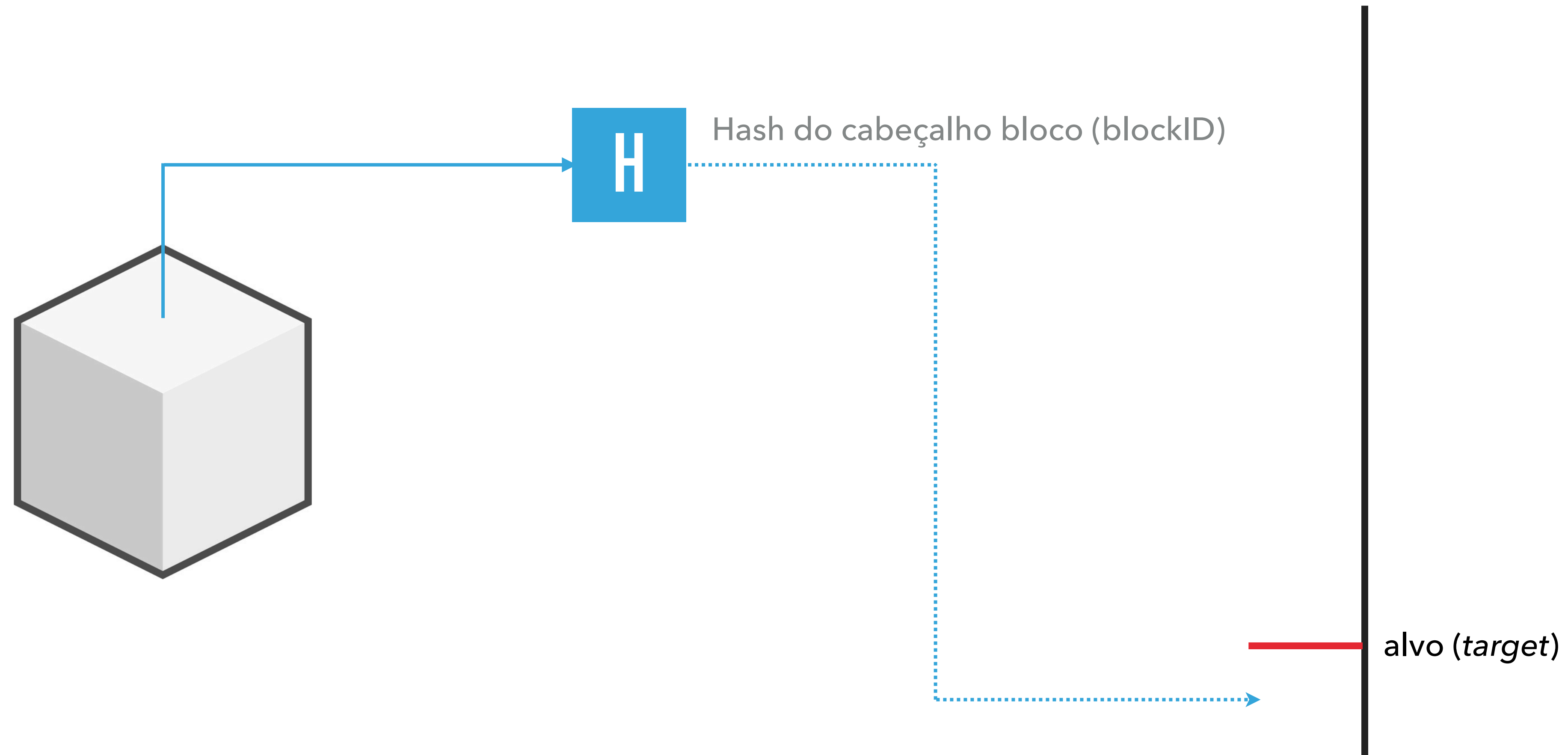
## CABEÇALHO DE UM BLOCO



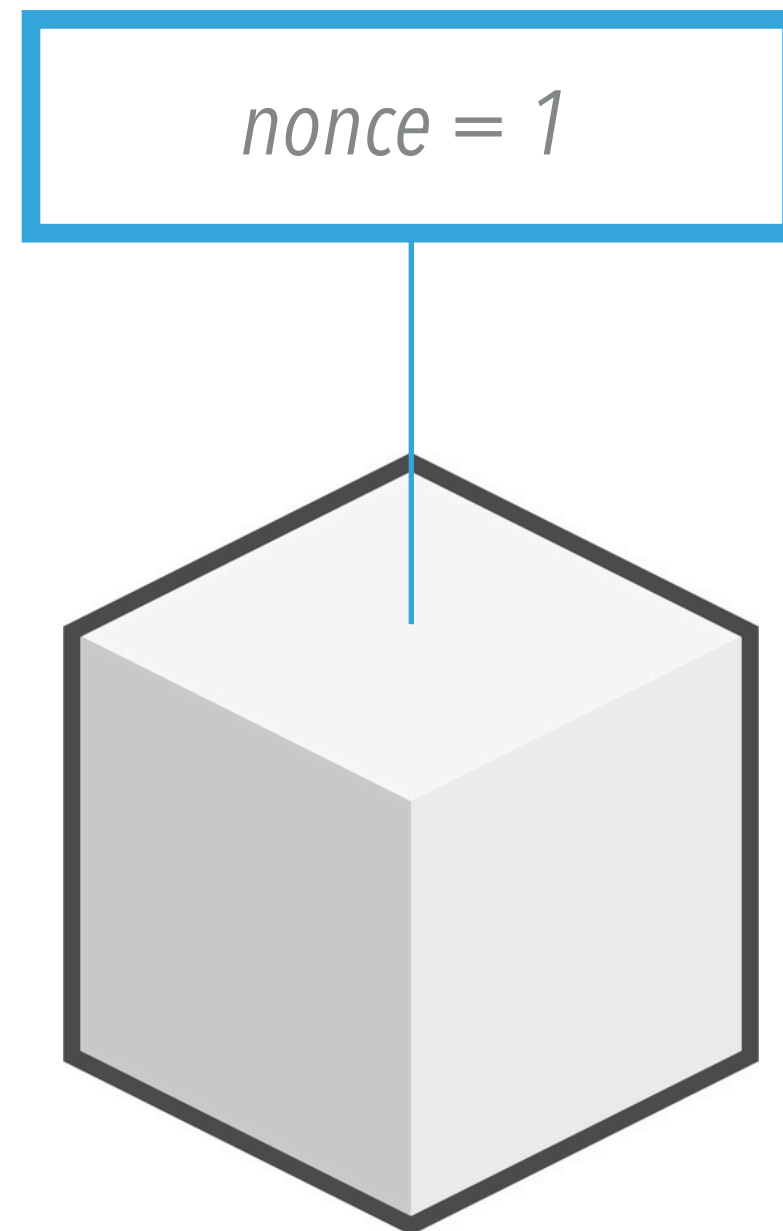
**Enigma criptográfico hash:** Encontrar um *nonce* que satisfaça a seguinte inequação:

