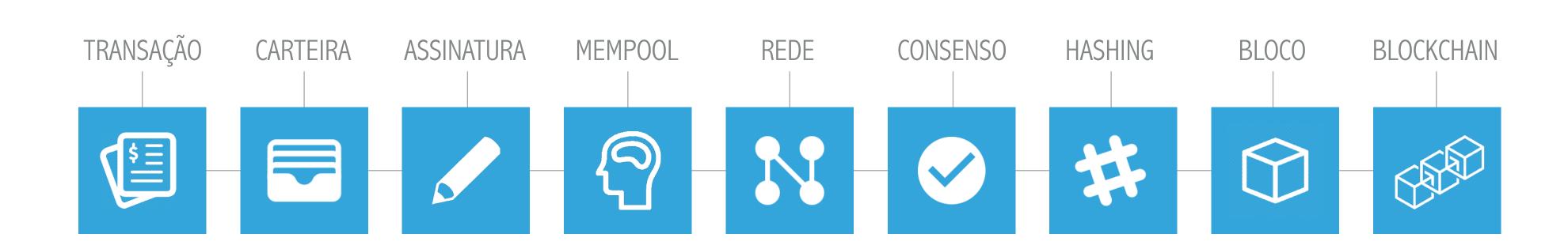
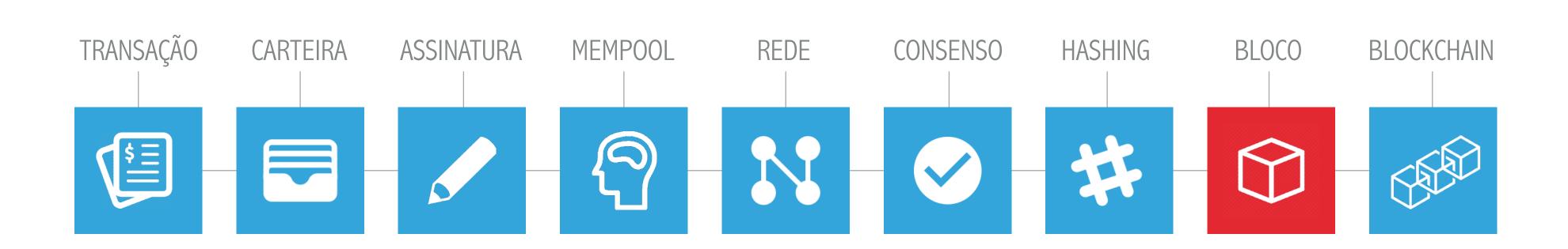


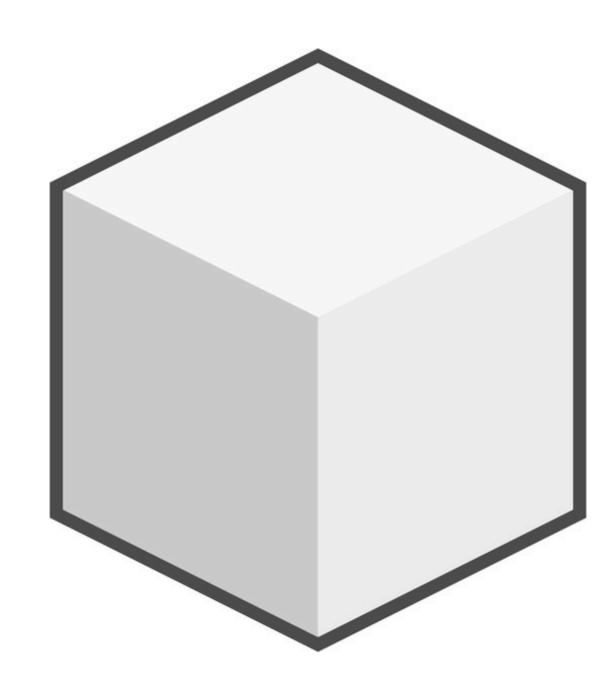
Arquitetura de um **Blockchain**



Arquitetura de um **Blockchain**



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



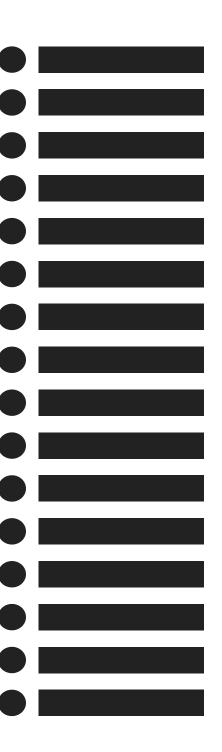
Bloco

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.

