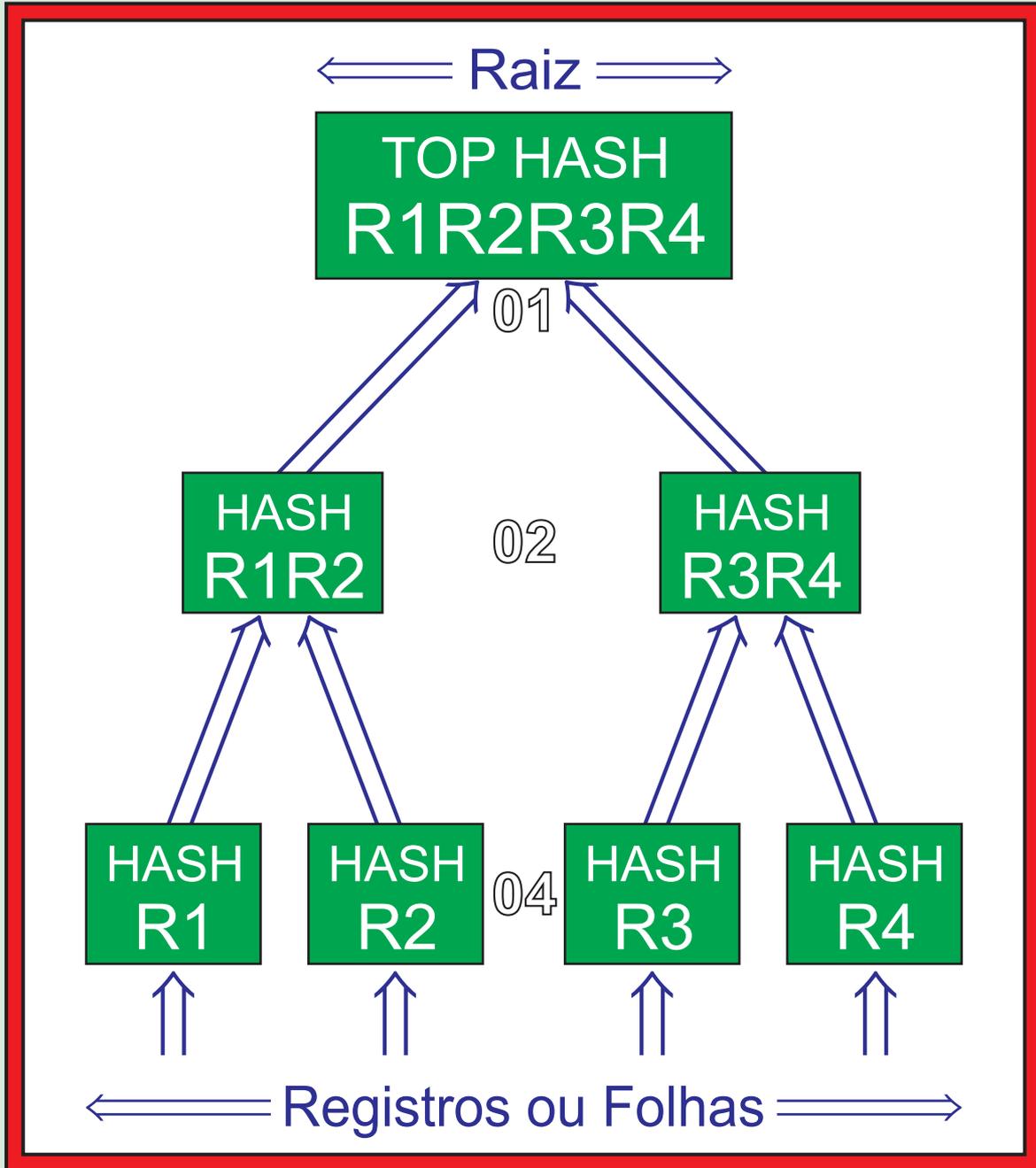




ÁRVORE MERKLE

Registros

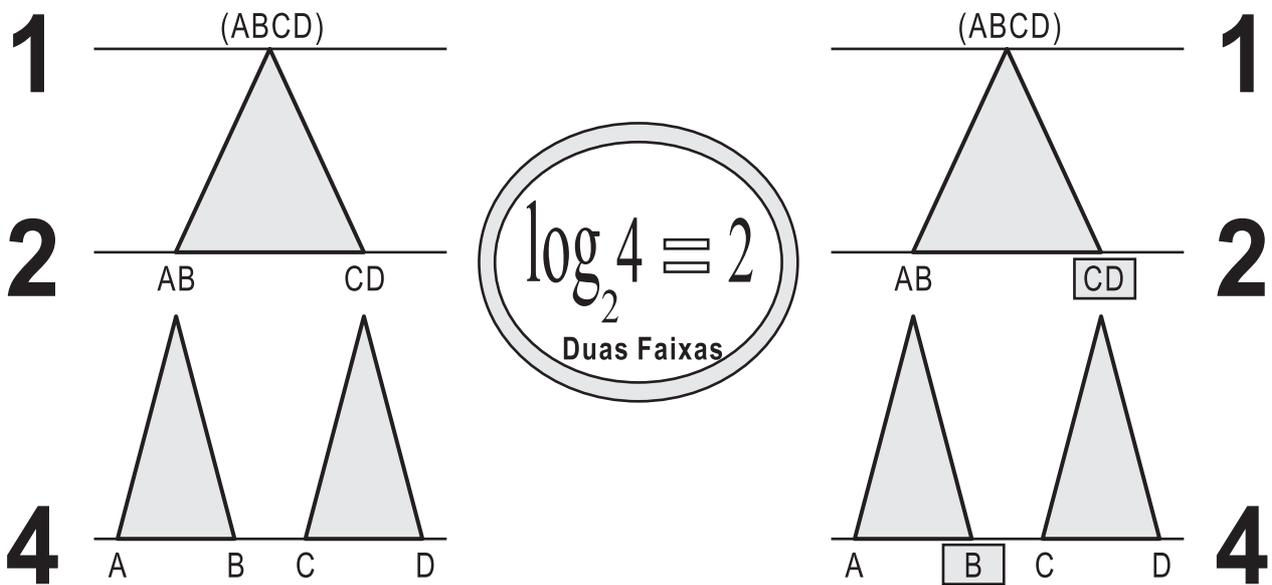


Ralph Merkle



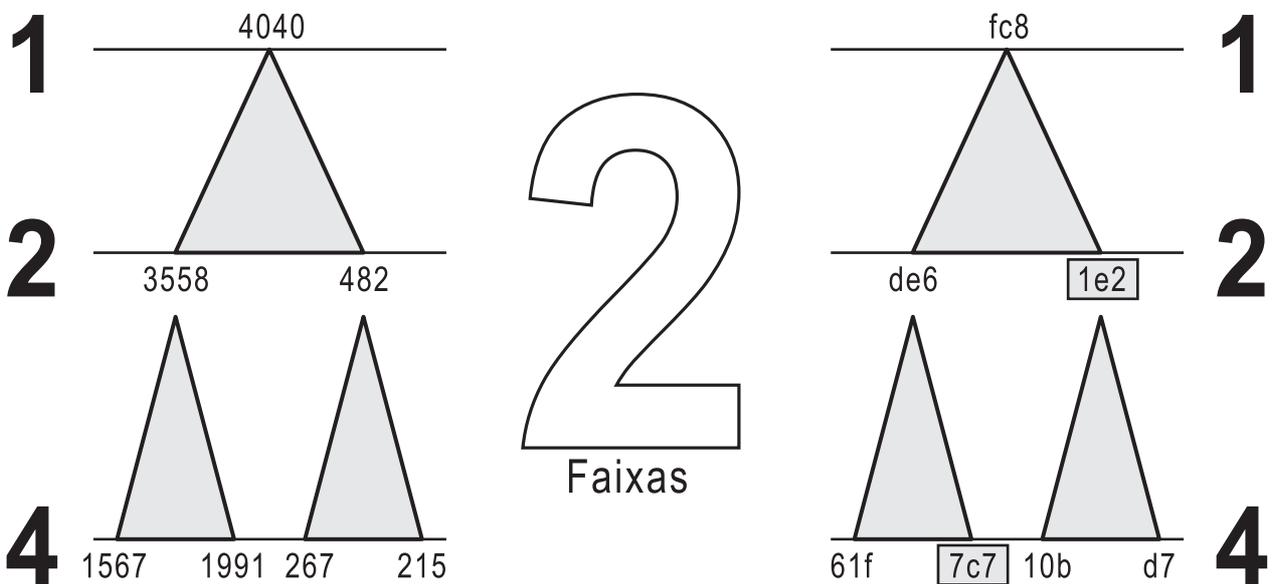
2.2 Árvore Secunda com Raiz ABCD Conhecida

Montagem da Árvore com ABCD



Para verificar se “A” pertence a tree basta conhecer “B” e “CD”.

Exemplo de Pertencimento



A = 1567 (61f) pertence a tree pois $4040 \square 482 = 3558 = (de6)$ e $3558 \square 1991 = 1567 = (61f)$ também, pertence a tree, o que valida 61f.