$$H(\text{prevBlockHash} || \text{merkleRoot} || \text{time} || \text{nonce}) < \text{target}$$

## CABEÇALHO DE UM BLOCO



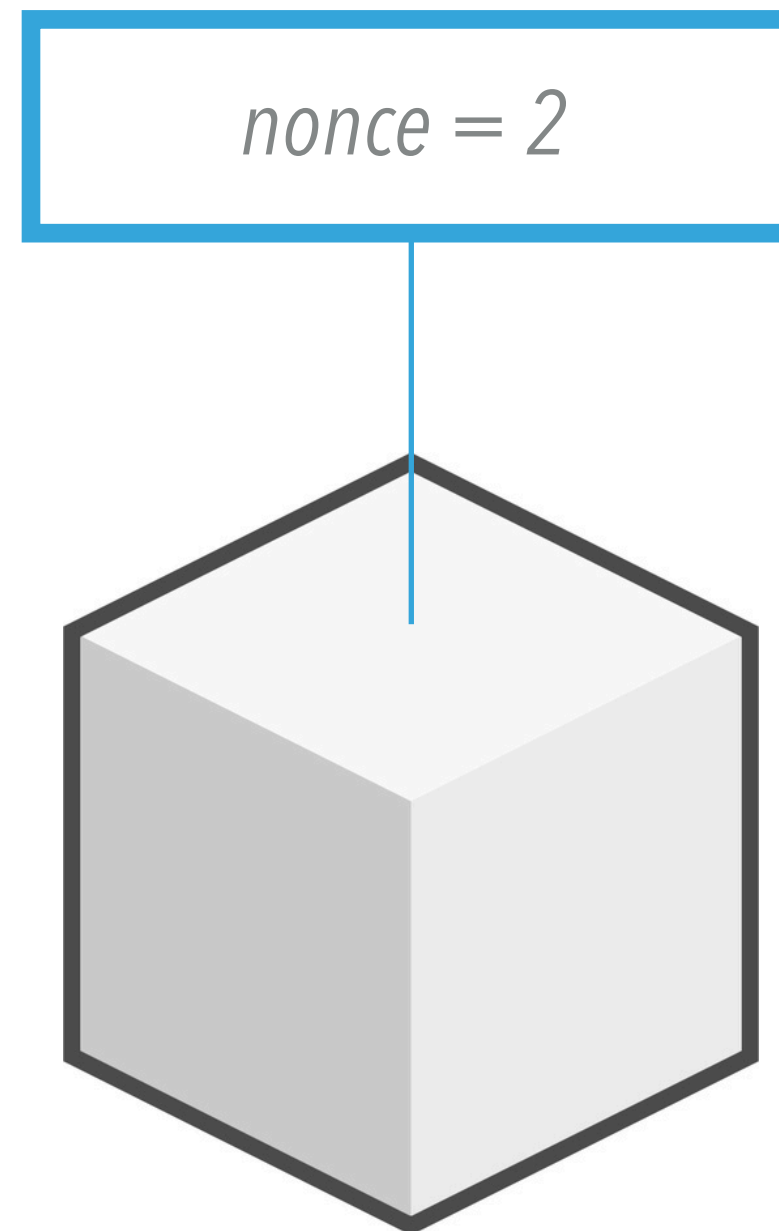
## CABEÇALHO DE UM BLOCO



4c47c2d47712cc266c3b7ed7e9a0bcda2e6786f7455b9af3e9df3c5a2b26ddbfb