transações



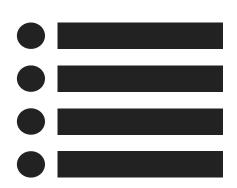
transações

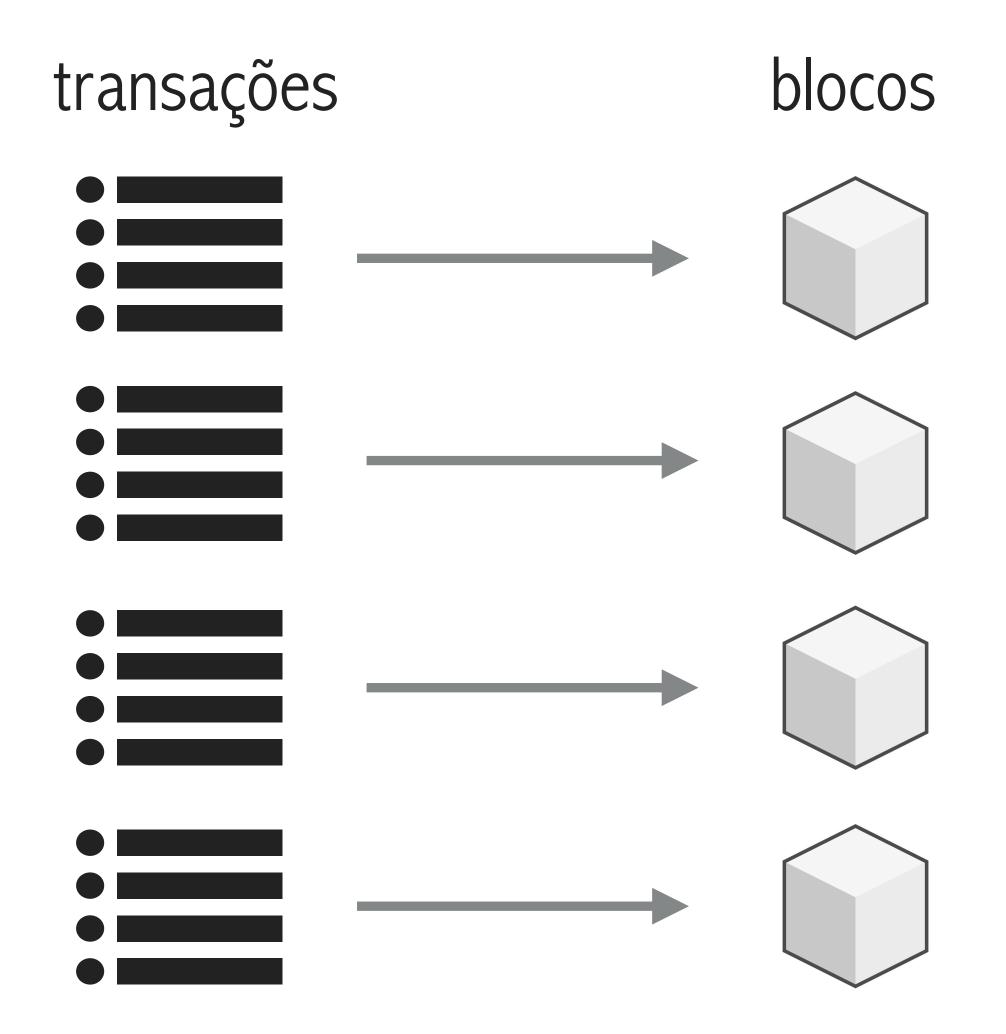




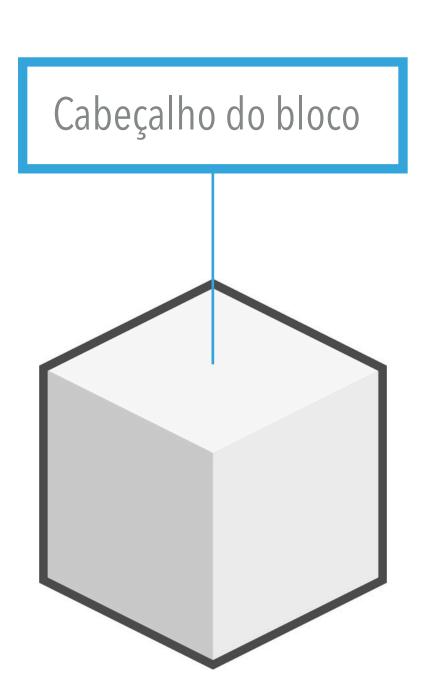


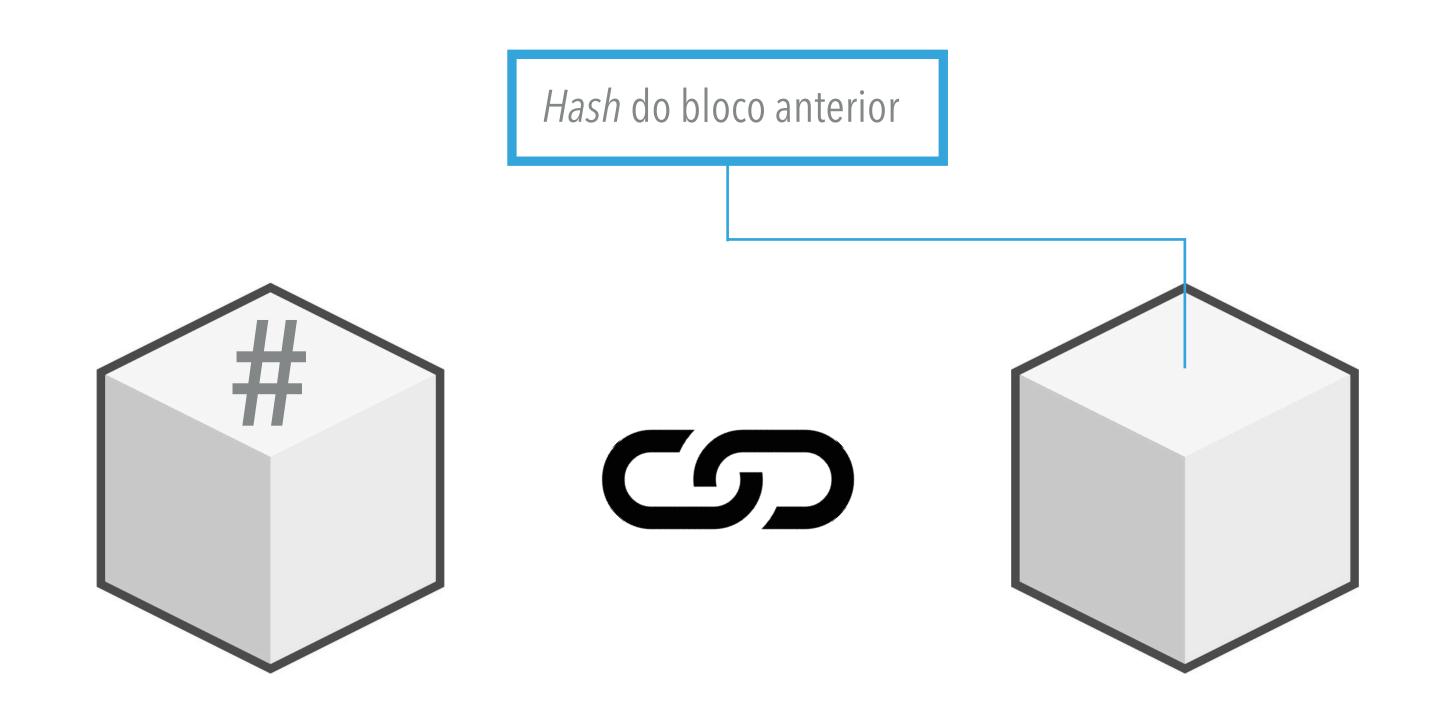




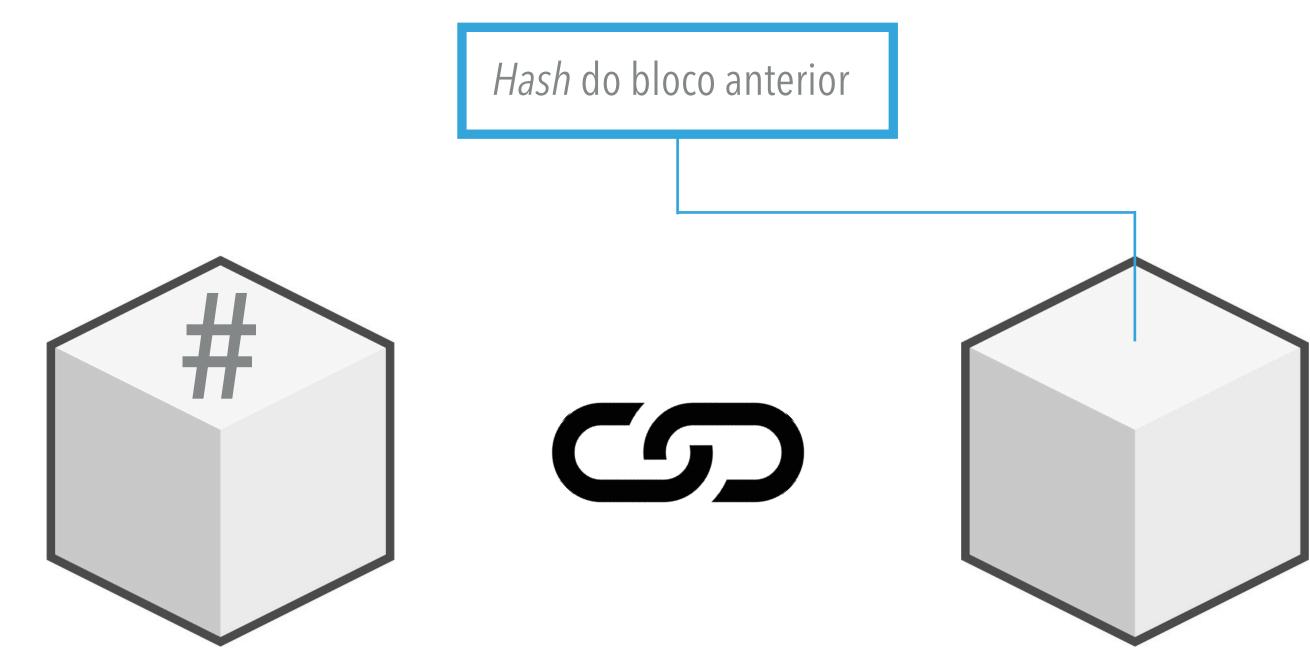


- Hash do bloco anterior (prevBlockHash)
- Timestamp
- Merkle Root
- Nonce

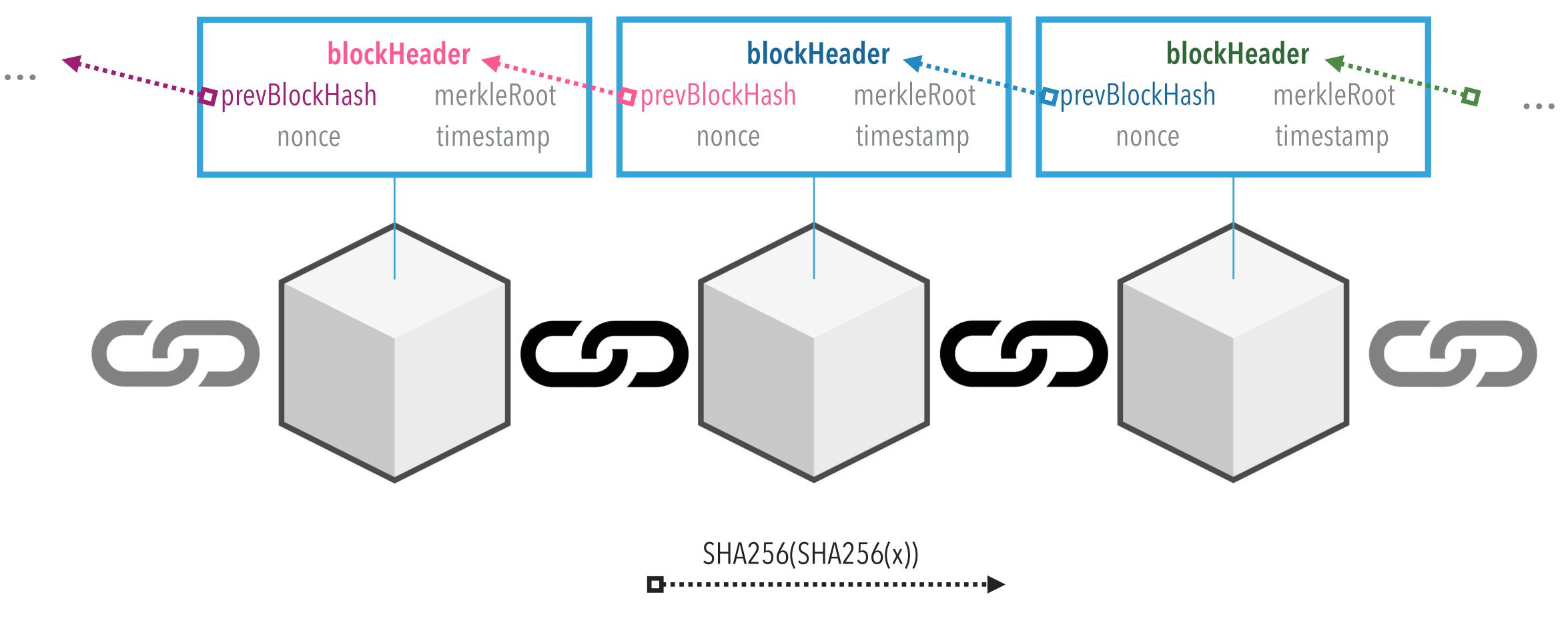




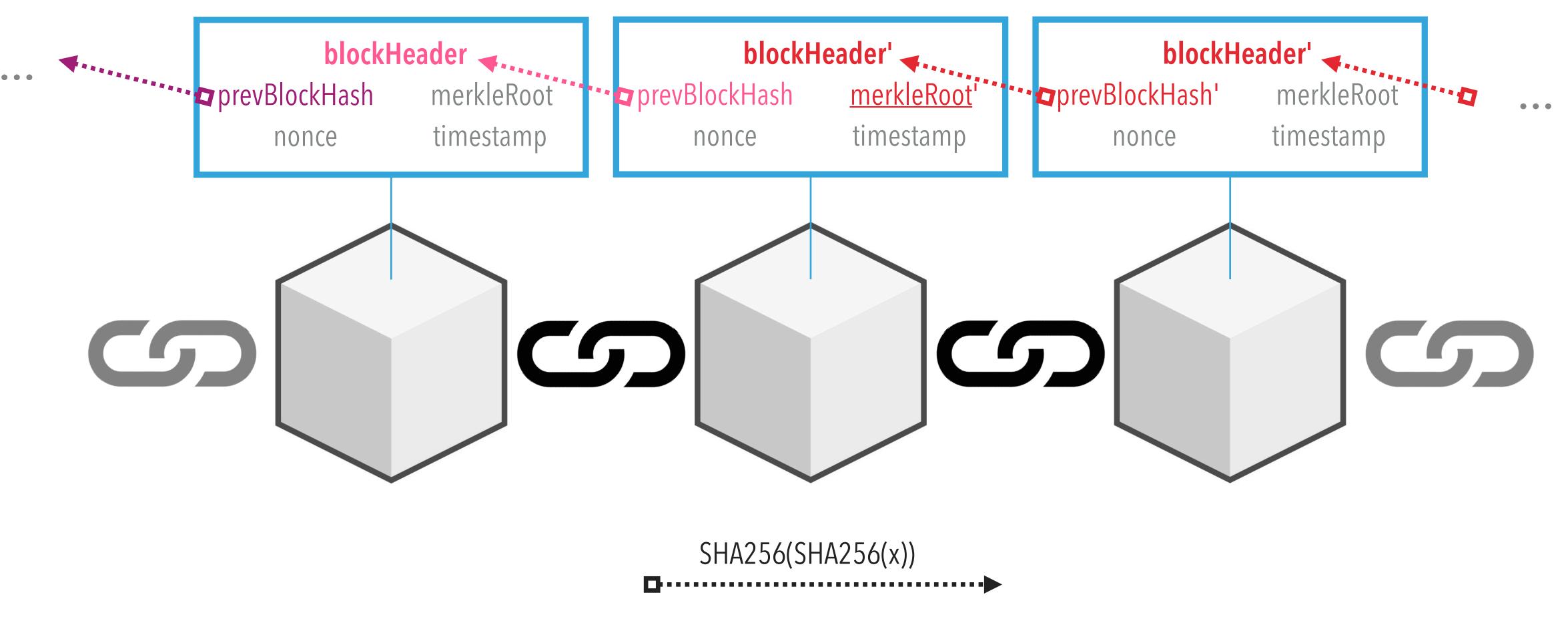
blockID = **H(blockHeader)** = H(prevBlockHash | merkleRoot | time | nonce | ...)



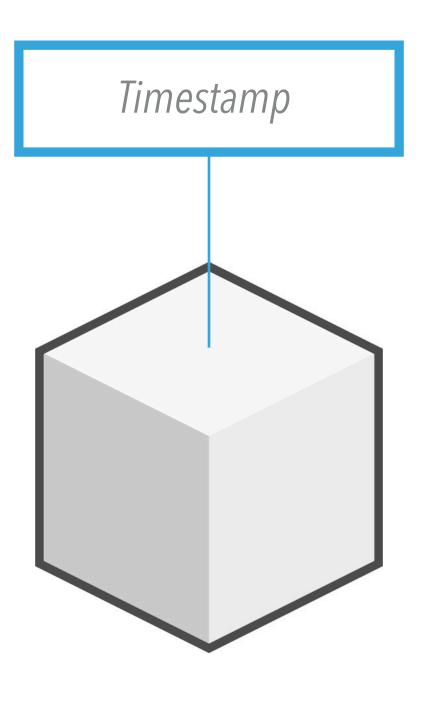
Bloco 123.456 do Bitcoin:

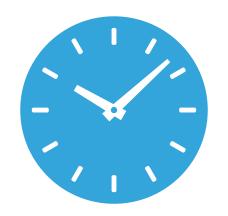


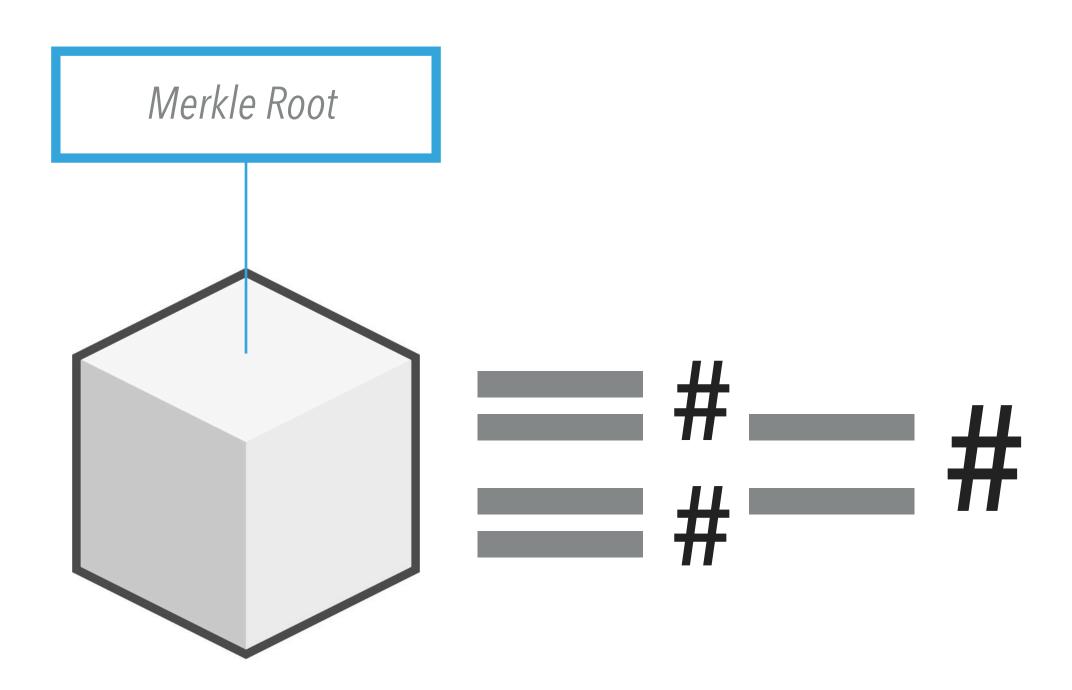
prevBlockHash = H(prevBlockHash | | merkleRoot | | time | | nonce)

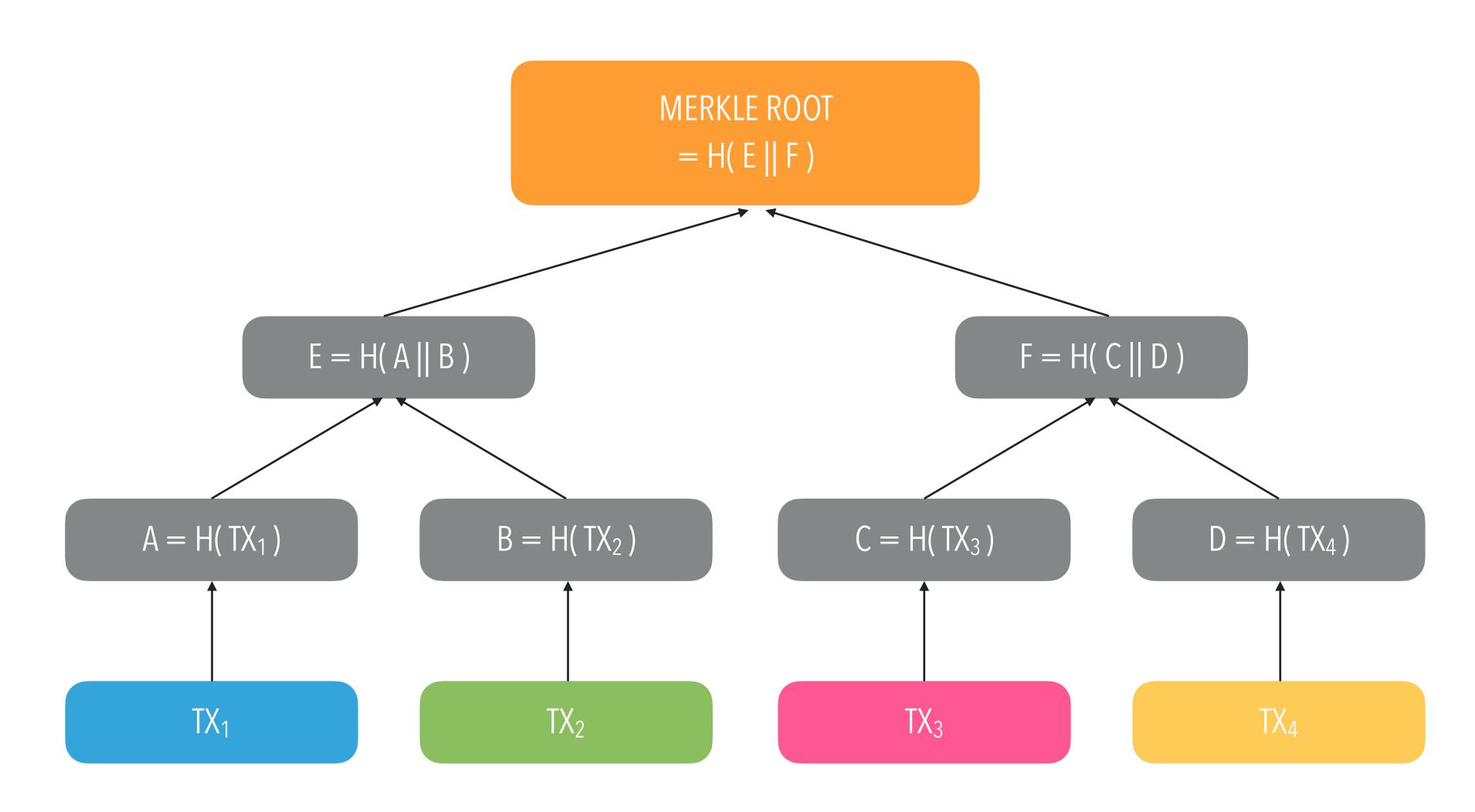


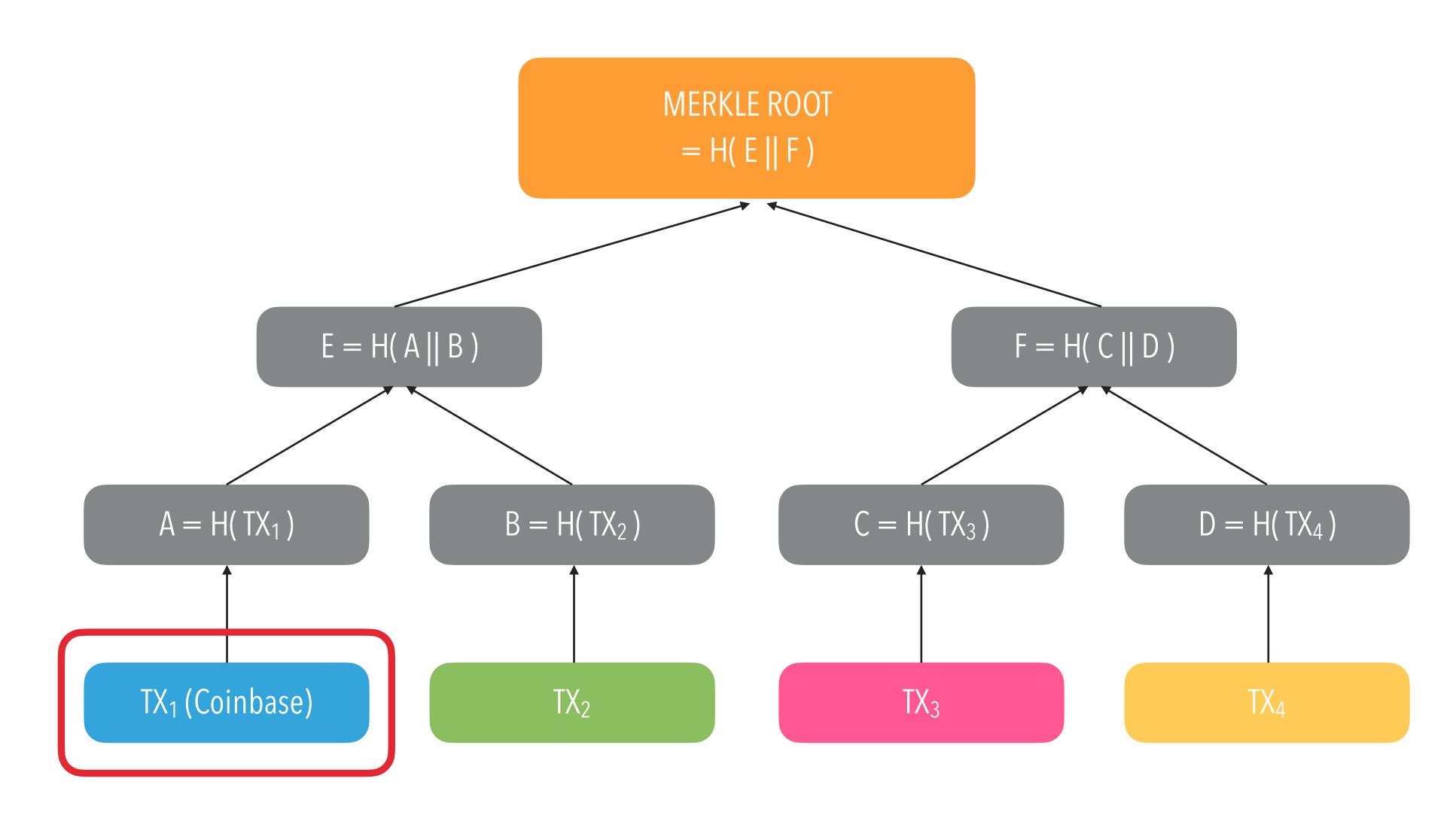
prevBlockHash = H(prevBlockHash | | merkleRoot | | time | | nonce)