Árvore Hashiada de Merkle



3.0 Árvore Hashiada de Ralph Merkle

Merkle Root

Hash(a · txt)(b · txt)(c · txt)(d · txt)

Altura
01

Hash(a ◦ txt)(b ◦ txt)

Altura
02

Hash(c ◦ txt)(d ◦ txt)

Hash(a ◦ txt)

Hash(b ◦ txt)

Altura
04

Hash(c ◦ txt)

Hash(d ◦ txt)

Leaf (a)

Leaf (b)

Leaf (c)

Leaf (d)

**757e42e17a7e11066d232539aeb37a86
c7408d85d08876e647a5cafb9da2e6ec**



Bloco/Altura/61802 e sua Raiz Merkle

Hash

0000000000000000000000000421d800240772265a1a4a38156f97322e143b49a5d9a3



Mineradores que Confirmaram = 25

Timestamp = 2020-02-18 20:31

Altura/ Index = 618002

Minerador = Desconhecido

Número de Transações = 2.835



Raiz Merkle

81bdd28a48f9c2581475cc34ab3d32172d4b7c7f112ed9e7c1832b12a5a770c9

SHA

Tamanho = 1.281.083 bytes

Nonce = 548.955.453

Volume das Transações = 7390.10358708 BTC

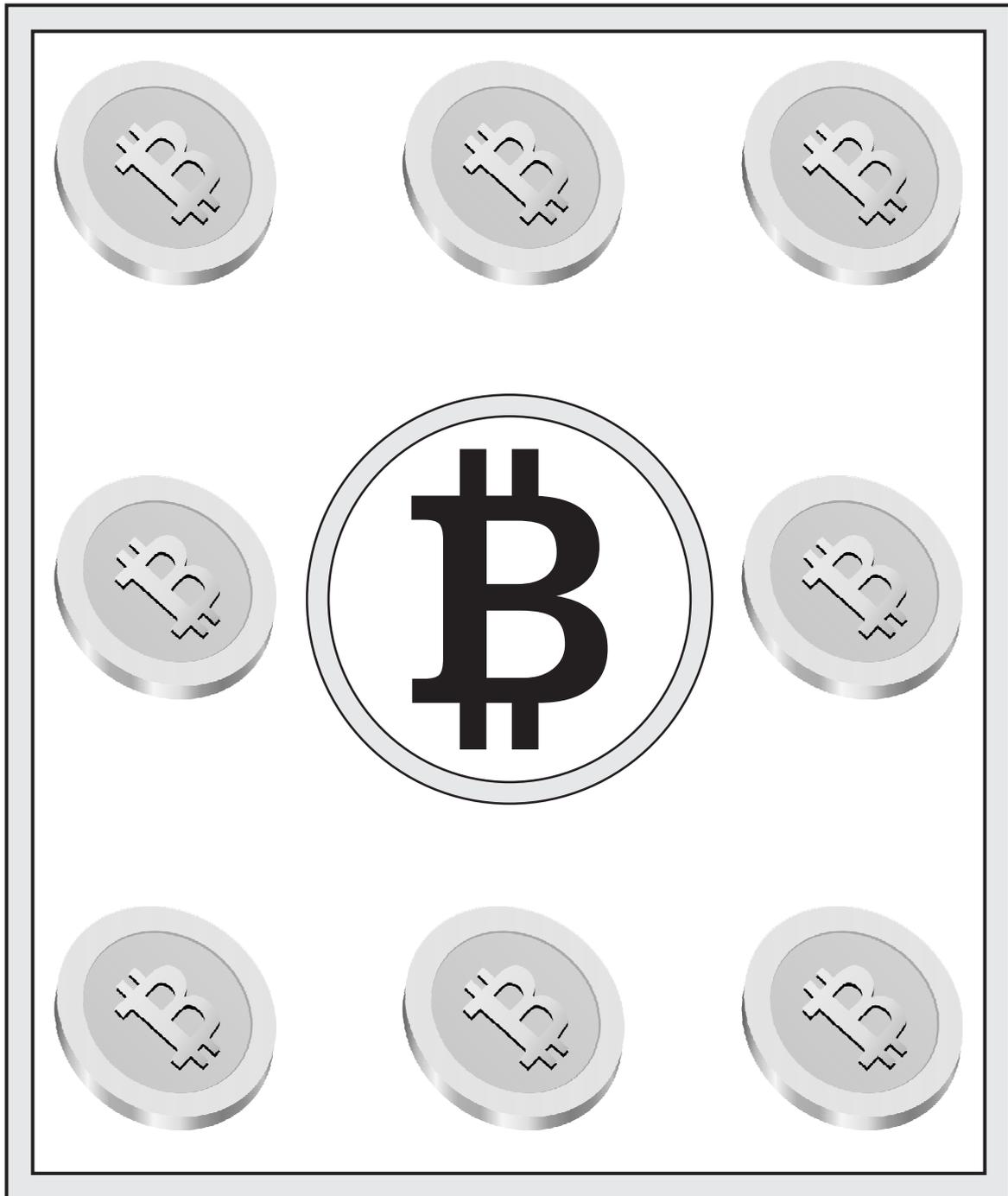
Recompensa Pelo Bloco = 12.50 BTC

652



Moeda Bitcoin

MINERS



Satoshi Nakamoto