## CABEÇALHO DE UM BLOCO<sub>3</sub>

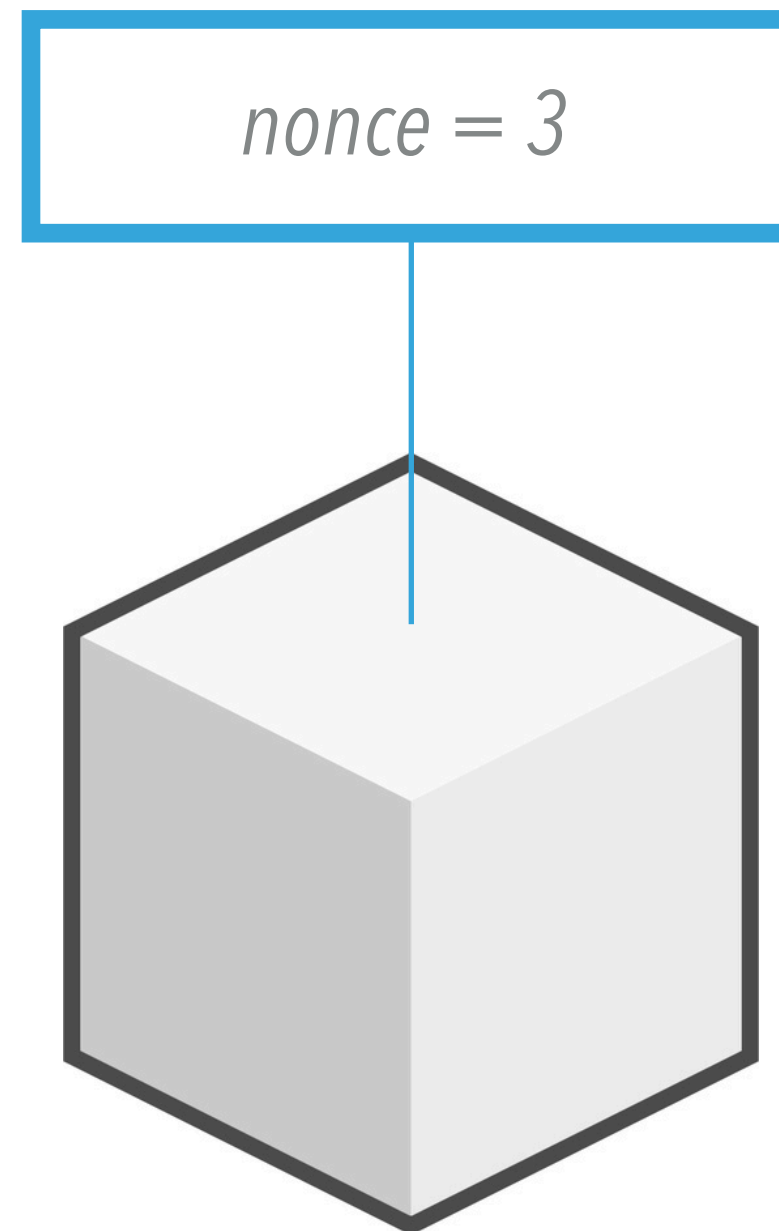


6bbe9136c059738eaf237c995a78971788ee87119d82ef640a7288b43928017





## CABEÇALHO DE UM BLOCO<sub>3</sub>

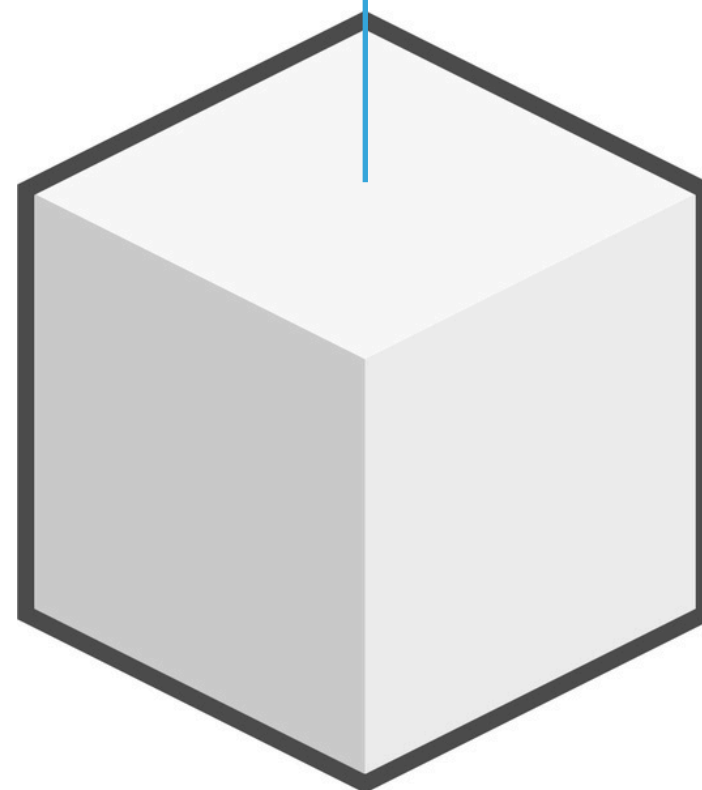


000004bb7c4d63435e1fa5595986fab643490560699bf35c43bdc6ecfd3ea721



