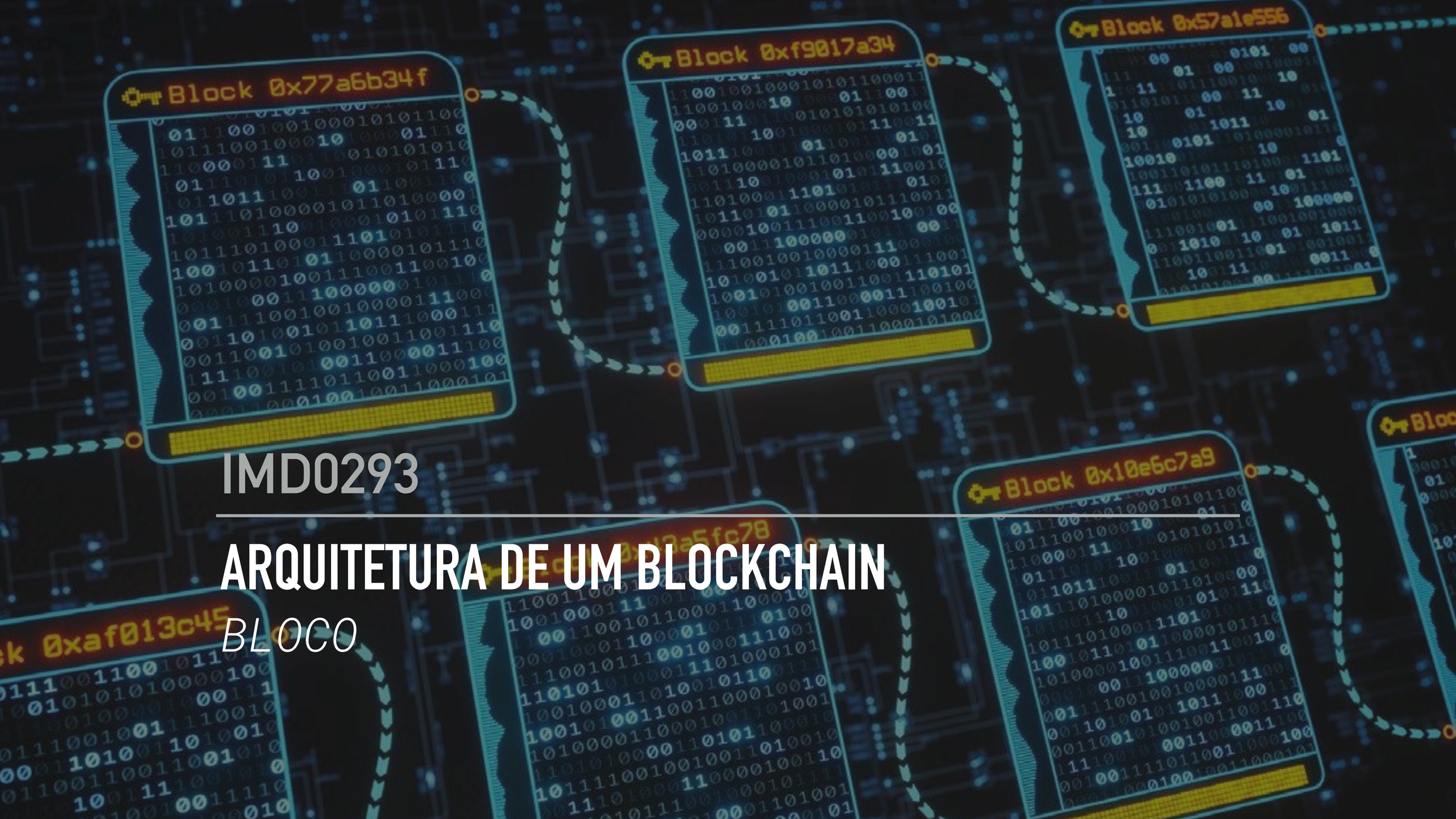
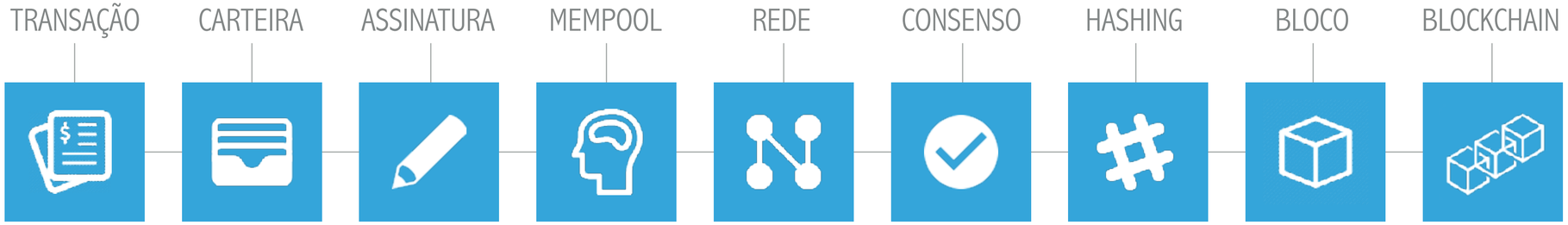


IMD0293

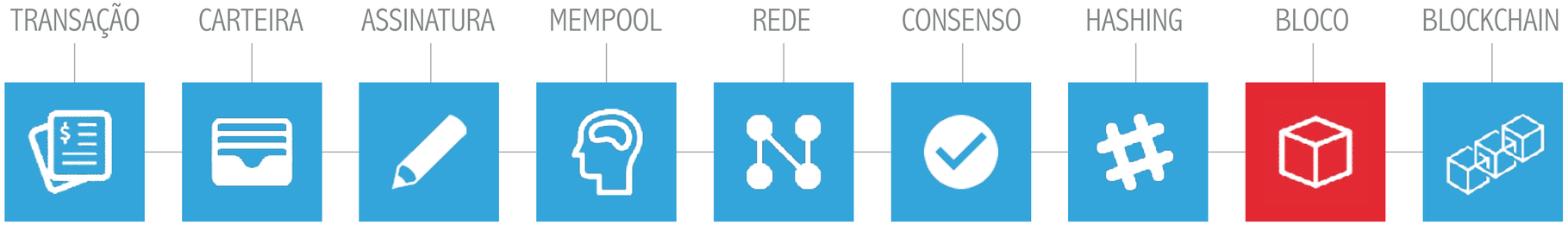
ARQUITETURA DE UM BLOCKCHAIN

BLOCO

ARQUITETURA DE UM **BLOCKCHAIN**

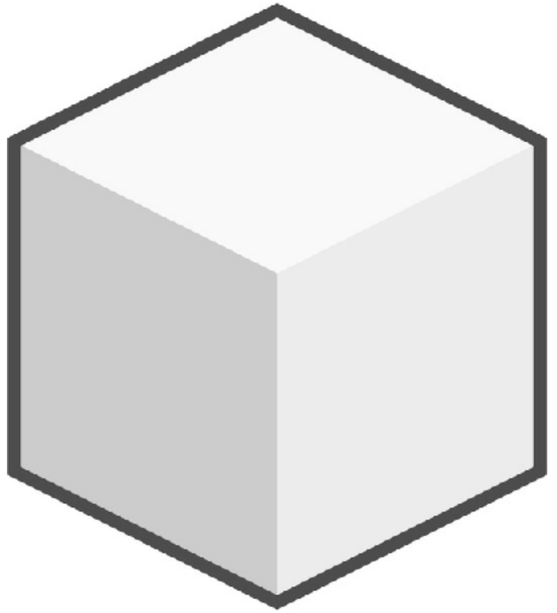


ARQUITETURA DE UM **BLOCKCHAIN**



BLOCOS

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



Bloco

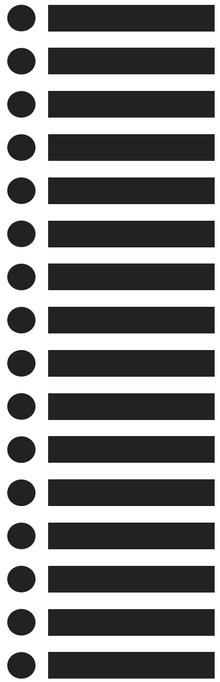
Um *container* que armazena uma lista de transações para serem adicionadas ao *blockchain*.

Blockchain

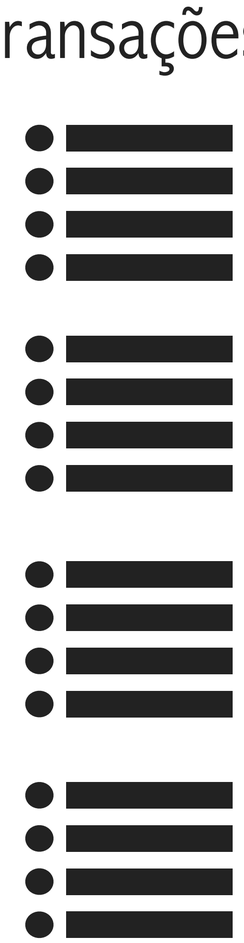
Um livro-razão digital e compartilhado que registra uma lista de transações no formato de uma sequências de blocos.