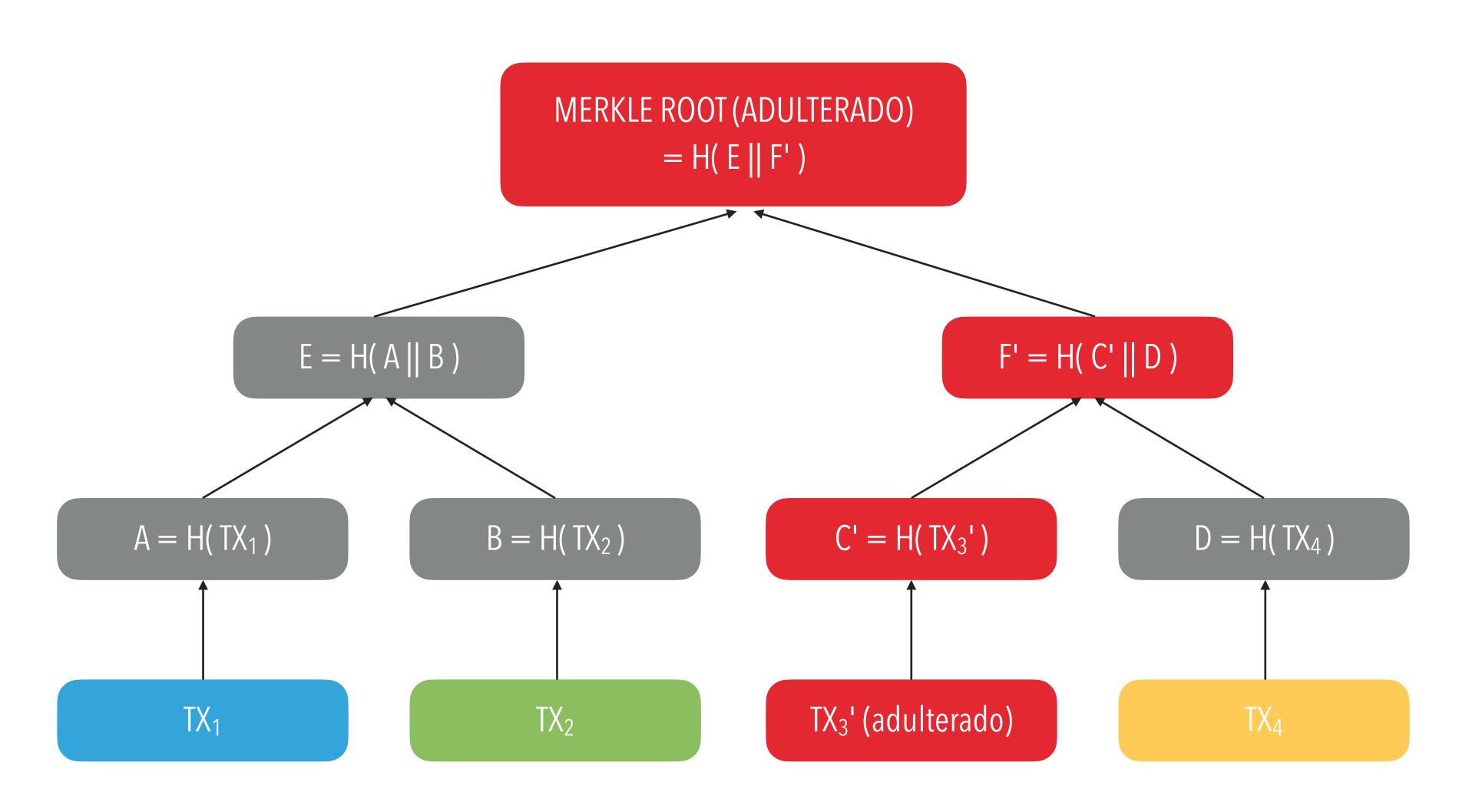




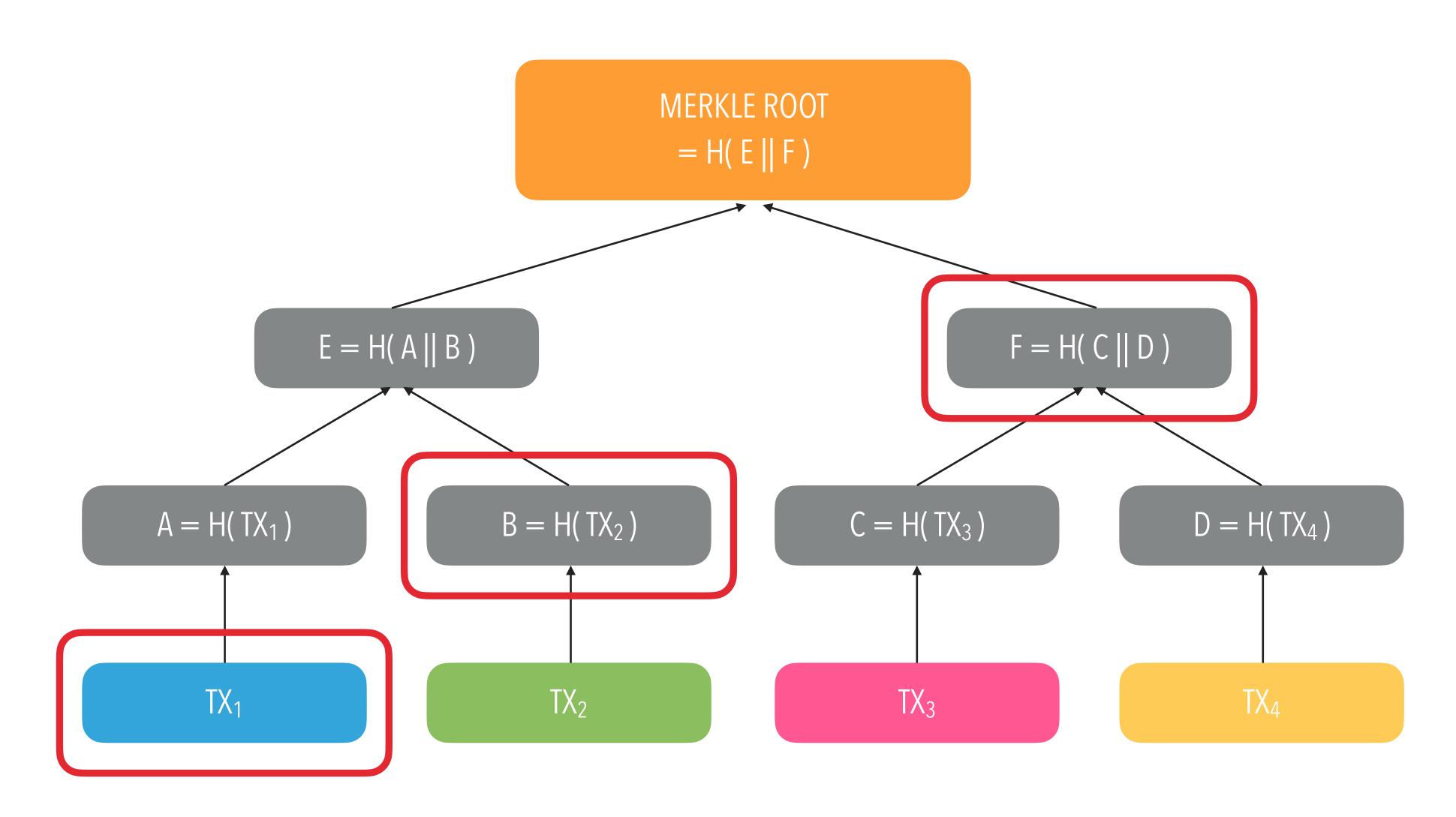


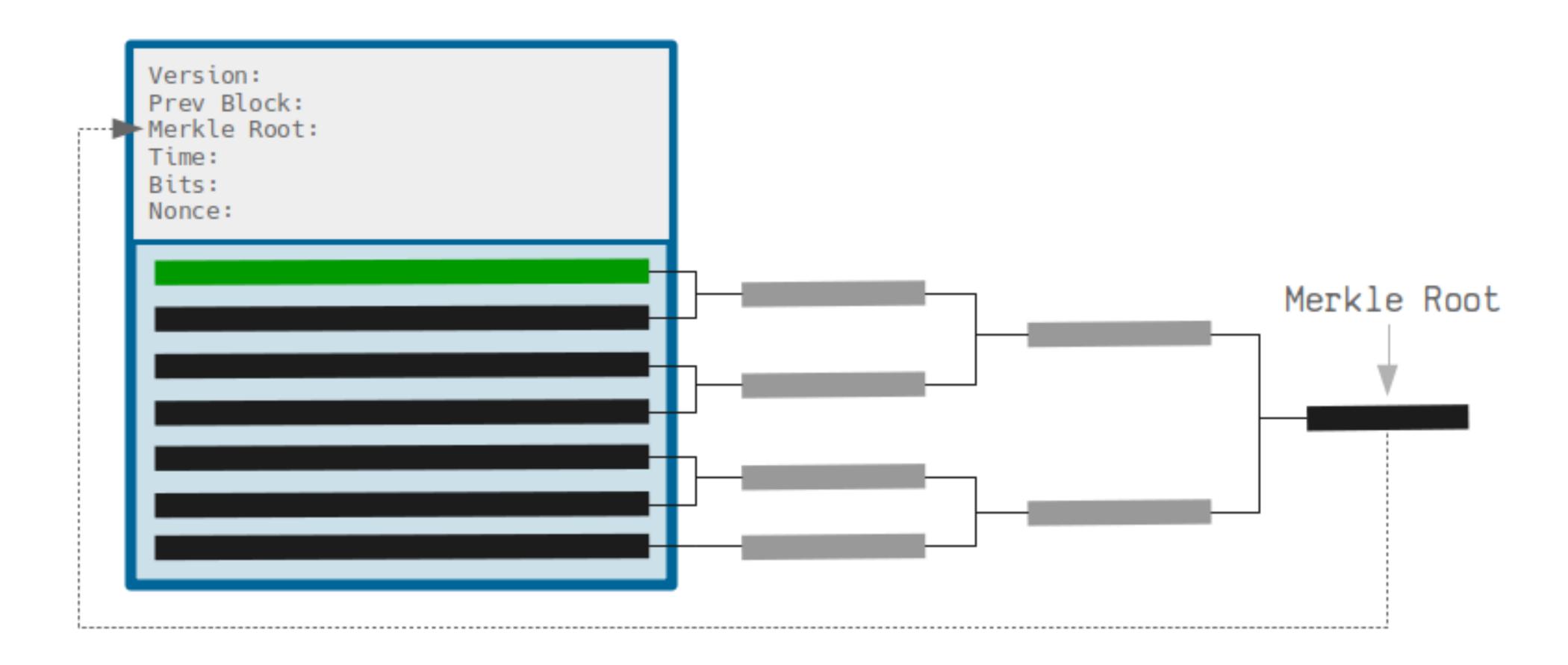


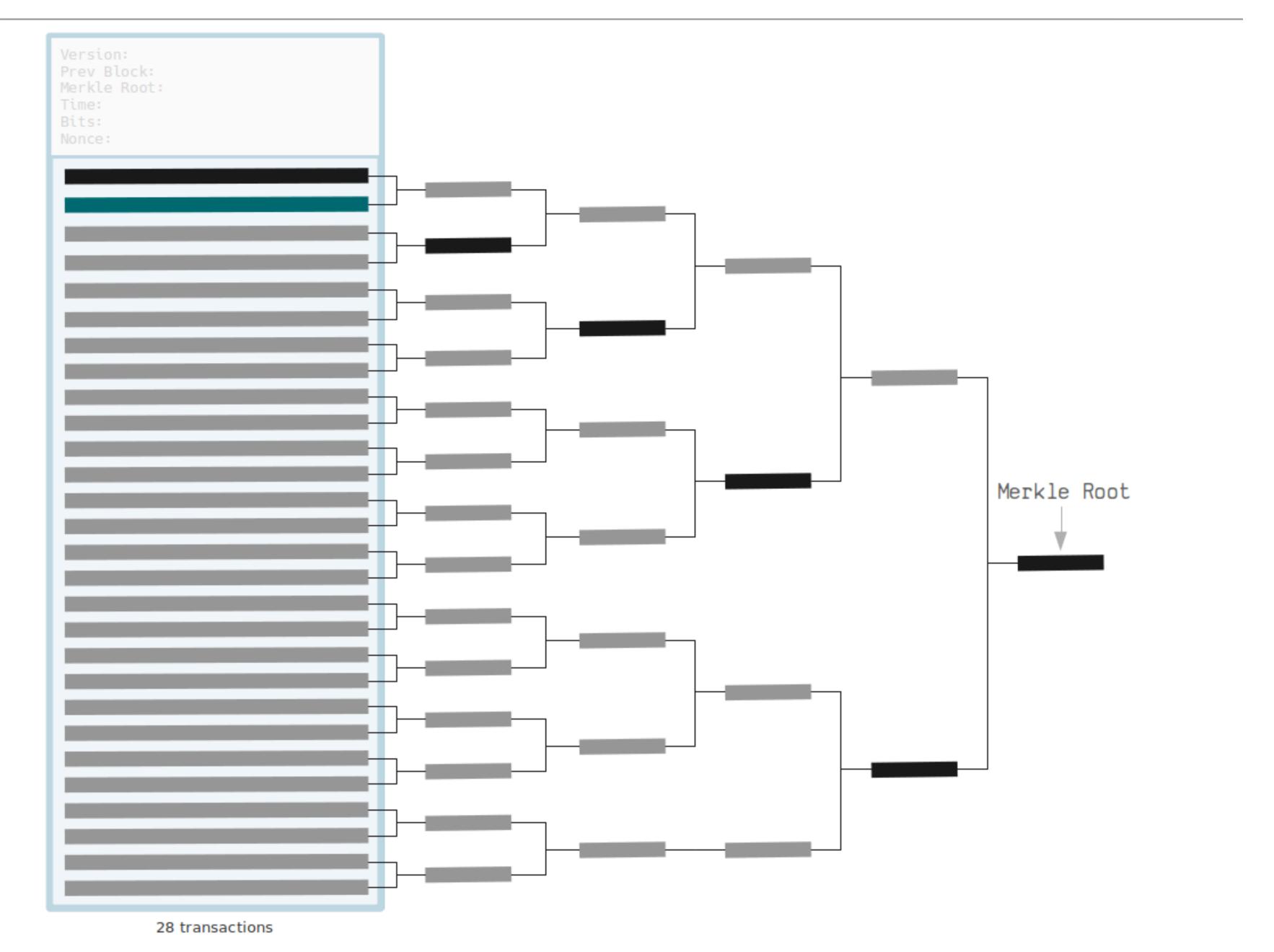


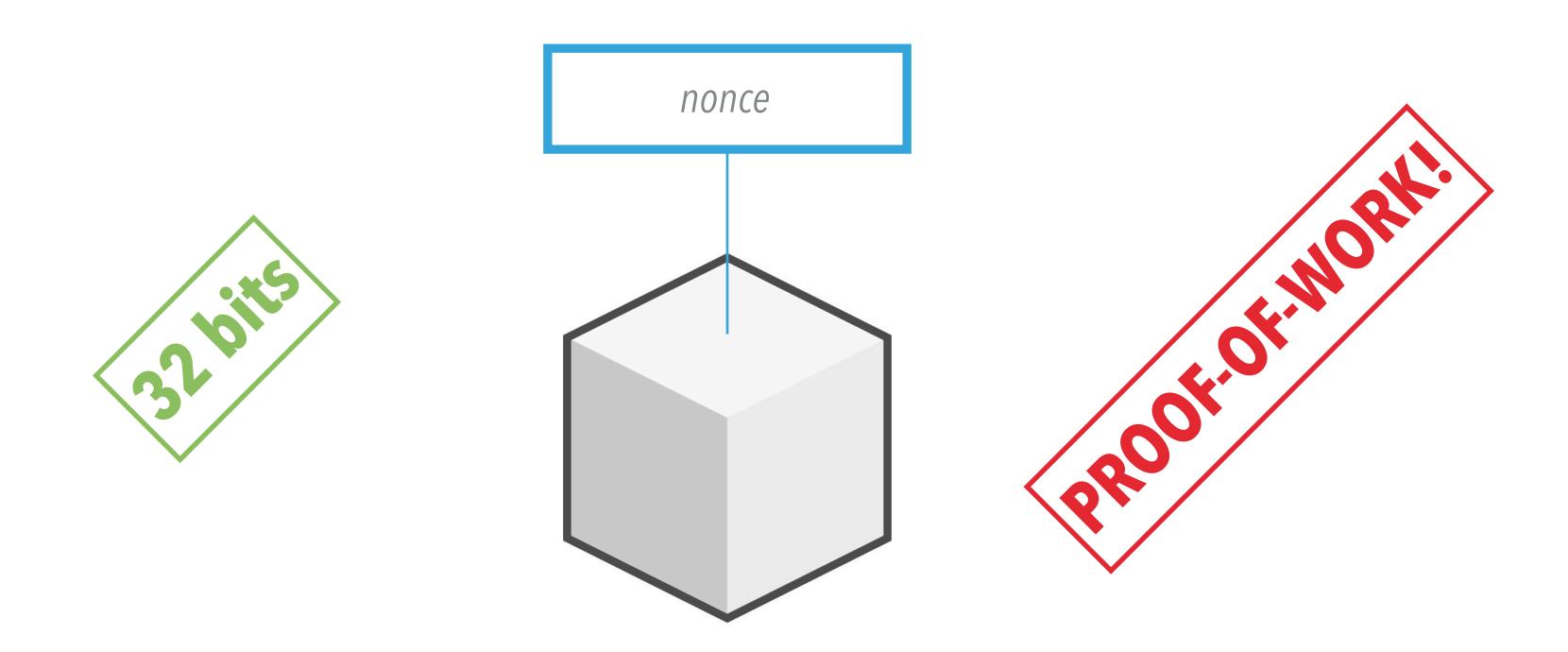


MERKLE ROOT E PROOF-OF-INCLUSION



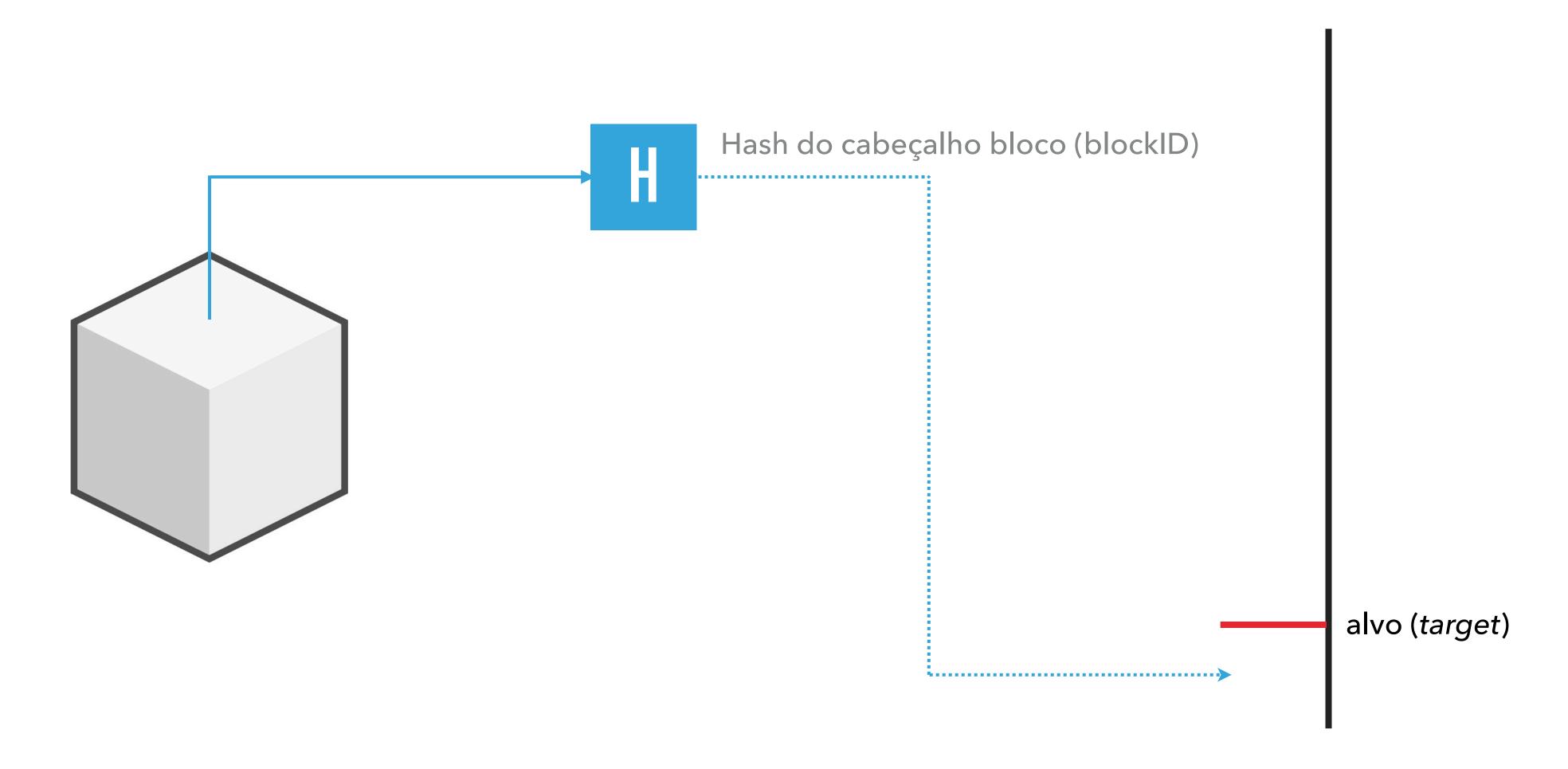


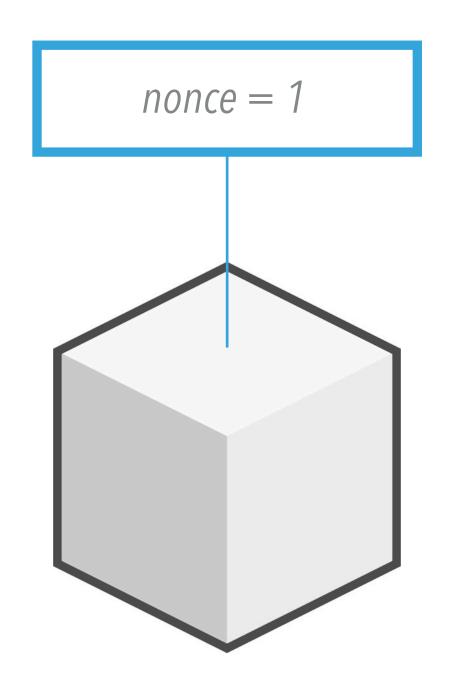