## CABEÇALHO DE UM BLOCO

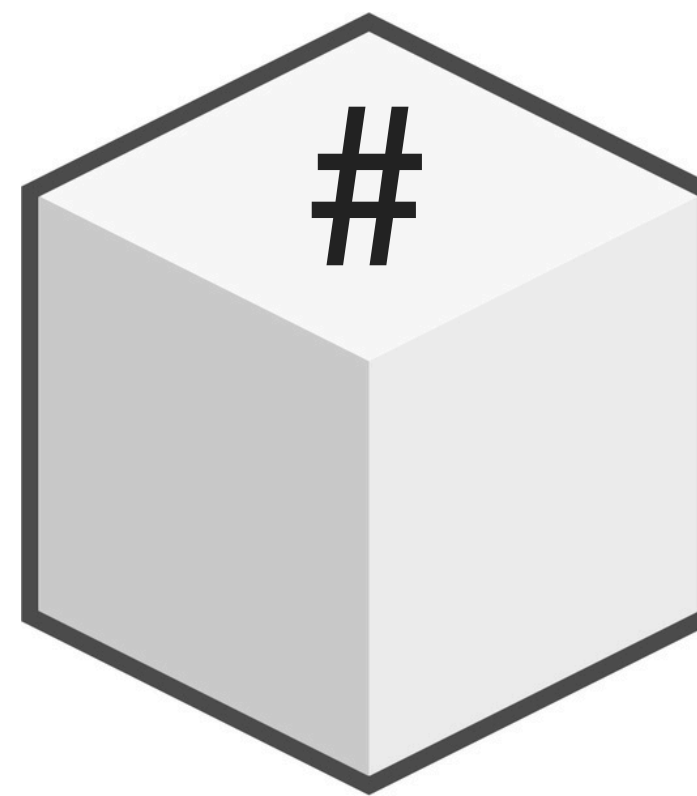
*nonce = 1.619.820.810*



00000000000000000274cb1a04c382475310f70cee3776af06414f22f8337044



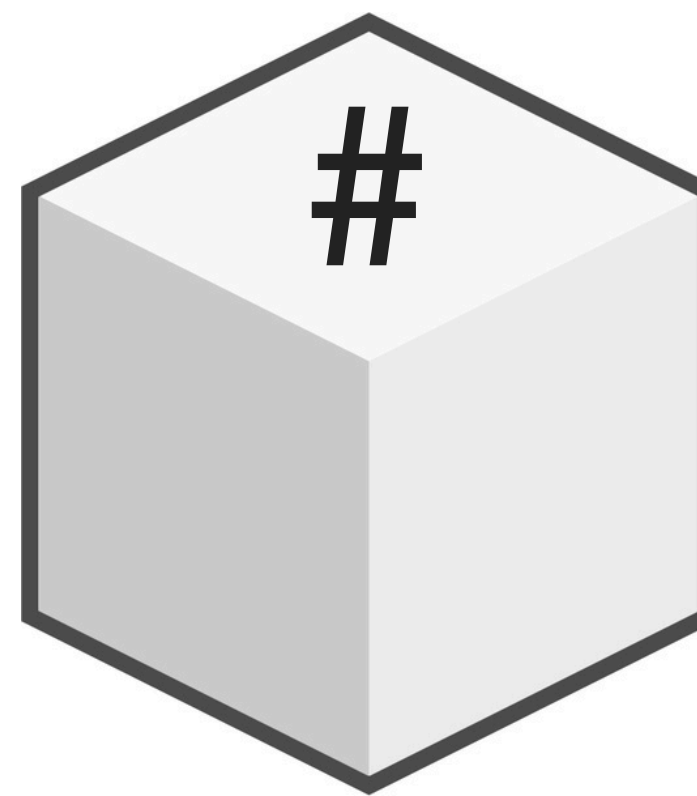
## DIFICULDADE DE UM BLOCO



**Dificuldade do bloco:**

000000HASHVALUE