BLOCOS

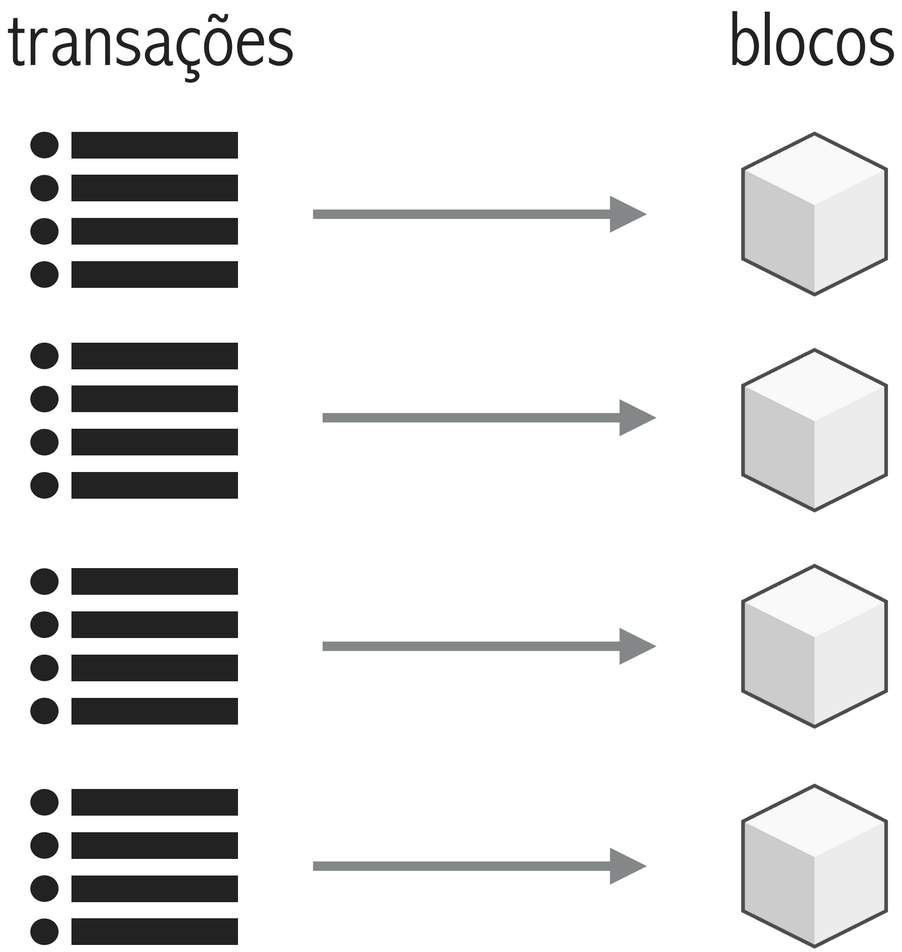
transações



BLOCOS

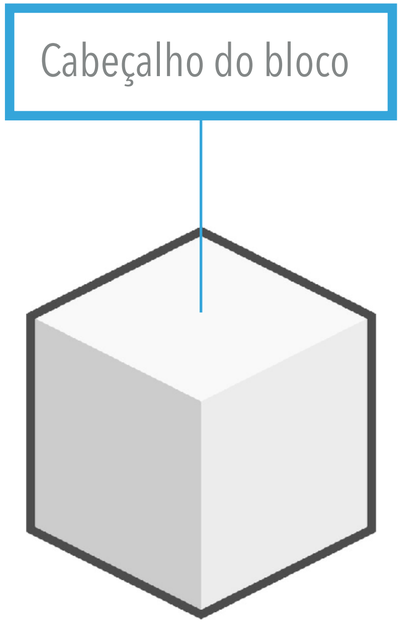


BLOCOS

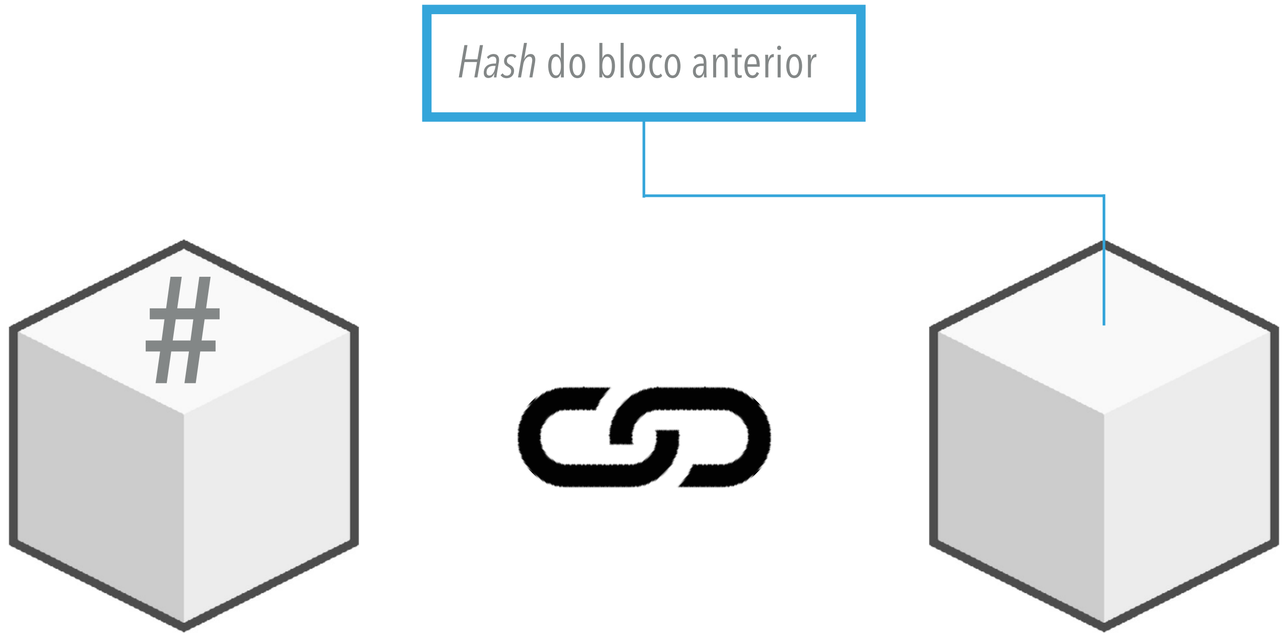


CABEÇALHO DE UM BLOCO

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



CABEÇALHO DE UM BLOCO



blockID = **H(blockHeader)** = H(prevBlockHash || merkleRoot || time || nonce || ...)

CABEÇALHO DE UM BLOCO

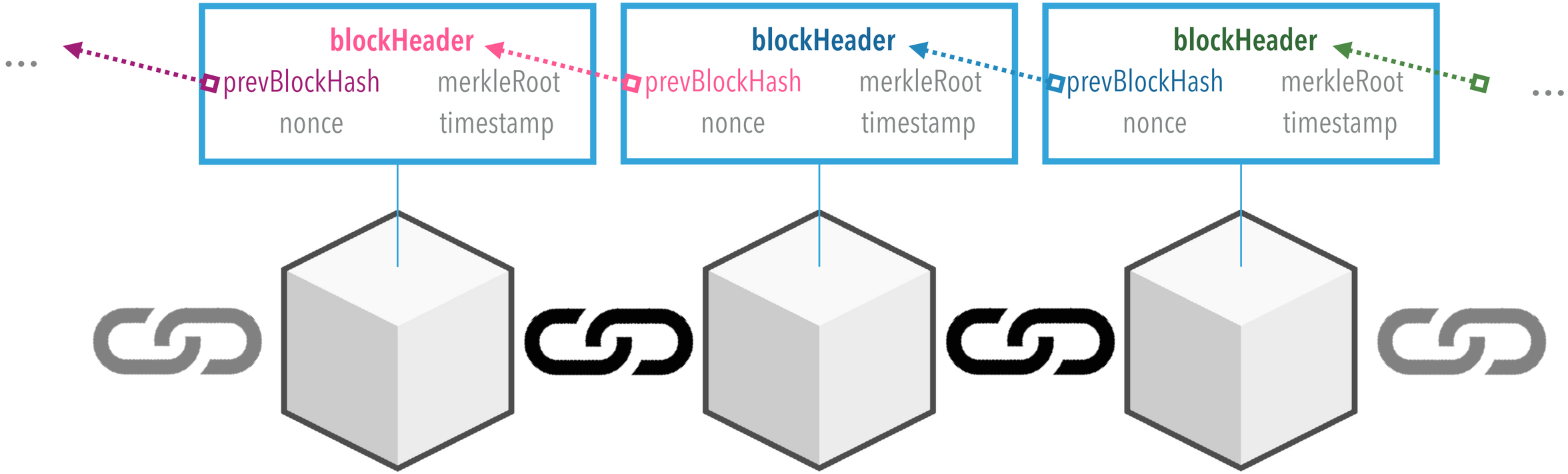
Bloco 123.456 do Bitcoin:

blockID = **SHA256(SHA256(** `010000009500c43a25c624520b5100adf82cb9f9da72fd2447a496bc600b0000000000006cd86237`
`0395dedf1da2841ccda0fc489e3039de5f1ccddef0e834991a65600ea6c8cb4db3936a1ae3143991` **))**

=

000000000002917ED80650C6174AAC8DFC46F5FE36480AAEF682FF6CD83C3CA

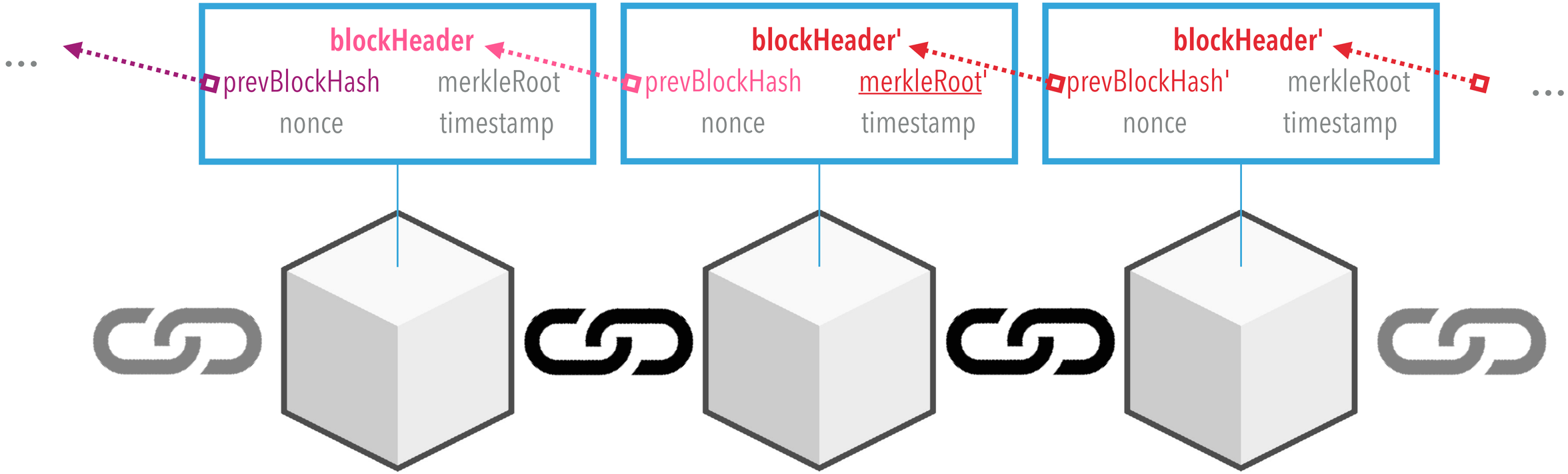
CABEÇALHO DE UM BLOCO



SHA256(SHA256(x))

prevBlockHash = H(prevBlockHash || merkleRoot || time || nonce)