Enigma criptográfico hash: Encontrar um nonce que satisfaça a seguinte inequação:

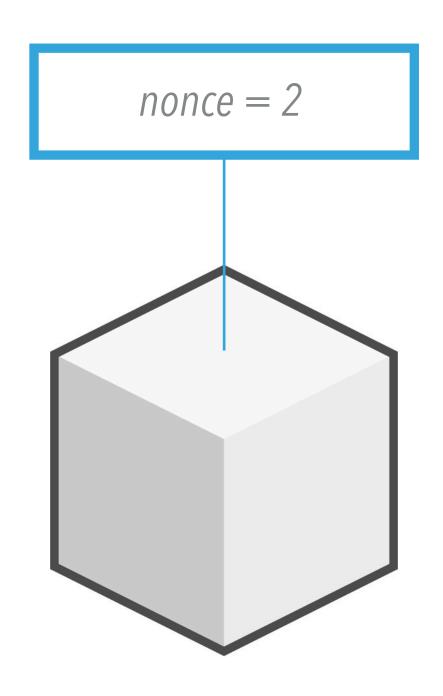
H(prevBlockHash | merkleRoot | time | nonce) < target





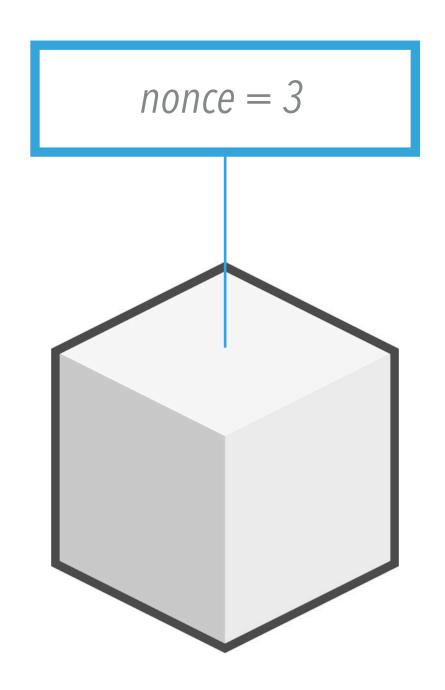
4c47c2d47712cc266c3b7ed7e9a0bcda2e6786f7455b9af3e9df3c5a2b26ddbf





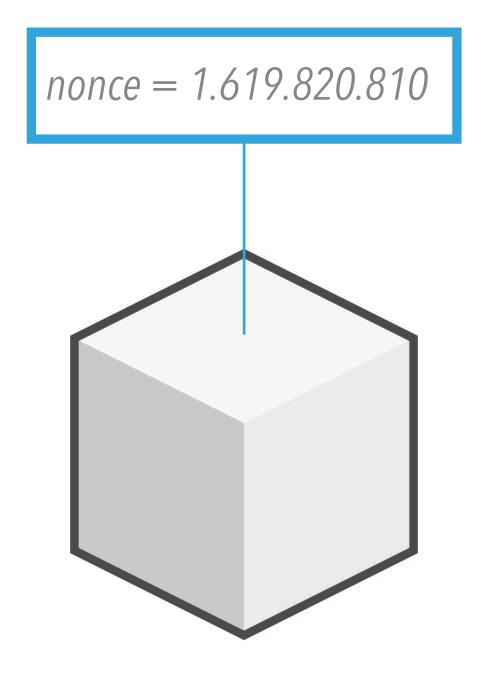
6bbe9136c059738eaaf237c995a78971788ee87119d82ef640a7288b43928017