## DIFICULDADE DE UM BLOCO

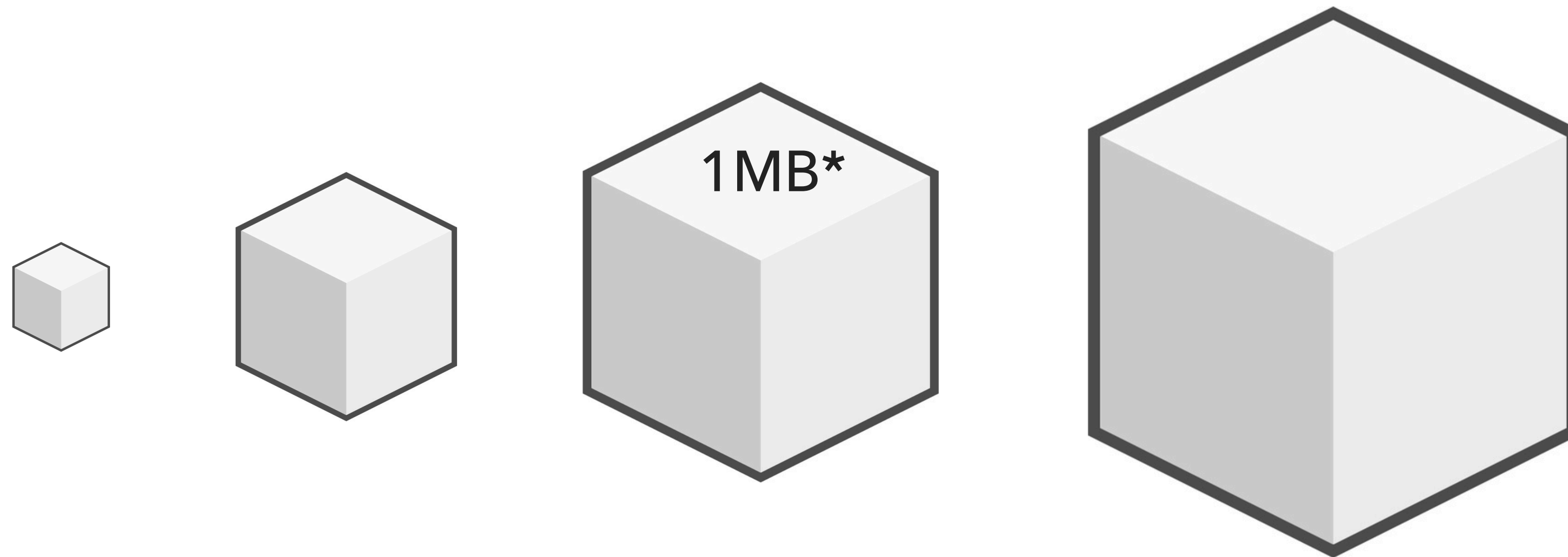


**Dificuldade do bloco:**

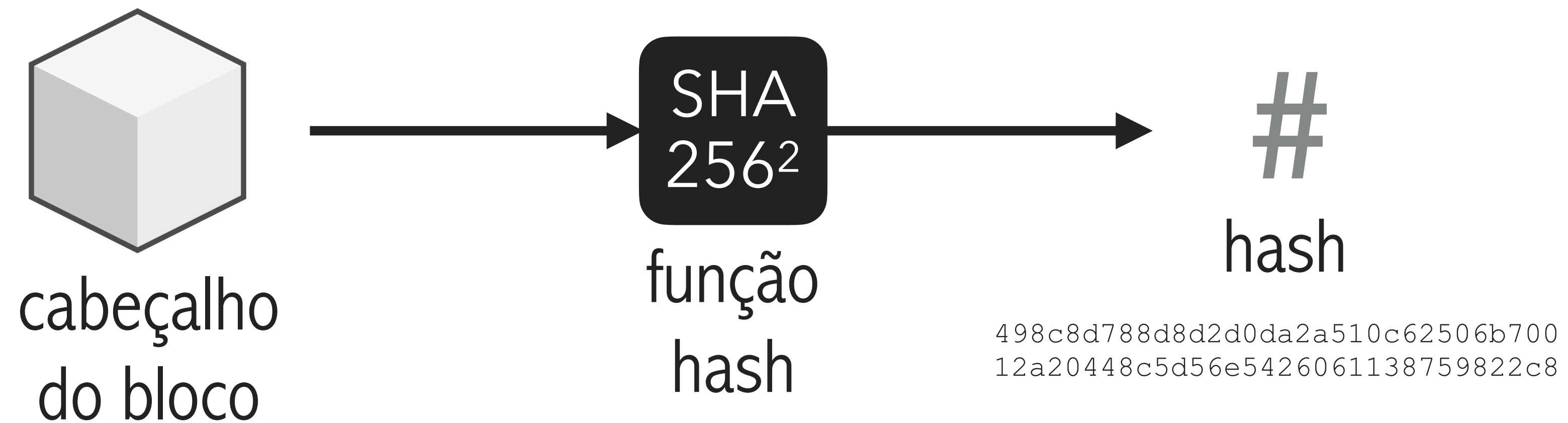
0000000HASHVALUE



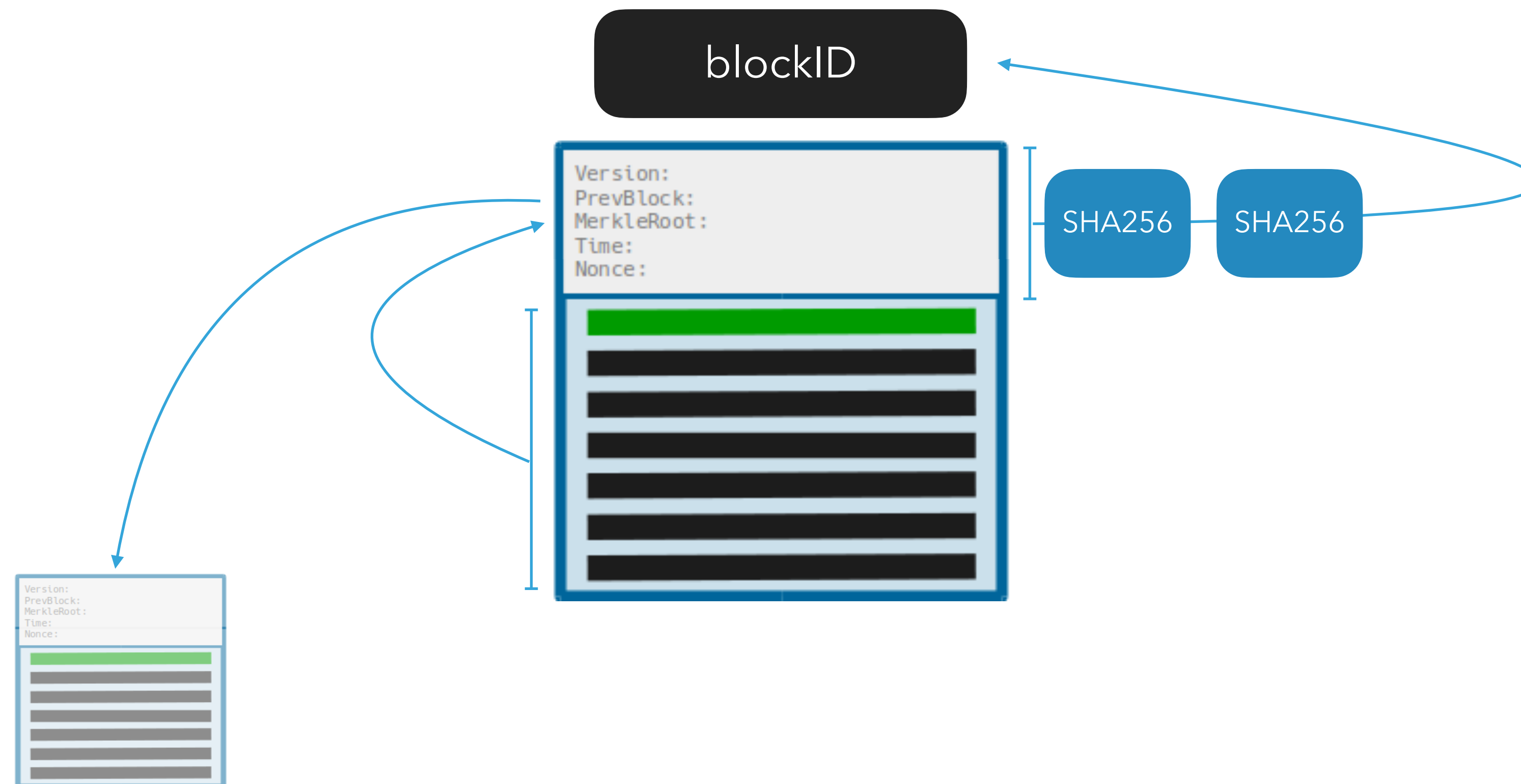
## TAMANHO DE UM BLOCO (BITCOIN)