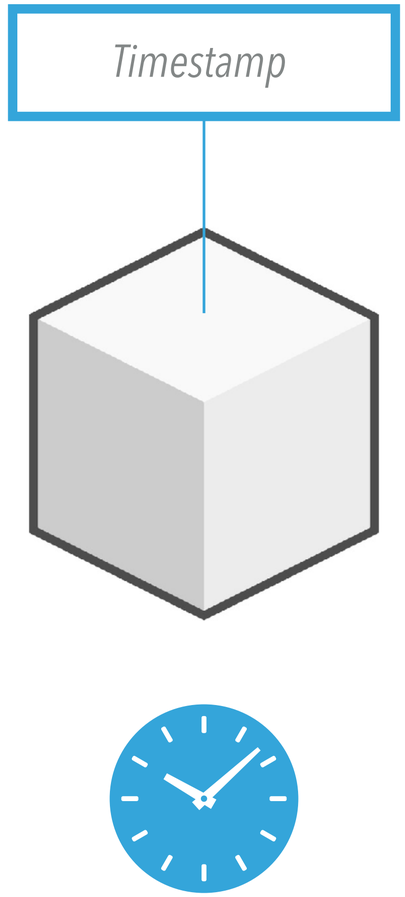
CABEÇALHO DE UM BLOCO



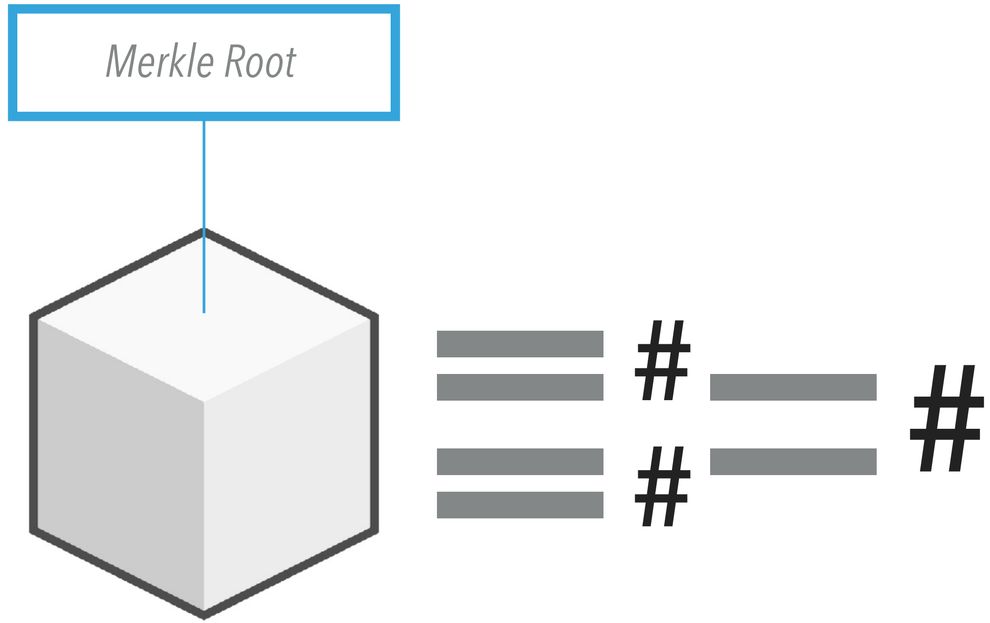
SHA256(SHA256(x))

prevBlockHash = H(prevBlockHash || merkleRoot || time || nonce)