000004bb7c4d63435e1fa5595986fab643490560699bf35c43bdc6ecfd3ea721

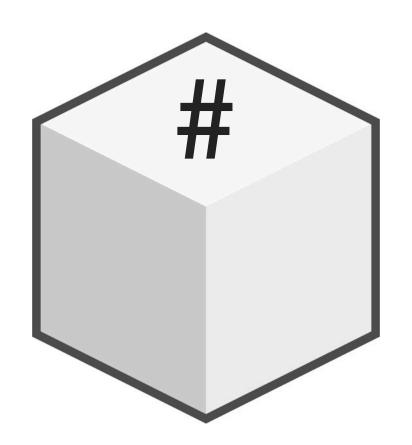




00000000000000000274cb1a04c382475310f70cee3776af06414f22f8337044



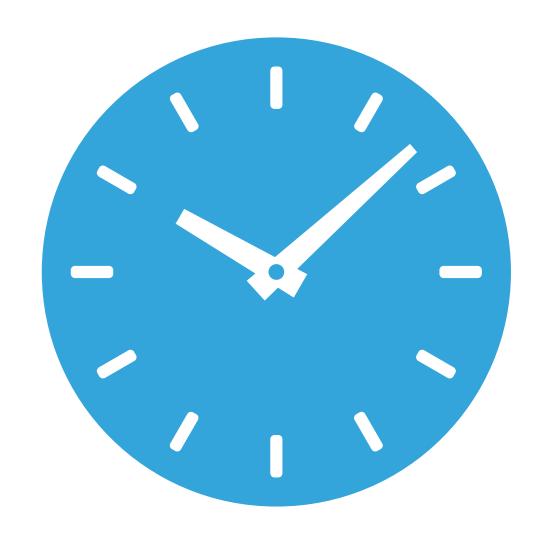
DIFICULDADE DE UM BLOCO

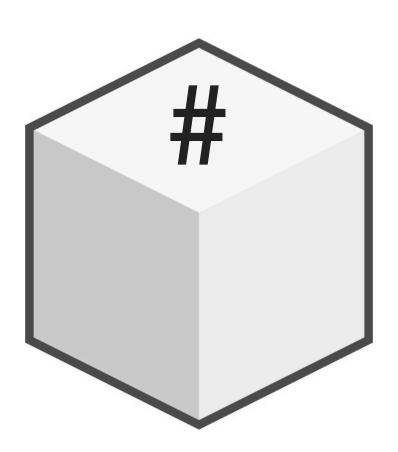


Dificuldade do bloco:

0000000HASHVALUE

DIFICULDADE DE UM BLOCO

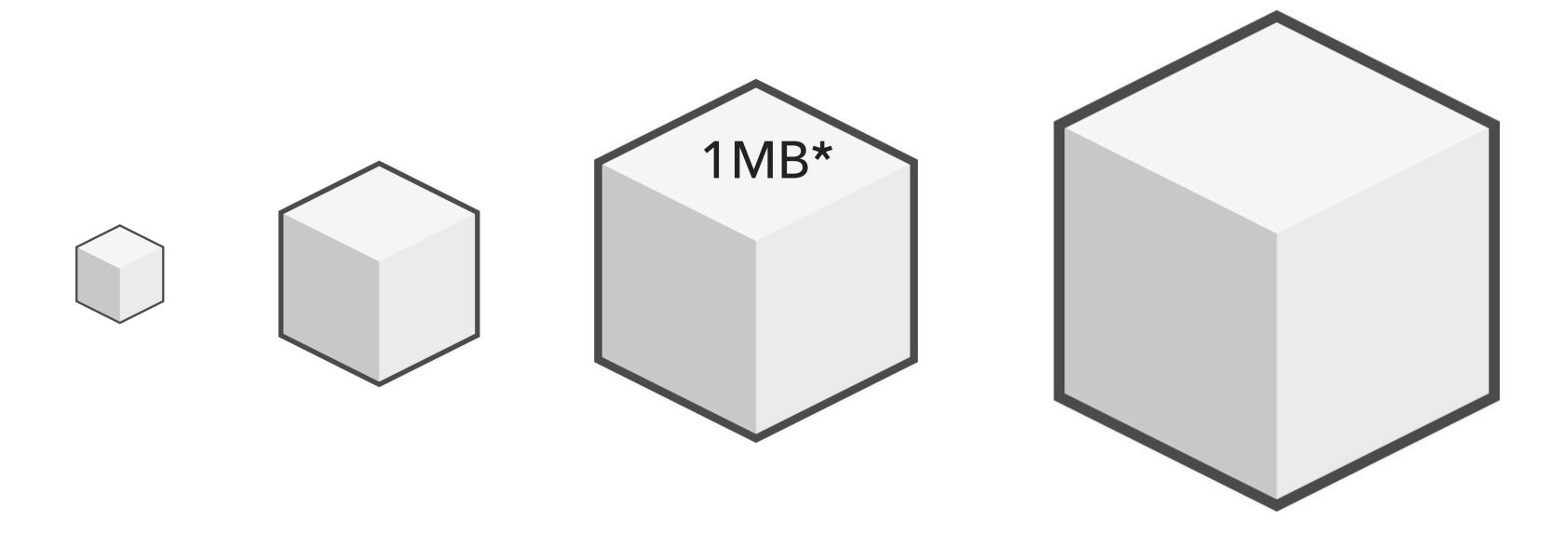




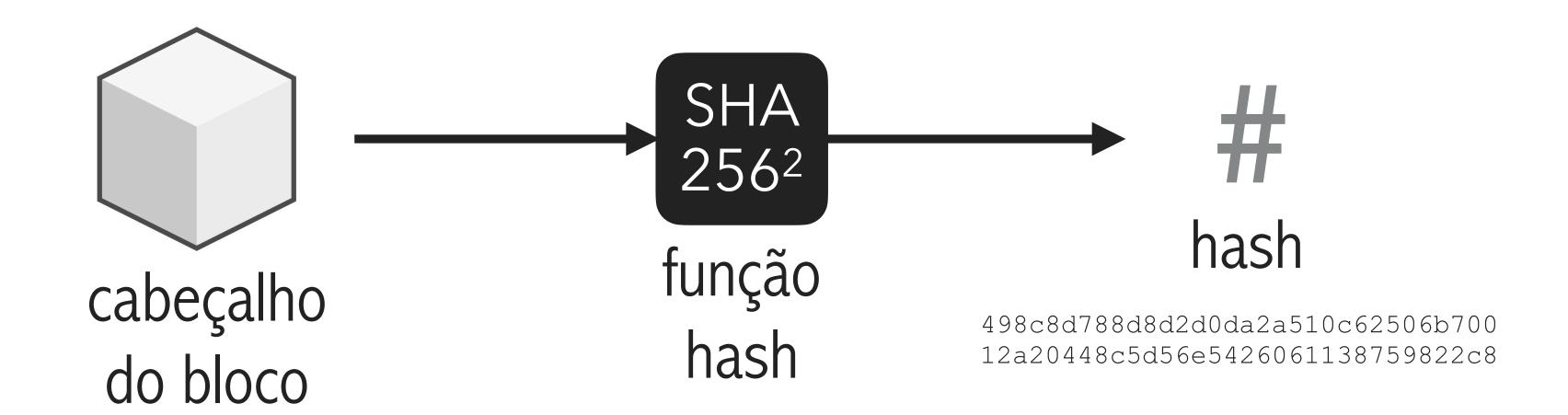
Dificuldade do bloco:

0000000HASHVALUE

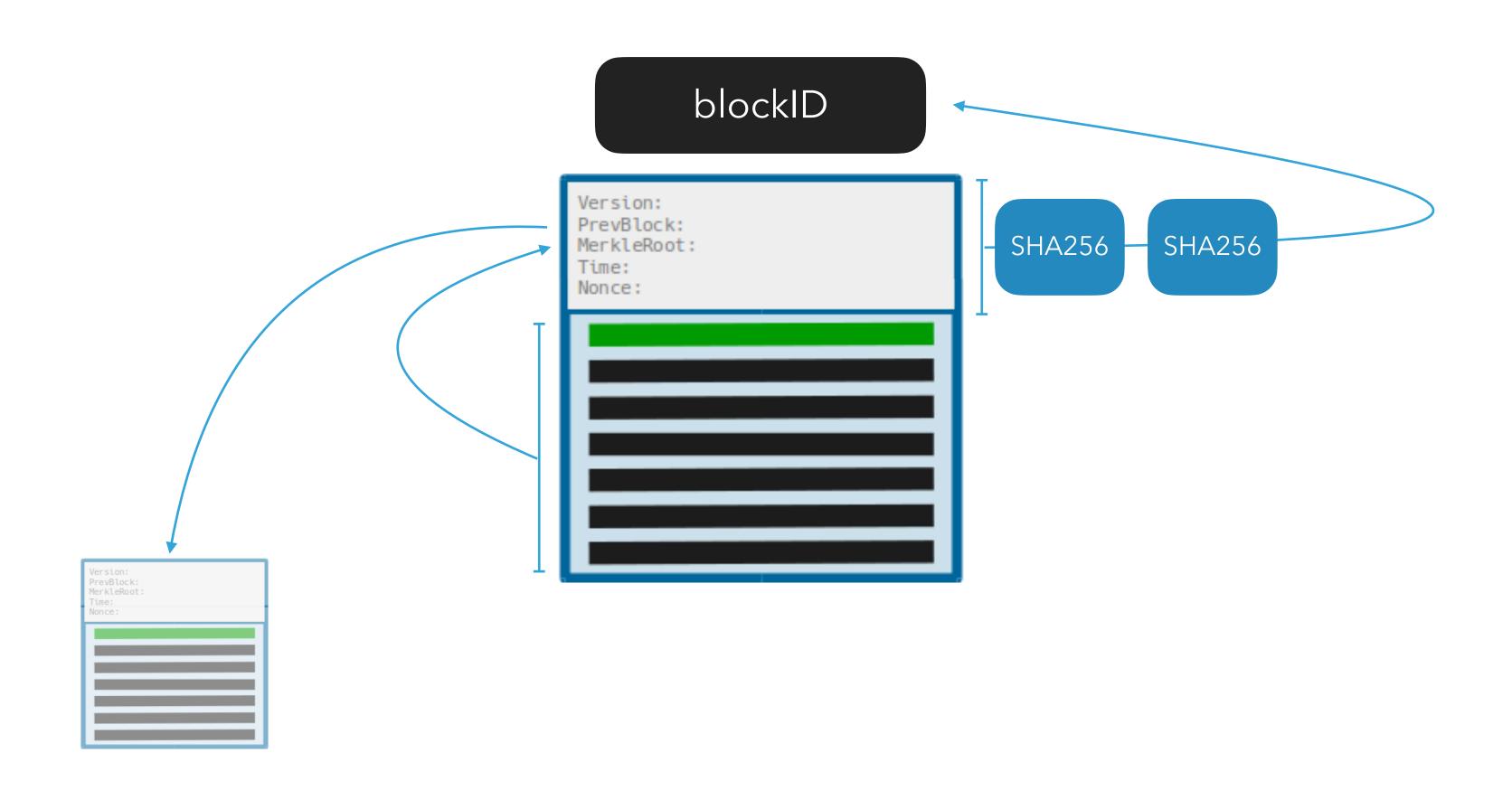
TAMANHO DE UM BLOCO (BITCOIN)