## HASH DE UM BLOCO



# ID DE UM BLOCO





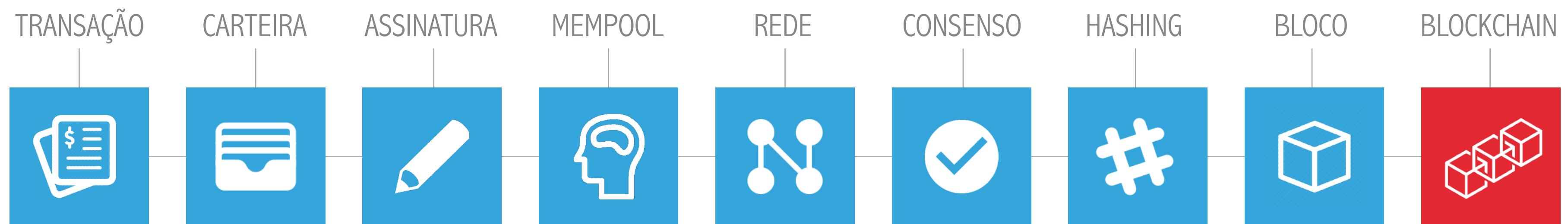
## BLOCO – DEMO

<https://andersbrownworth.com/blockchain/block>



## ARQUITETURA DE UM **BLOCKCHAIN**

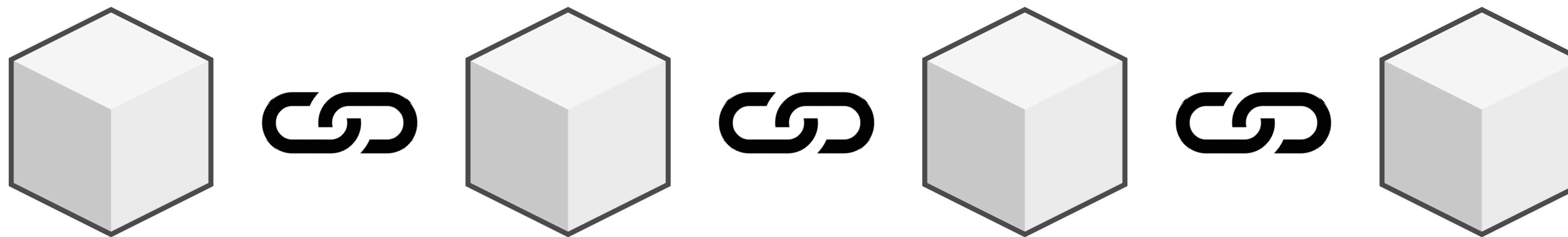
---



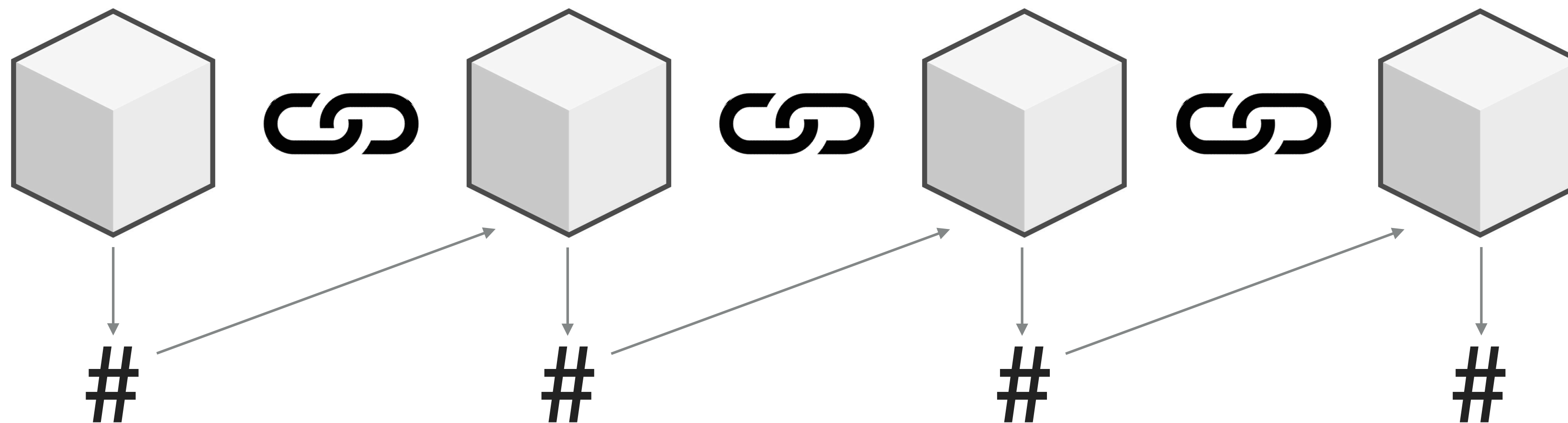
## Blockchain

Um livro-razão digital e compartilhado que registra um histórico de transações feitas na rede.