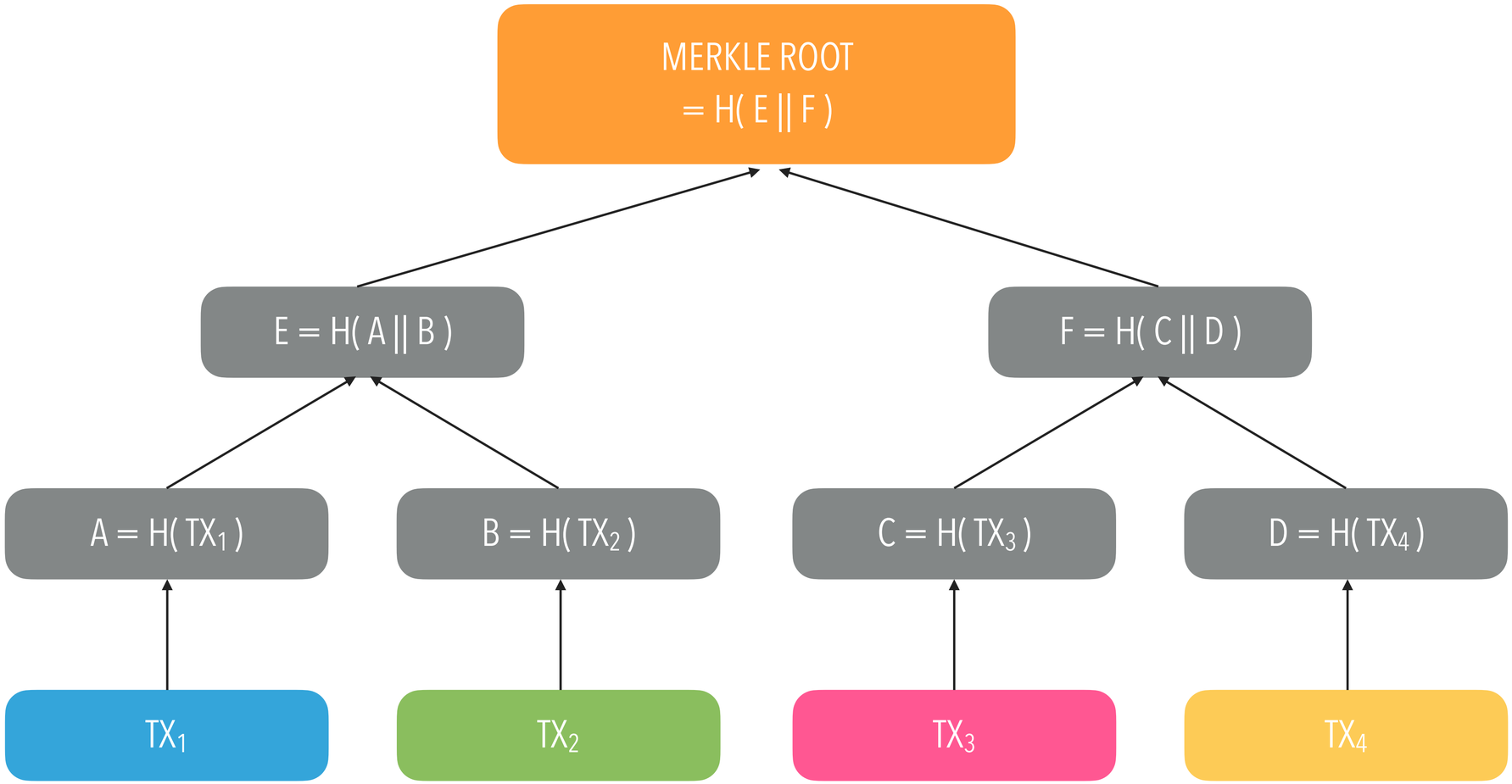
CABEÇALHO DE UM BLOCO



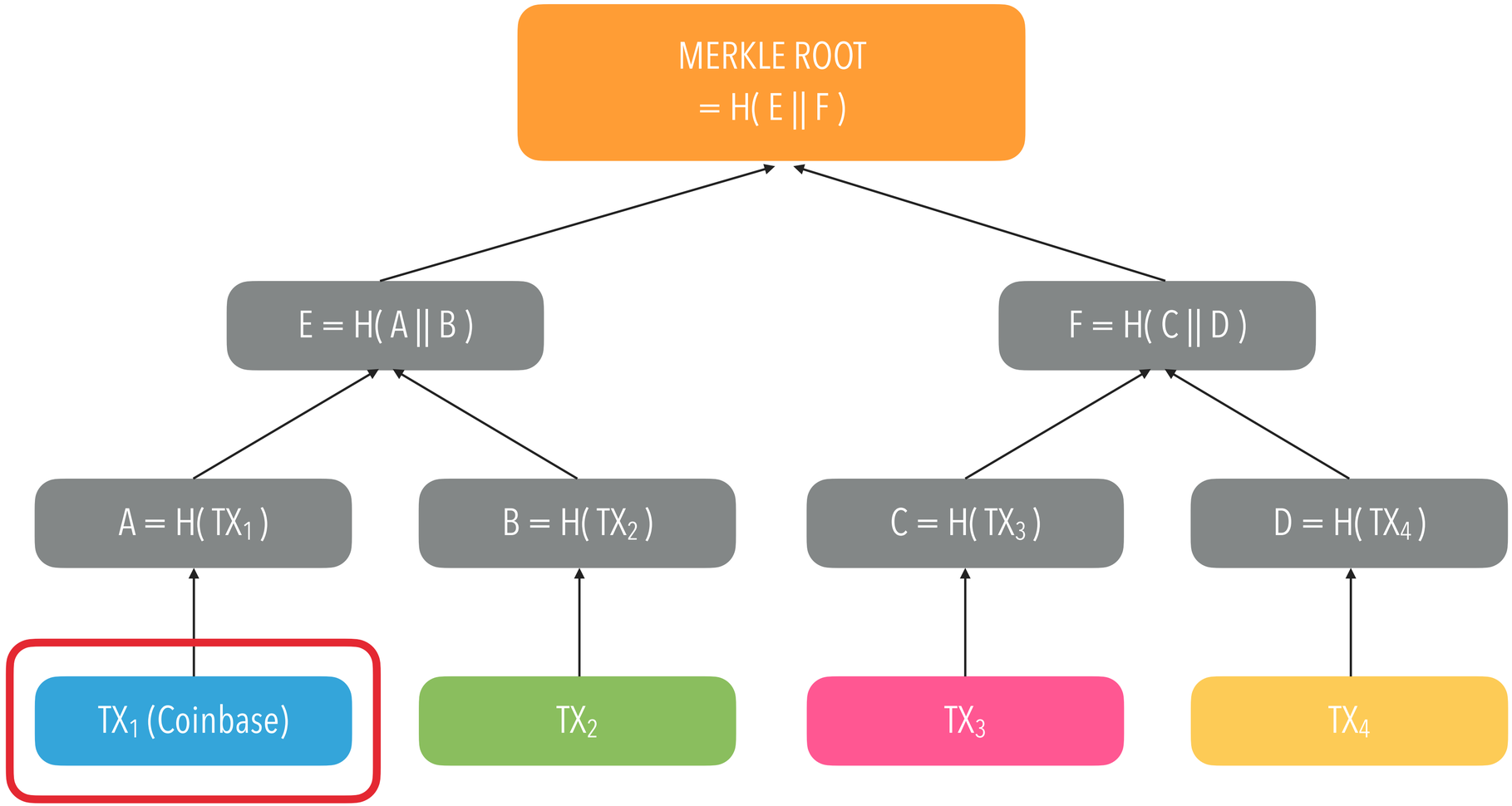
CABEÇALHO DE UM BLOCO



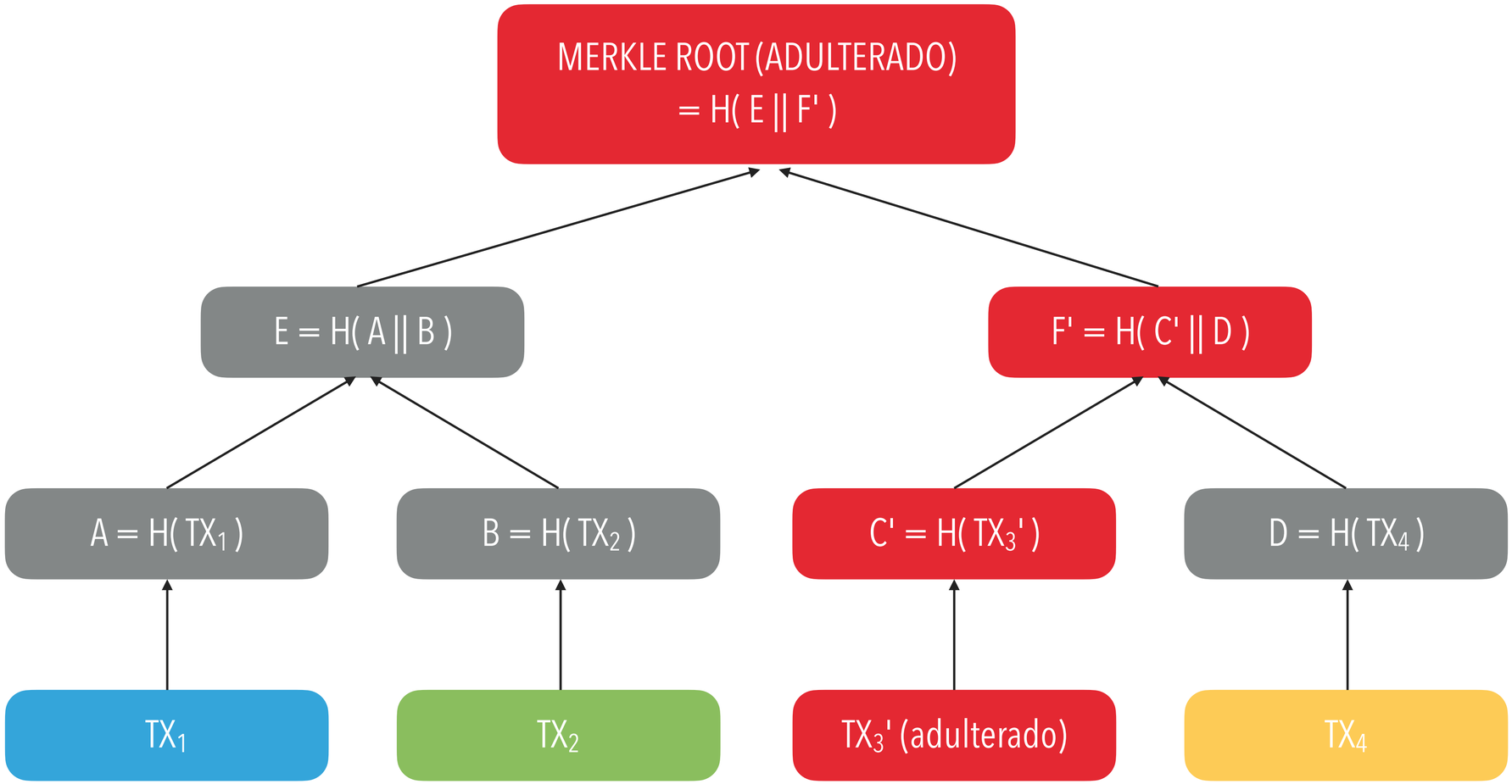
MERKLE ROOT


MERKLE ROOT
= H(E || F)
E = H(A || B)
F = H(C || D)
A = H(TX1)
B = H(TX2)
C = H(TX3)
D = H(TX4)
TX1
TX2
TX3
TX4

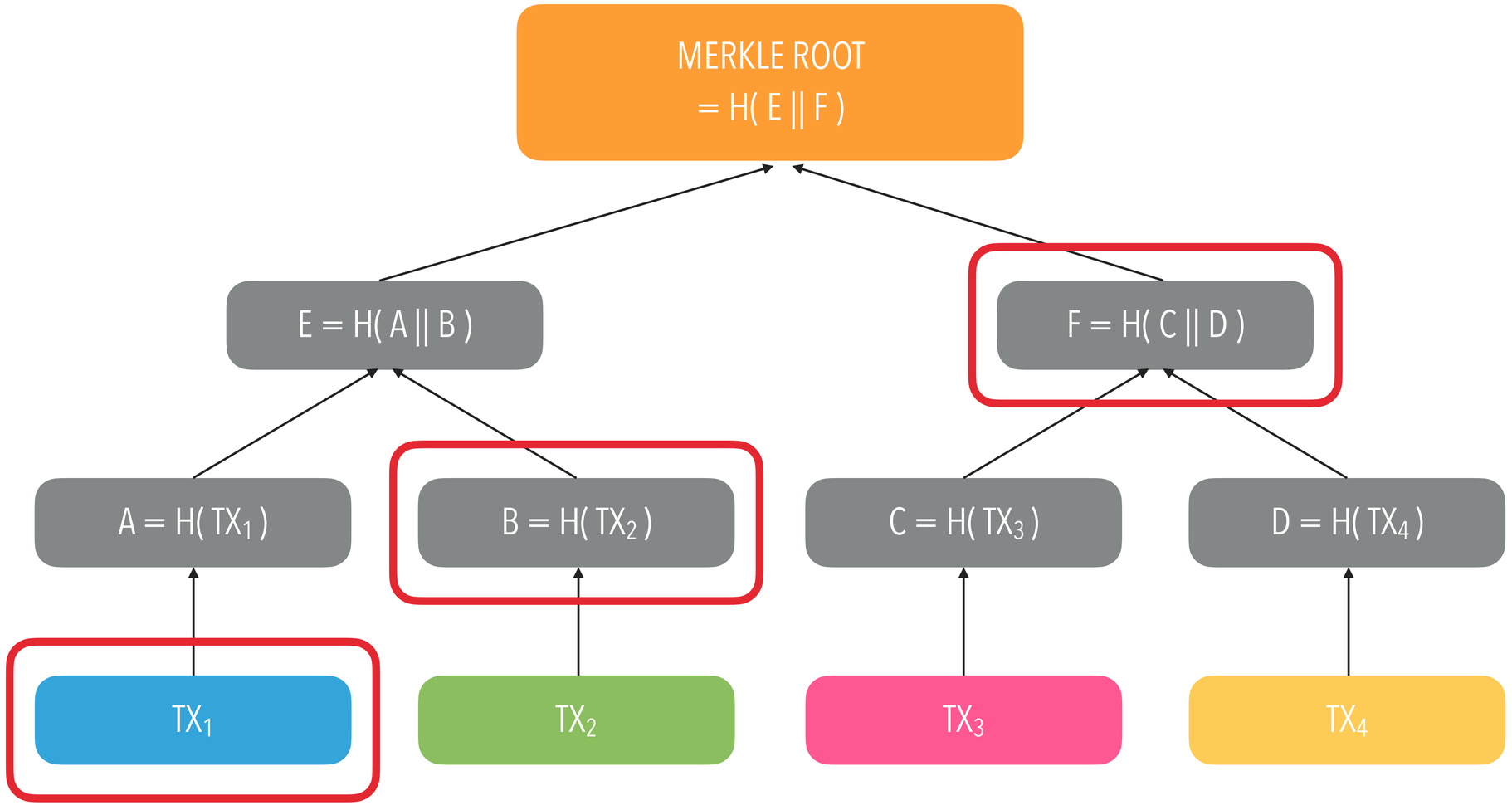
MERKLE ROOT


MERKLE ROOT
= H(E || F)
E = H(A || B)
F = H(C || D)
A = H(TX1)
B = H(TX2)
C = H(TX3)
D = H(TX4)
TX1 (Coinbase)
TX2
TX3
TX4

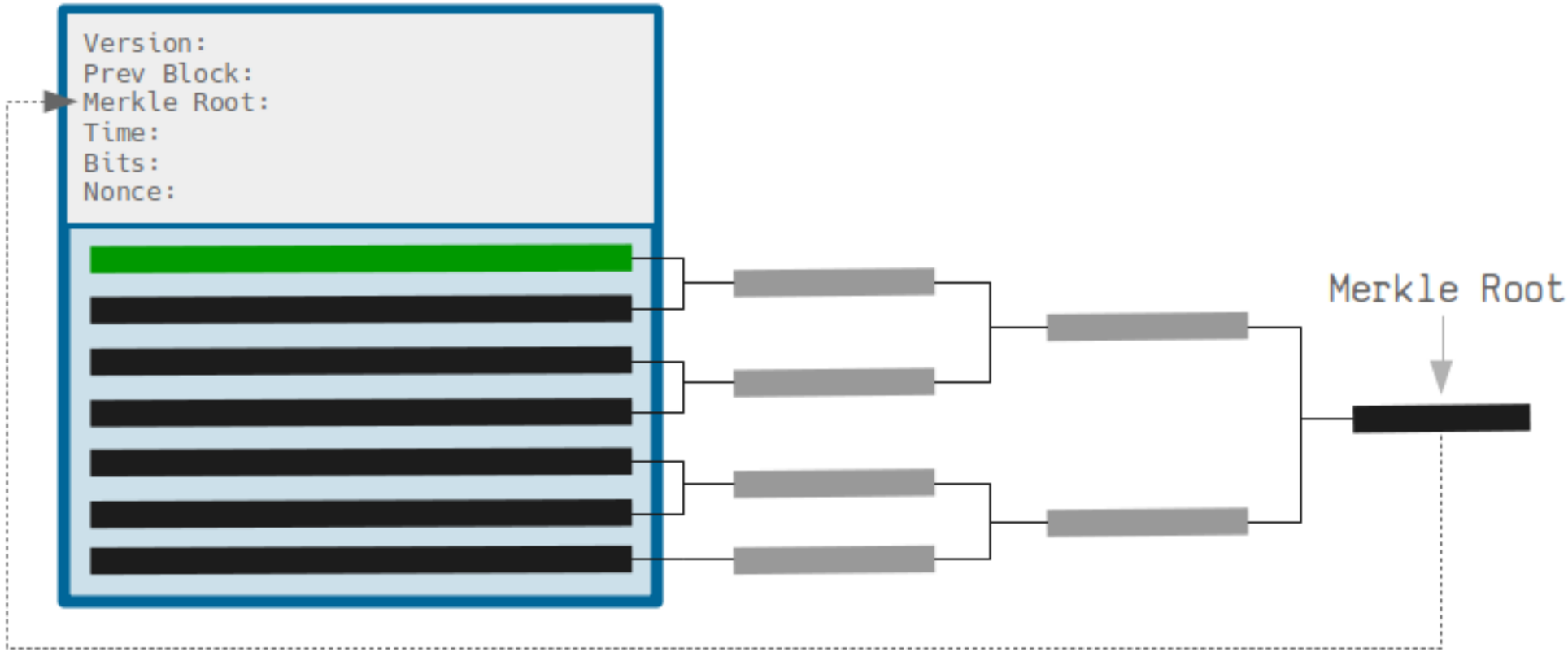
MERKLE ROOT


MERKLE ROOT (ADULTERADO)
= H(E || F')
E = H(A || B)
F' = H(C' || D)
A = H(TX1)
B = H(TX2)
C' = H(TX3')
D = H(TX4)
TX1
TX2
TX3' (adulterado)
TX4