HASH DE UM BLOCO



ID DE UM BLOCO



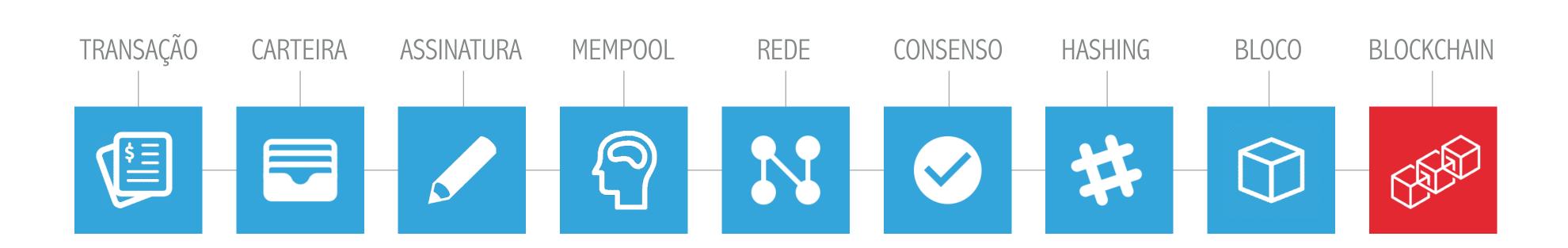
EXEMPLO - BLOCO #485963

https://www.blockchain.com/btc/block/0000000000000000000013942c4215cd92306bbce769cfcb349d0b42f031c994eb

BLOCO - DEMO

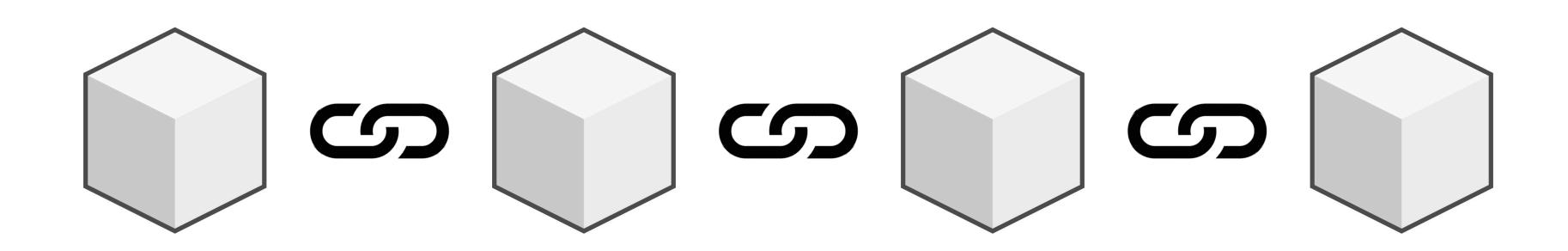
https://andersbrownworth.com/blockchain/block