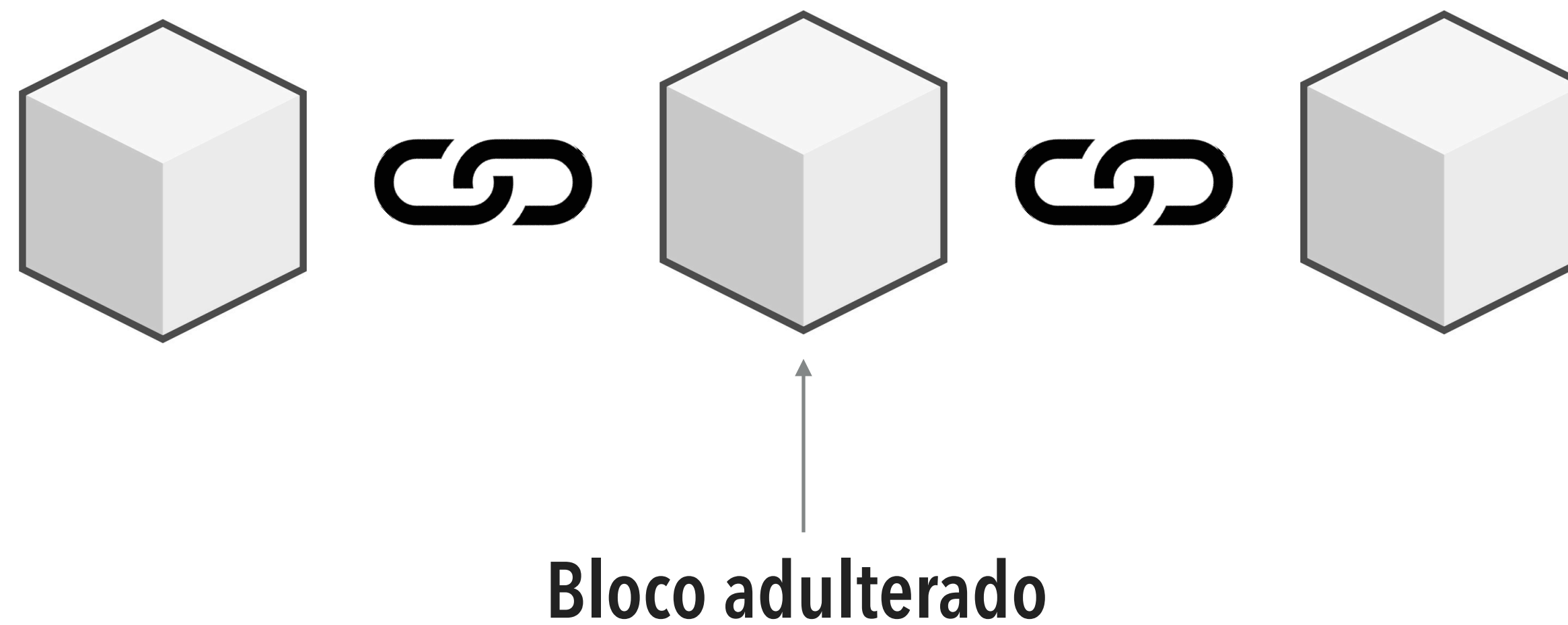
## CORRENTE DE BLOCOS



## CORRENTE DE BLOCOS

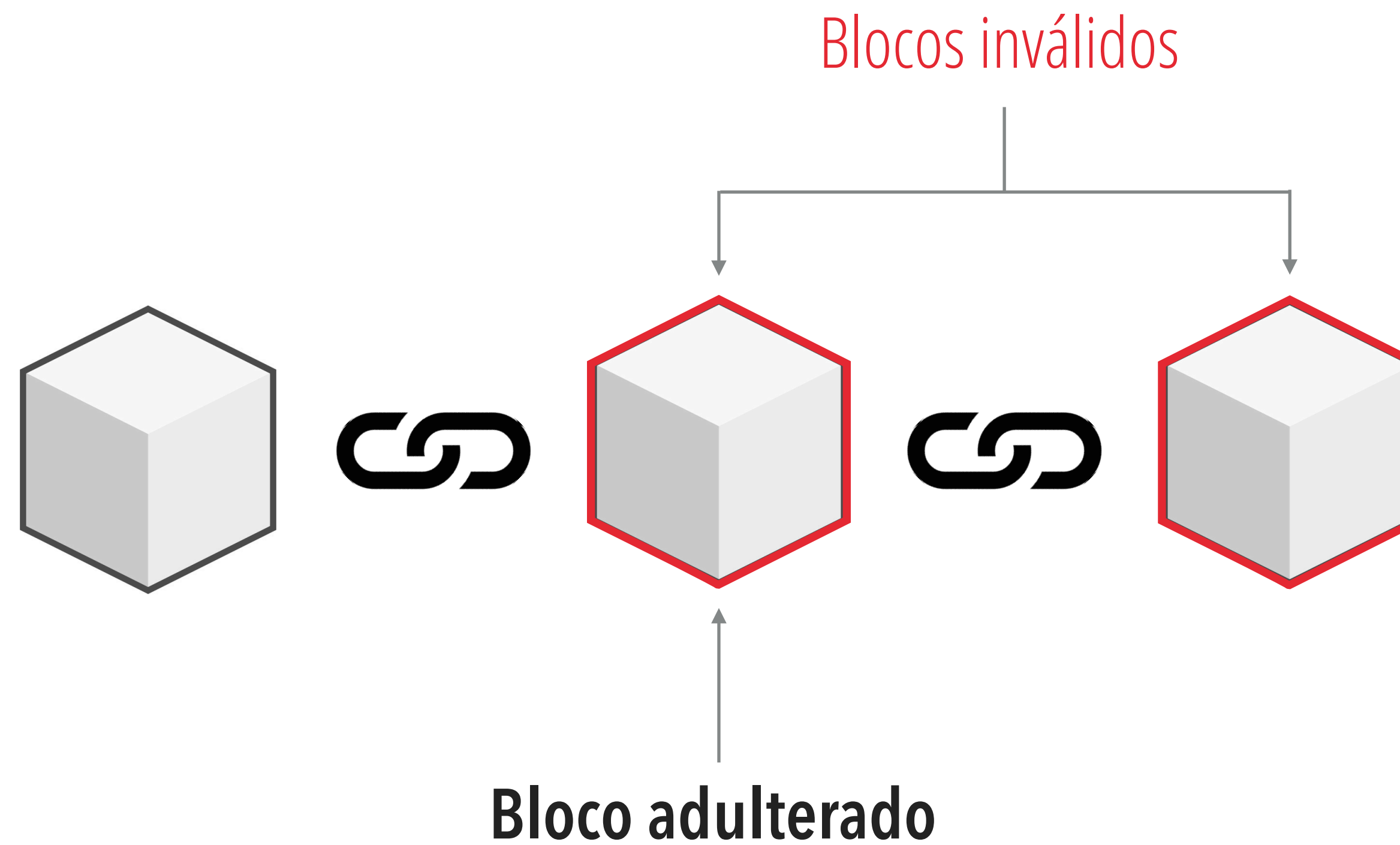


## CORRENTE DE BLOCOS

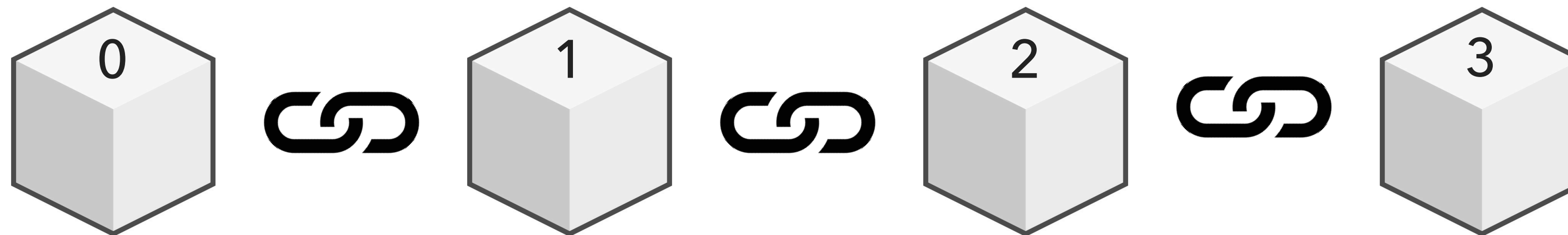




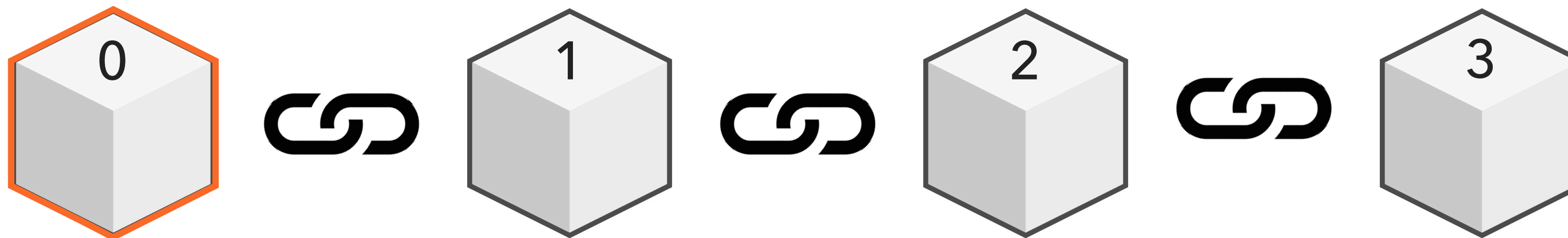
## CORRENTE DE BLOCOS



## NÚMERO DO BLOCO

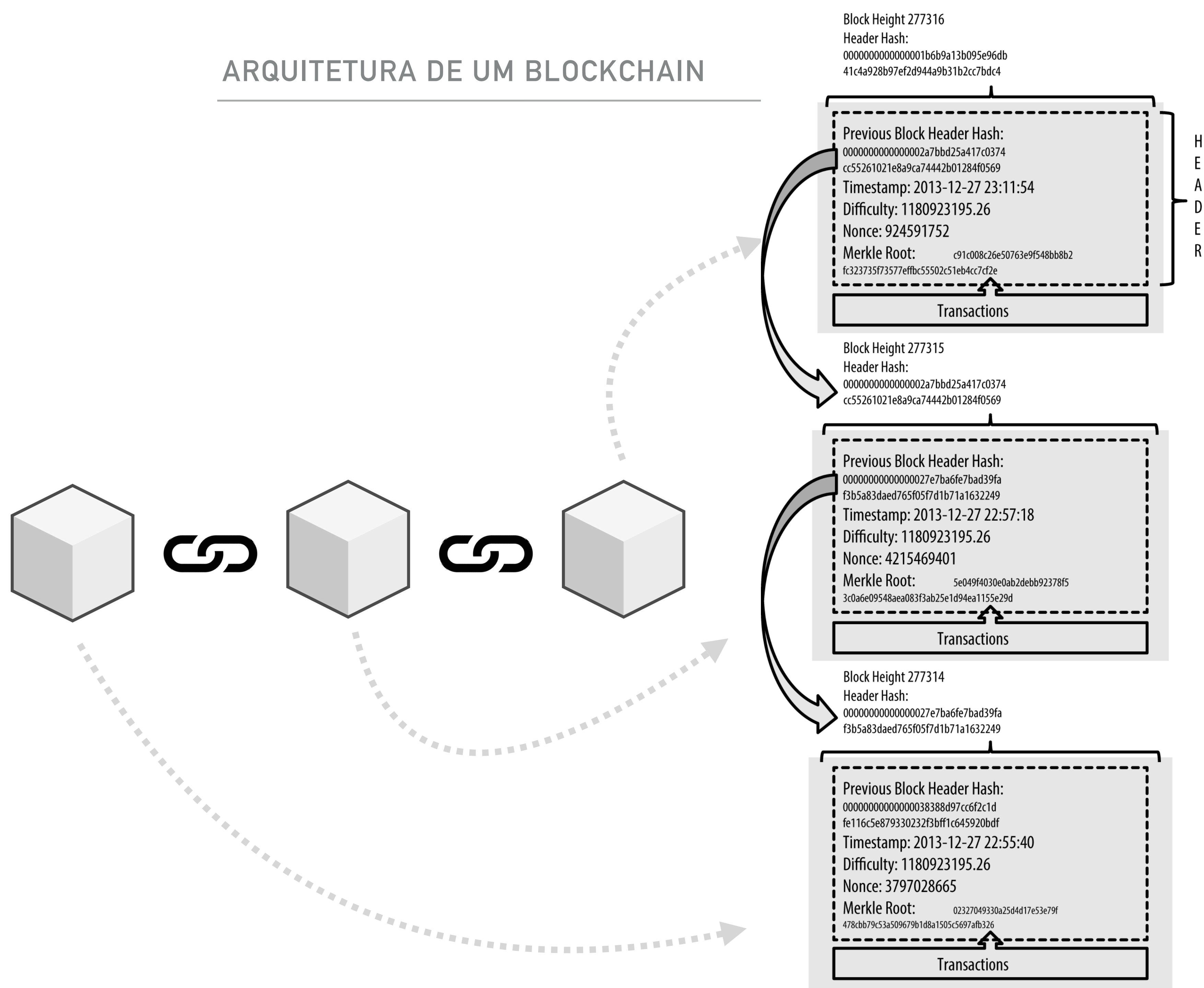


# BLOCO GÊNESIS



# ARQUITETURA DE UM BLOCKCHAIN

PROF. DANILO CURVELO



# BLOCKCHAIN – DEMO

<https://andersbrownworth.com/blockchain/blockchain>



[illegible]



# BLOCOS EM PYTHON

```
block = {
    'index': 2,
    'timestamp': 1506057125,
    'nonce': 324984,
    'merkleRoot': "13c8bbf1dde38d5f86bfc48a5c027df0d8eb19c8a647de49976755e1b35b31ca",
    'previousHash': "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824",
    'transactions': [
        {
            'sender': "8527147fe1f5426f9dd545de4b27ee00",
            'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
            'amount': 500000,
        }
    ]
}
```

```
block_header = {
    'index': 2,
    'timestamp': 1506057125,
    'nonce': 324984,
    'merkleRoot': "13c8bbf1dde38d5f86bfc48a5c027df0d8eb19c8a647de49976755e1b35b31ca",
    'previousHash': "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
}
```

# ATIVIDADE: BLOCOS

GitHub Classroom

`./02-blocks/`