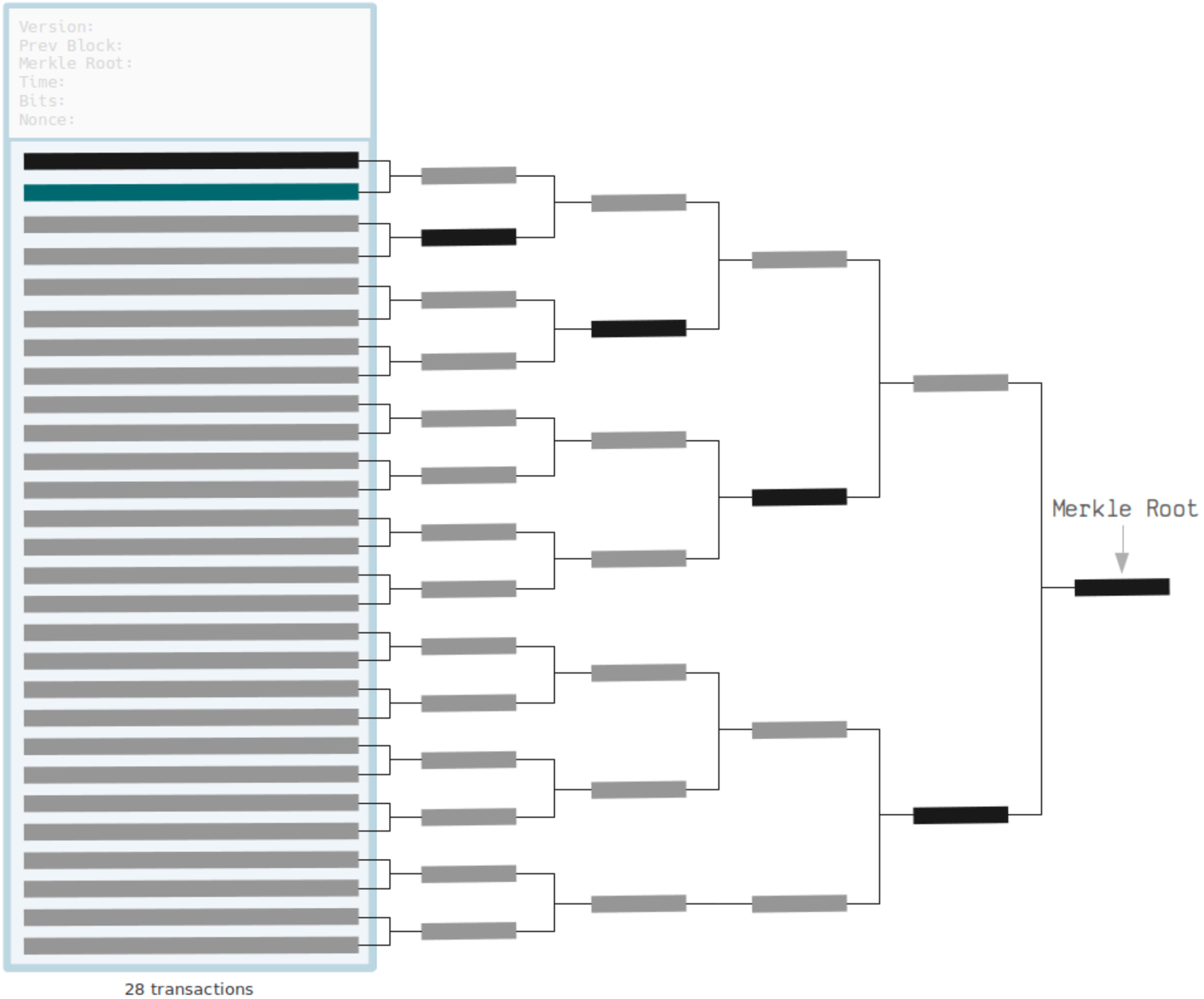
MERKLE ROOT E PROOF-OF-INCLUSION



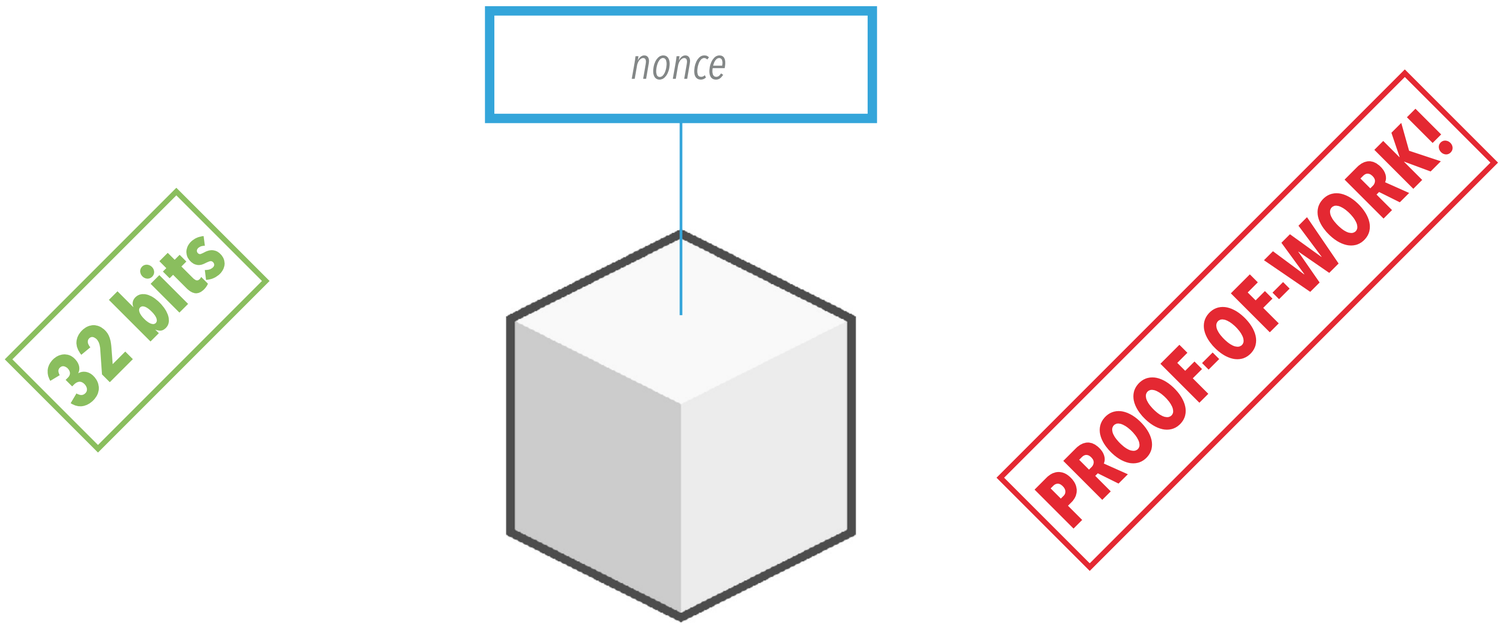
MERKLE ROOT



ARQUITETURA DE UM BLOCKCHAIN



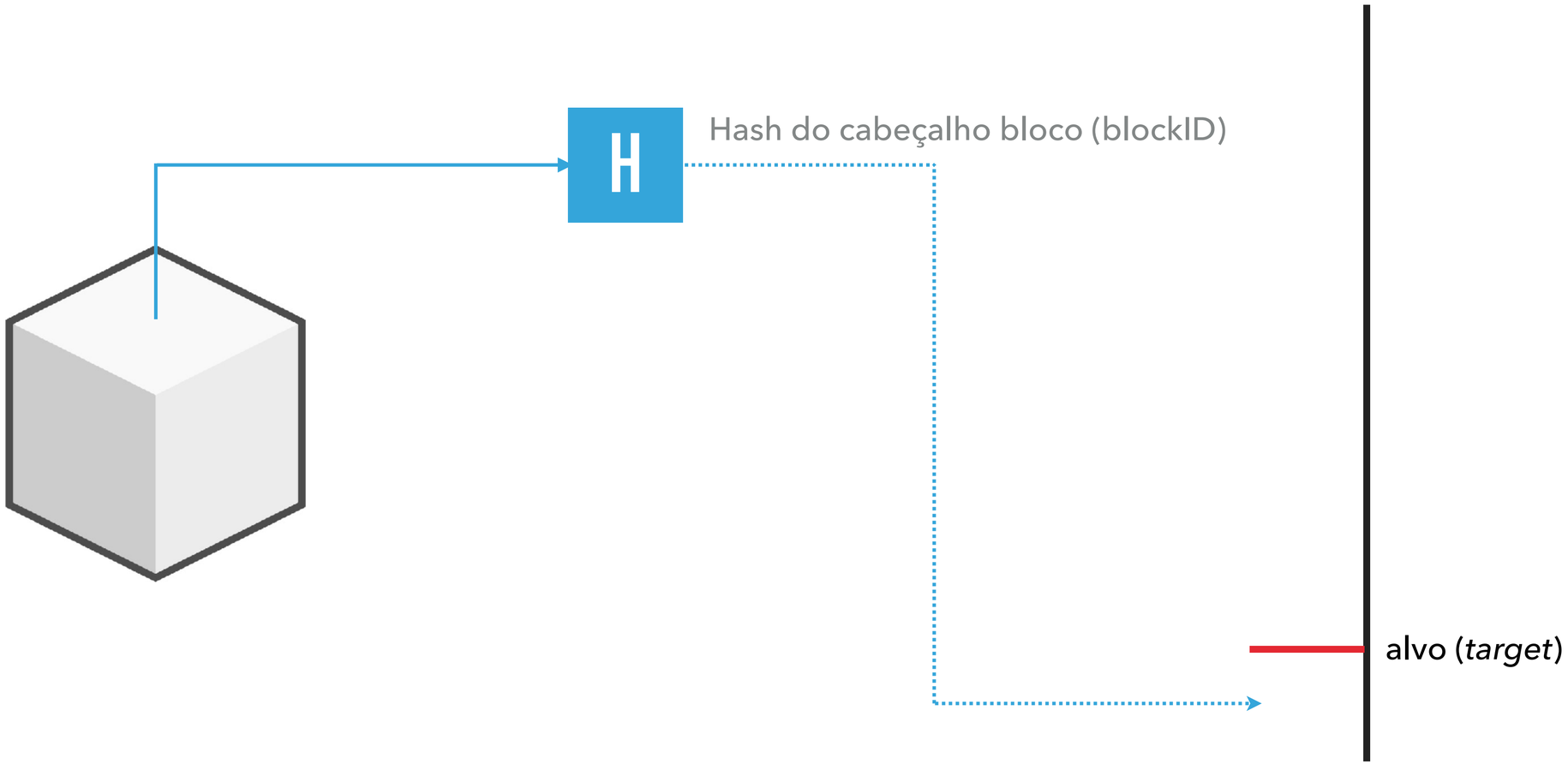
CABEÇALHO DE UM BLOCO



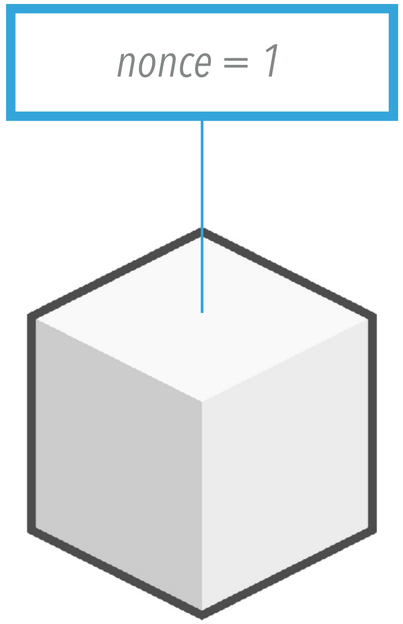
Enigma criptográfico hash: Encontrar um *nonce* que satisfaça a seguinte inequação:

H(prevBlockHash || merkleRoot || time || nonce) < target

CABEÇALHO DE UM BLOCO

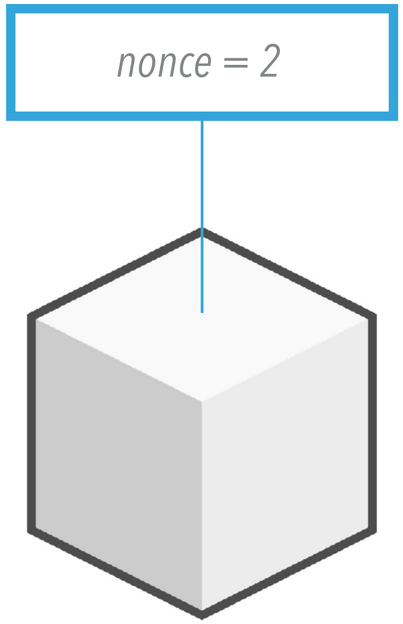


CABEÇALHO DE UM BLOCO



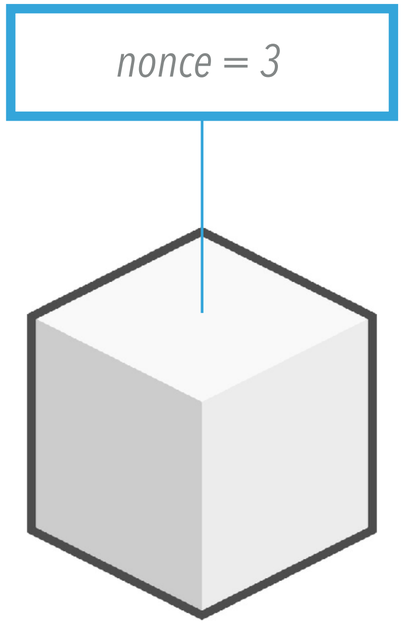
4c47c2d47712cc266c3b7ed7e9a0bcda2e6786f7455b9af3e9df3c5a2b26ddbf

CABEÇALHO DE UM BLOCO



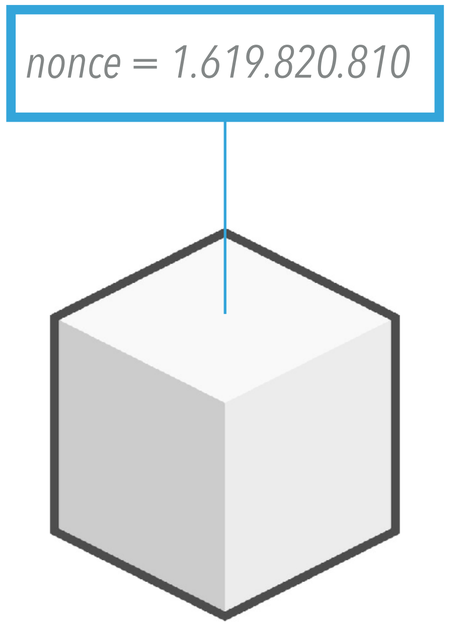
6bbe9136c059738eaaf237c995a78971788ee87119d82ef640a7288b43928017

CABEÇALHO DE UM BLOCO



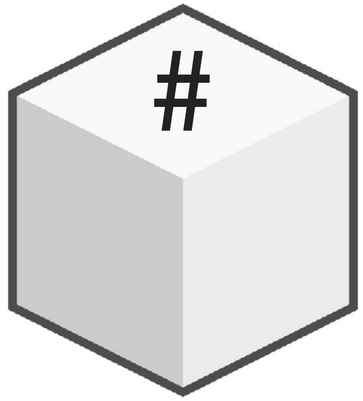
000004bb7c4d63435e1fa5595986fab643490560699bf35c43bdc6ecfd3ea721

CABEÇALHO DE UM BLOCO



00000000000000000274cb1a04c382475310f70cee3776af06414f22f8337044

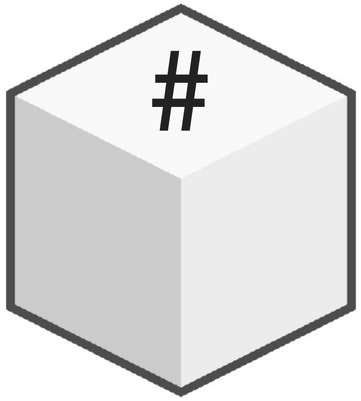
DIFICULDADE DE UM BLOCO



Dificuldade do bloco:

0000000HASHVALUE

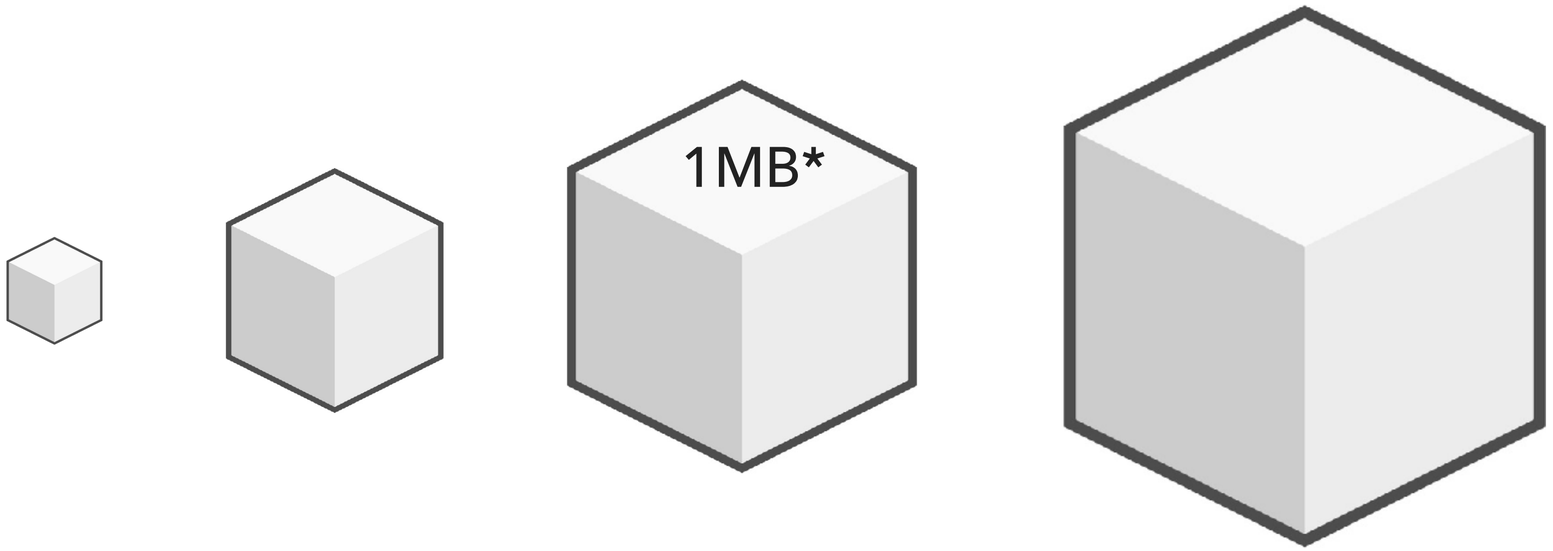
DIFICULDADE DE UM BLOCO



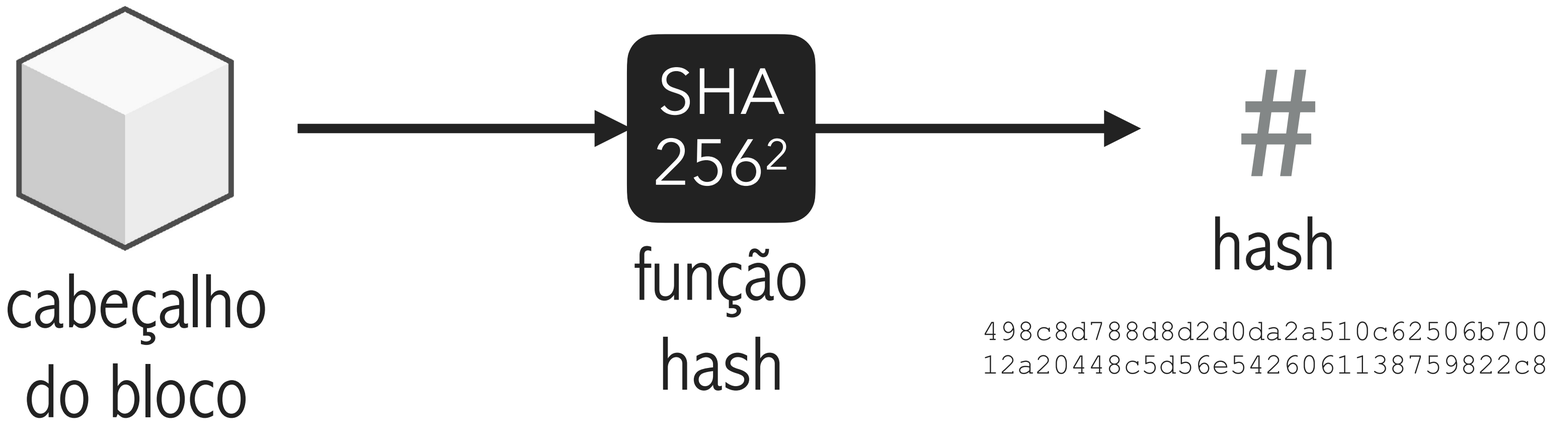
Dificuldade do bloco:

0000000HASHVALUE

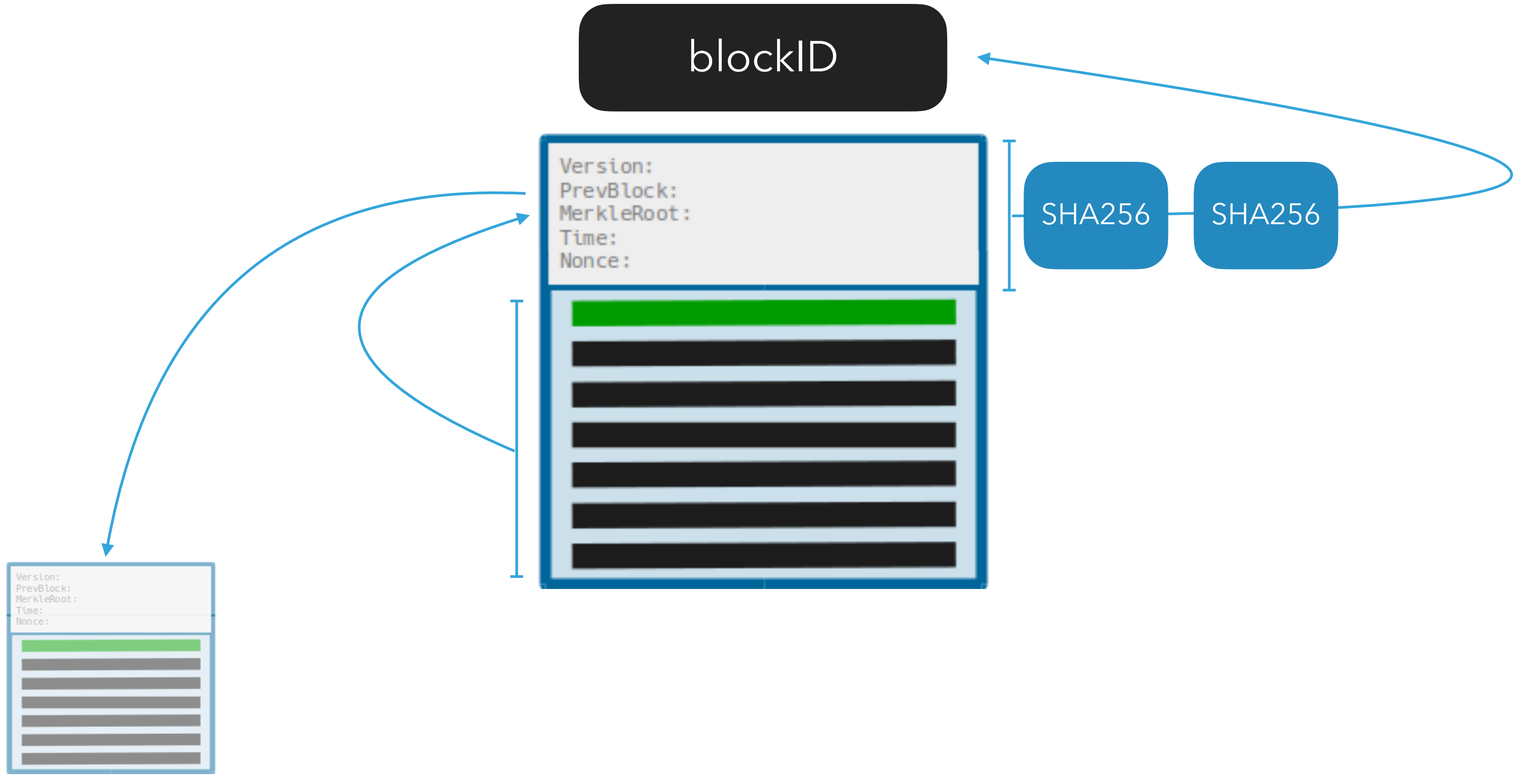
TAMANHO DE UM BLOCO (BITCOIN)



HASH DE UM BLOCO



ID DE UM BLOCO



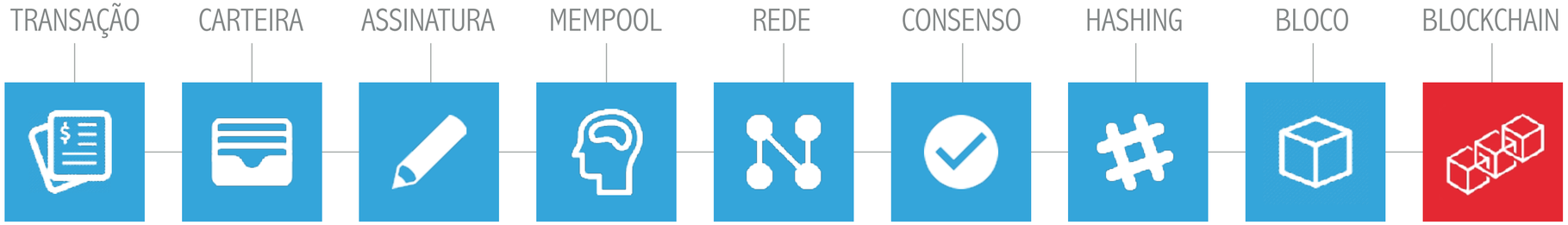
EXEMPLO – BLOCO #485963

https://www.blockchain.com/btc/block/0000000000000000013942c4215cd92306bbce769cfcb349d0b42f031c994eb

BLOCO - DEMO

https://andersbrownworth.com/blockchain/block

ARQUITETURA DE UM **BLOCKCHAIN**

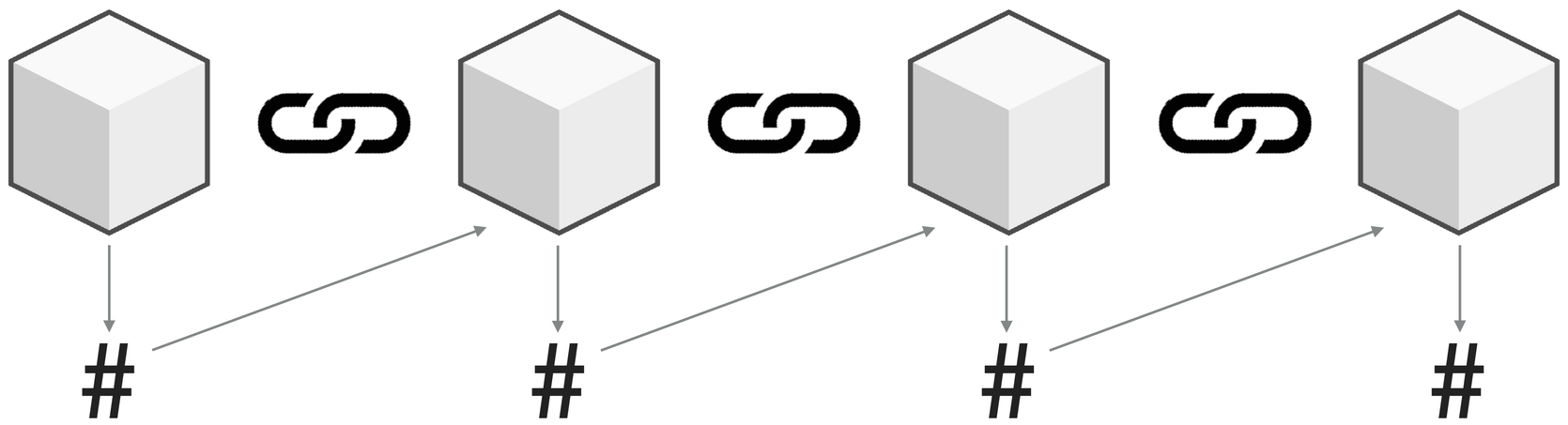


Blockchain

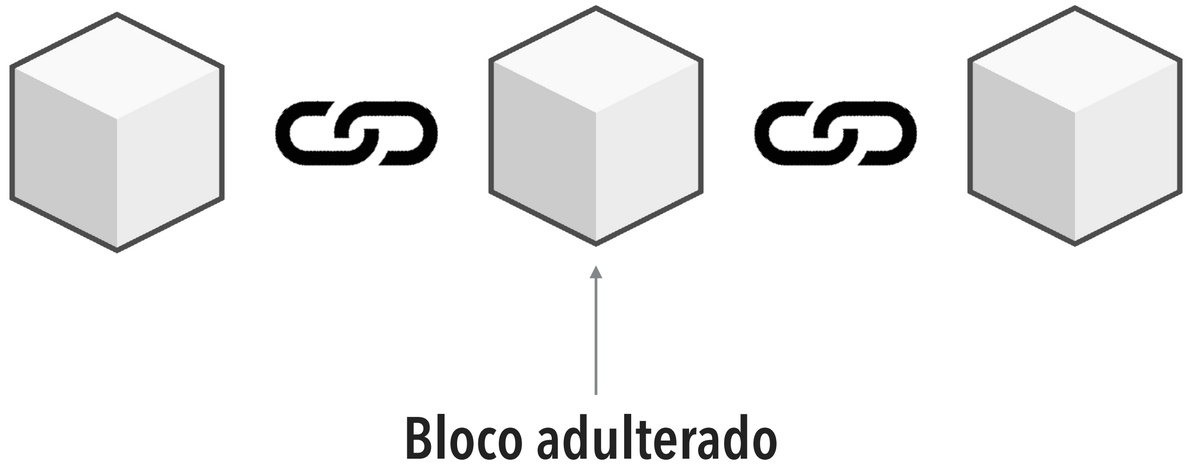
Um livro-razão digital e compartilhado que registra um histórico de transações feitas na rede.

CORRENTE DE BLOCOS

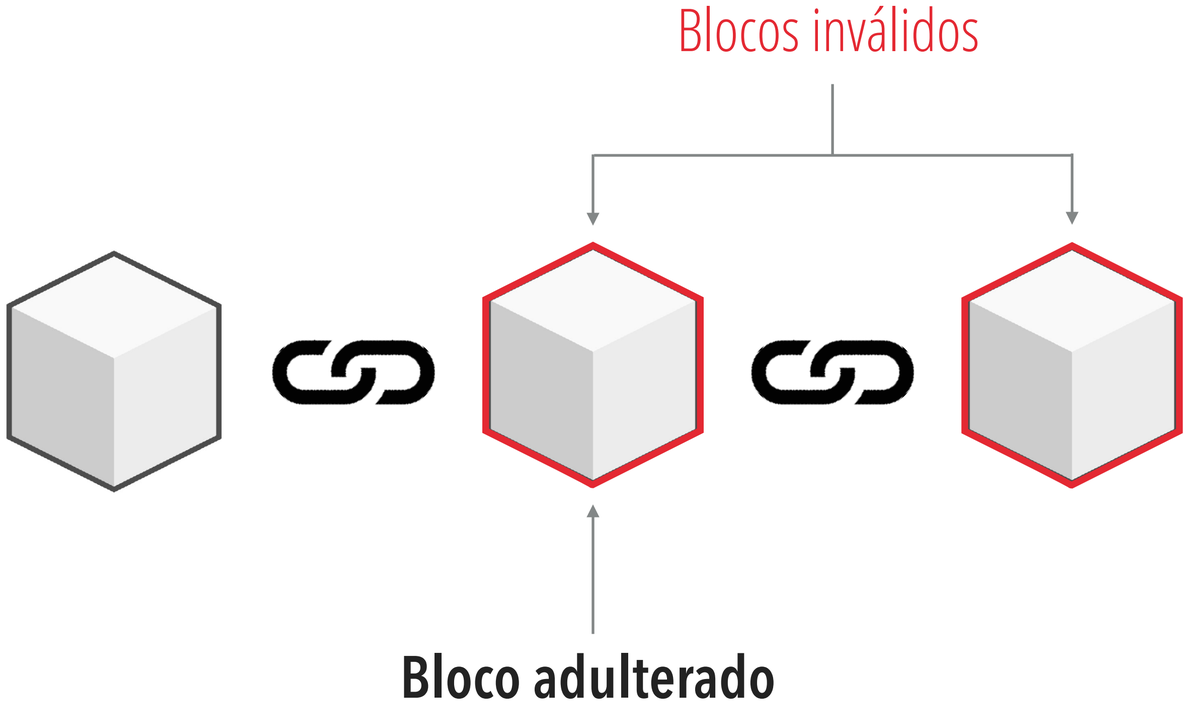
CORRENTE DE BLOCOS



CORRENTE DE BLOCOS



CORRENTE DE BLOCOS

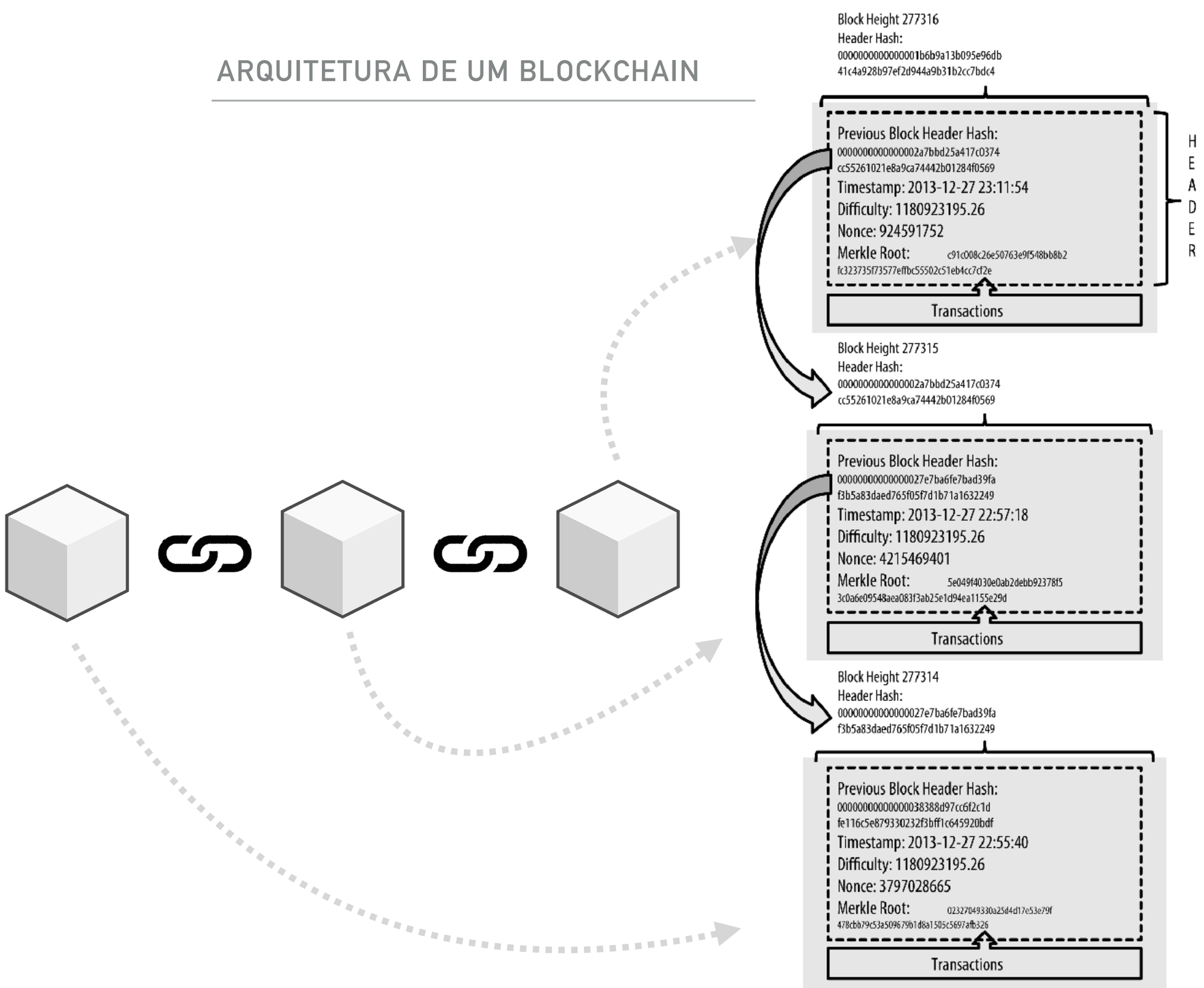


NÚMERO DO BLOCO

BLOCO GÊNESIS

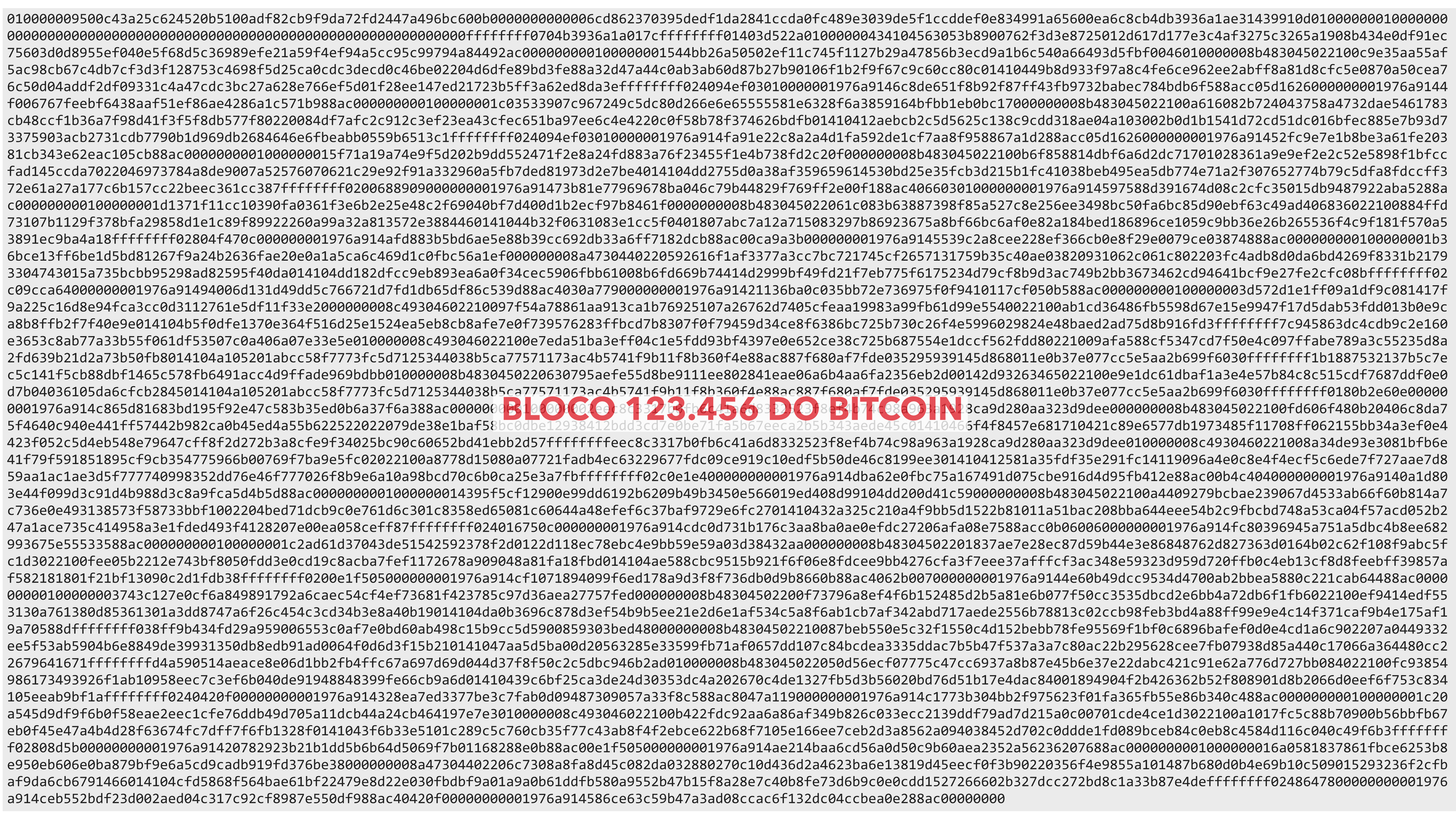
https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

ARQUITETURA DE UM BLOCKCHAIN



BLOCKCHAIN - DEMO

https://andersbrownworth.com/blockchain/blockchain


BLOCO 123.456 DO BITCOIN

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/