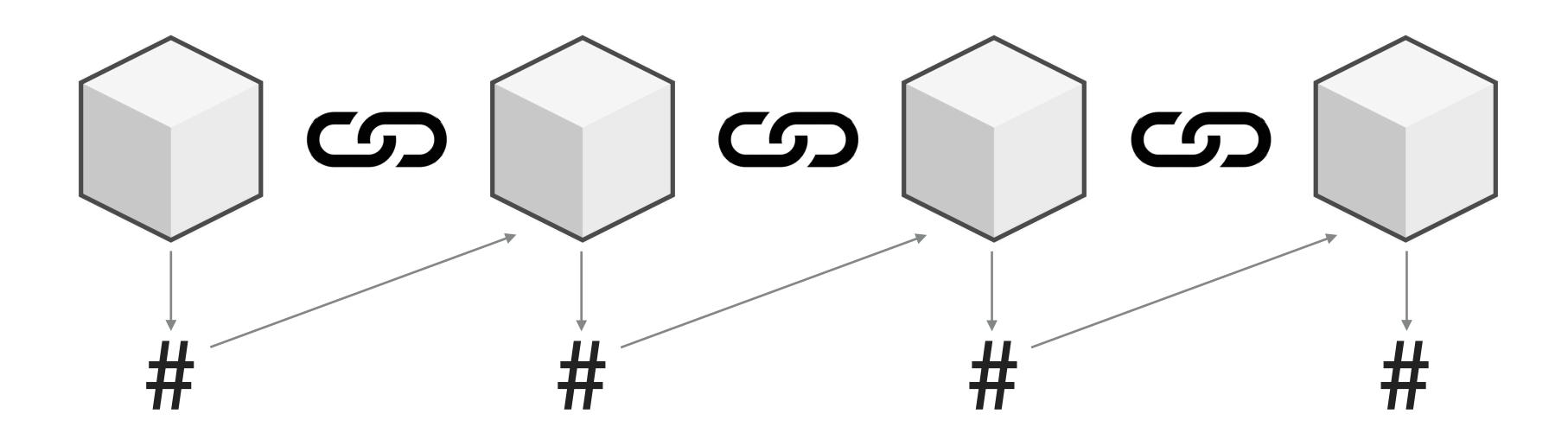
Arquitetura de um **Blockchain**

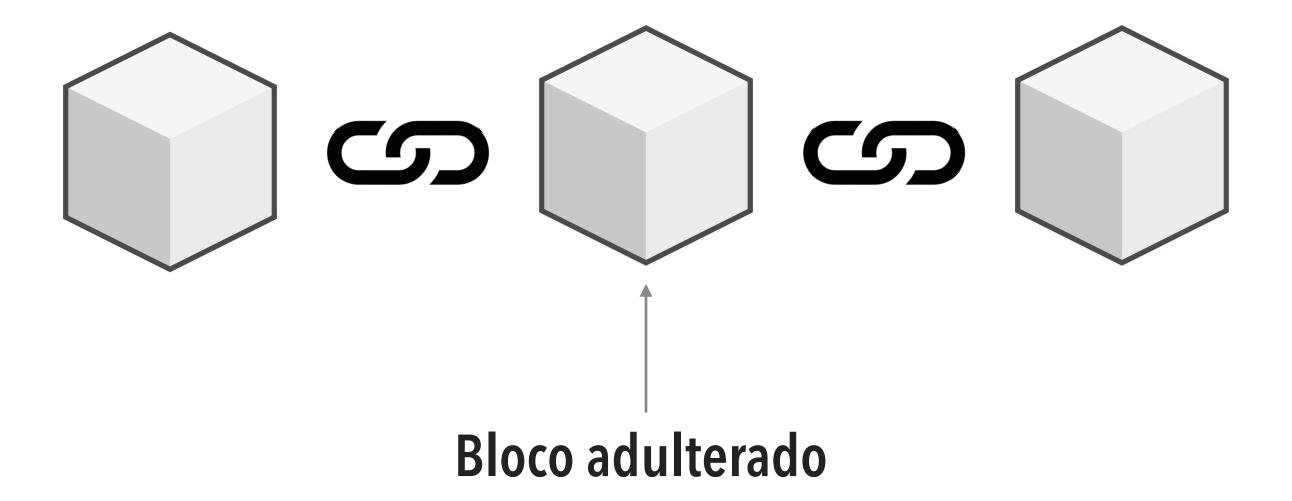


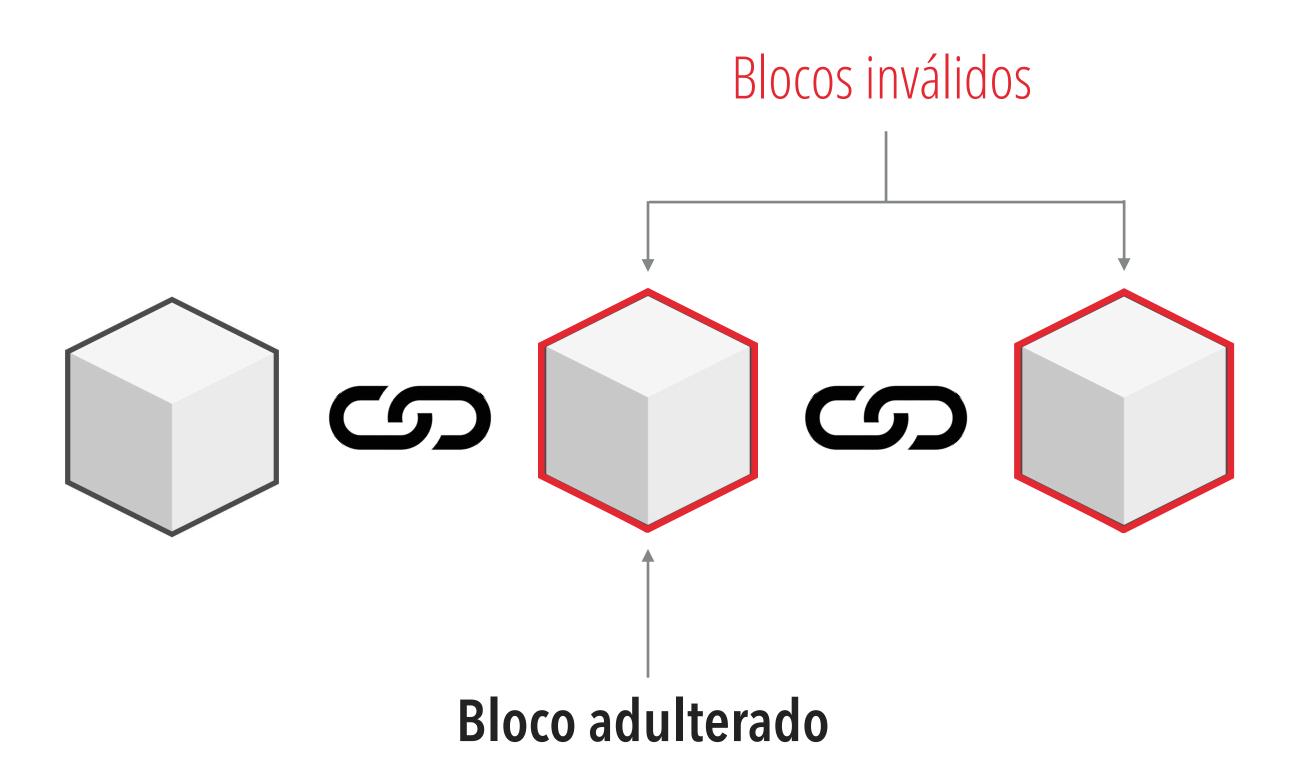
Blockchain

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

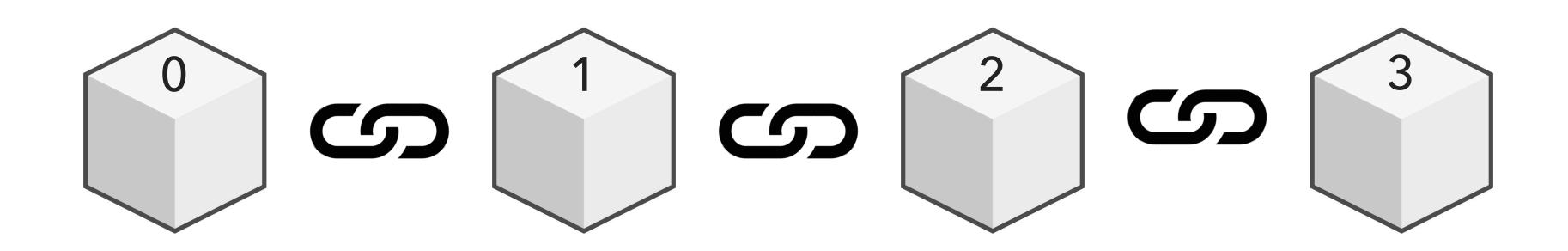




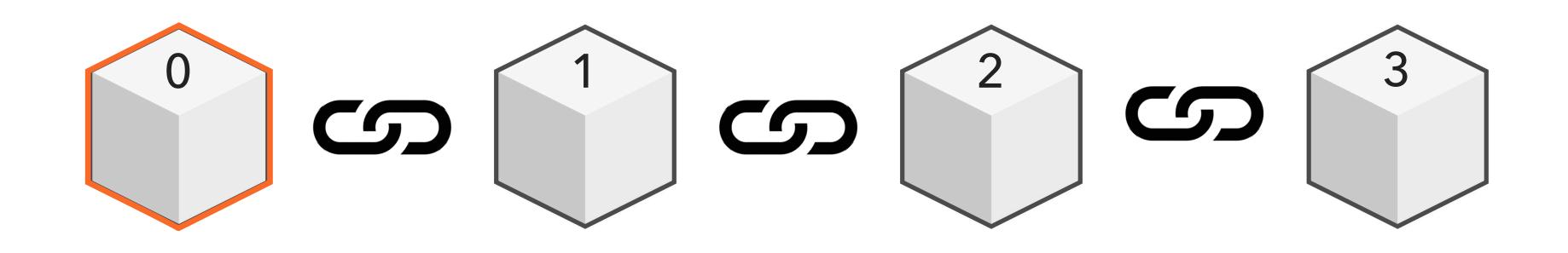




NÚMERO DO BLOCO

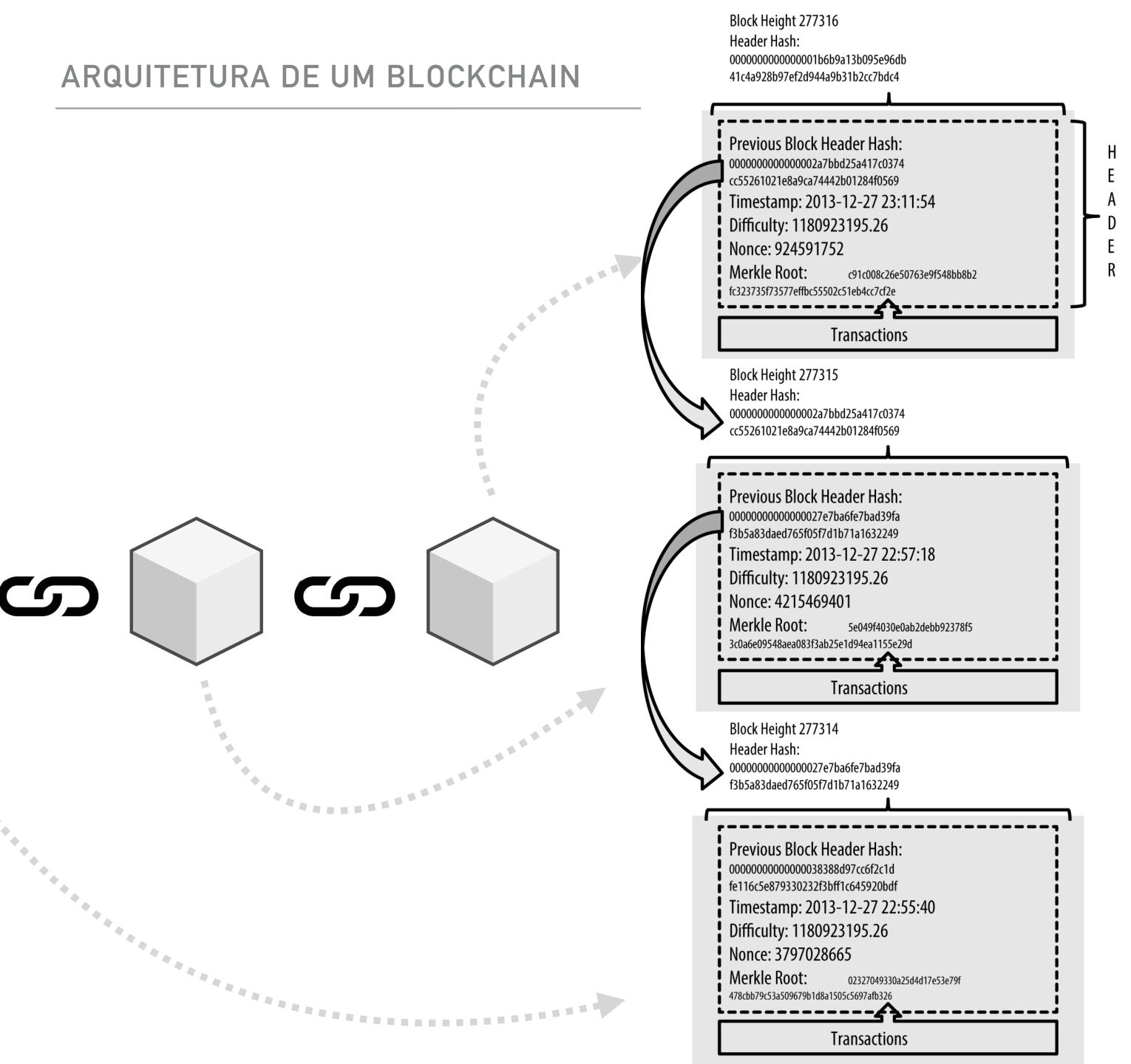


BLOCO GÊNESIS



ARQUITETURA DE UM BLOCKCHAIN

S



PROF. DANILO CURVELO

BLOCKCHAIN - DEMO

https://andersbrownworth.com/blockchain/blockchain

```
75603d0d8955ef040e5f68d5c36989efe21a59f4ef94a5cc95c99794a84492ac00000000000001000000001544bb26a50502ef11c745f1127b29a47856b3ecd9a1b6c540a66493d5fbf004601000000008b483045022100c9e35aa55af
5ac98cb67c4db7cf3d3f128753c4698f5d25ca0cdc3decd0c46be02204d6dfe89bd3fe88a32d47a44c0ab3ab60d87b27b90106f1b2f9f67c9c60cc80c01410449b8d933f97a8c4fe6ce962ee2abff8a81d8cfc5e0870a50cea7
6c50d04addf2df09331c4a47cdc3bc27a628e766ef5d01f28ee147ed21723b5ff3a62ed8da3effffff024094ef03010000001976a9146c8de651f8b92f87ff43fb9732babec784bdb6f588acc05d1626000000001976a9144
cb48ccf1b36a7f98d41f3f5f8db577f80220084df7afc2c912c3ef23ea43cfec651ba97ee6c4e4220c0f58b78f374626bdfb01410412aebcb2c5d5625c138c9cdd318ae04a103002b0d1b1541d72cd51dc016bfec885e7b93d7
3375903acb2731cdb7790b1d969db2684646e6fbeabb0559b6513c1ffffff024094ef03010000001976a914fa91e22c8a2a4d1fa592de1cf7aa8f958867a1d288acc05d1626000000001976a91452fc9e7e1b8be3a61fe203
81cb343e62eac105cb88ac0000000000000000015f71a19a74e9f5d202b9dd552471f2e8a24fd883a76f23455f1e4b738fd2c20f00000000000000006f858814dbf6a6d2dc71701028361a9e9ef2e2c52e5898f1bfcc
fad145ccda7022046973784a8de9007a52576070621c29e92f91a332960a5fb7ded81973d2e7be4014104dd2755d0a38af359659614530bd25e35fcb3d215b1fc41038beb495ea5db774e71a2f307652774b79c5dfa8fdccff3
72e61a27a177c6b157cc22beec361cc387ffffff020068890900000001976a91473b81e77969678ba046c79b44829f769ff2e00f188ac4066030100000001976a914597588d391674d08c2cfc35015db9487922aba5288a
c00000000010000001d1371f11cc10390fa0361f3e6b2e25e48c2f69040bf7d400d1b2ecf97b8461f000000008b483045022061c083b63887398f85a527c8e256ee3498bc50fa6bc85d90ebf63c49ad406836022100884ffd
73107b1129f378bfa29858d1e1c89f89922260a99a32a813572e3884460141044b32f0631083e1cc5f0401807abc7a12a715083297b86923675a8bf66bc6af0e82a184bed186896ce1059c9bb36e26b265536f4c9f181f570a5
3891ec9ba4a18fffffff02804f470c0000000001976a914afd883b5bd6ae5e88b39cc692db33a6ff7182dcb88ac00ca9a3b00000001976a9145539c2a8cee228ef366cb0e8f29e0079ce03874888ac00000000000000001b3
6bce13ff6be1d5bd81267f9a24b2636fae20e0a1a5ca6c469d1c0fbc56a1ef000000008a4730440220592616f1af3377a3cc7bc721745cf2657131759b35c40ae03820931062c061c802203fc4adb8d0da6bd4269f8331b2179
3304743015a735bcbb95298ad82595f40da014104dd182dfcc9eb893ea6a0f34cec5906fbb61008b6fd669b74414d2999bf49fd21f7eb775f6175234d79cf8b9d3ac749b2bb3673462cd94641bcf9e27fe2cfc08bfffffff02
9a225c16d8e94fca3cc0d3112761e5df11f33e20000000008c49304602210097f54a78861aa913ca1b76925107a26762d7405cfeaa19983a99fb61d99e5540022100ab1cd36486fb5598d67e15e9947f17d5dab53fdd013b0e9c
a8b8ffb2f7f40e9e014104b5f0dfe1370e364f516d25e1524ea5eb8cb8afe7e0f739576283ffbcd7b8307f0f79459d34ce8f6386bc725b730c26f4e5996029824e48baed2ad75d8b916fd3ffffffff7c945863dc4cdb9c2e160
e3653c8ab77a33b55f061df53507c0a406a07e33e5e010000008c493046022100e7eda51ba3eff04c1e5fdd93bf4397e0e652ce38c725b687554e1dccf562fdd80221009afa588cf5347cd7f50e4c097ffabe789a3c55235d8a
2fd639b21d2a73b50fb8014104a105201abcc58f7773fc5d7125344038b5ca77571173ac4b5741f9b11f8b360f4e88ac887f680af7fde035295939145d868011e0b37e077cc5e5aa2b699f6030ffffffff1b1887532137b5c7e
c5c141f5cb88dbf1465c578fb6491acc4d9ffade969bdbb010000008b4830450220630795aefe55d8be9111ee802841eae06a6b4aa6fa2356eb2d00142d93263465022100e9e1dc61dbaf1a3e4e57b84c8c515cdf7687ddf0e0
d7b04036105da6cfcb2845014104a105201abcc58f7773fc5d7125344038b5ca77571173ac4b5741f9b11f8b360f4e88ac887f680af7fde035295939145d868011e0b37e077cc5e5aa2b699f6030ffffffff0180b2e60e00000
6f4f8457e681710421c89e6577db1973485f11708ff062155bb34a3ef0e4
5f4640c940e441ff57442b982ca0b45ed4a55b622522022079de38e1baf58
                                                        c0dbe12938412bdd3cd7e0be71fa5b67eeca2b5b343aede45c014104
423f052c5d4eb548e79647cff8f2d272b3a8cfe9f34025bc90c60652bd41ebb2d57ffffffeec8c3317b0fb6c41a6d8332523f8ef4b74c98a963a1928ca9d280aa323d9dee010000008c4930460221008a34de93e3081bfb6e
41f79f591851895cf9cb354775966b00769f7ba9e5fc02022100a8778d15080a07721fadb4ec63229677fdc09ce919c10edf5b50de46c8199ee301410412581a35fdf35e291fc14119096a4e0c8e4f4ecf5c6ede7f727aae7d8
59aa1ac1ae3d5f777740998352dd76e46f777026f8b9e6a10a98bcd70c6b0ca25e3a7fbfffff02c0e1e40000000001976a914dba62e0fbc75a167491d075cbe916d4d95fb412e88ac00b4c404000000001976a9140a1d80
3e44f099d3c91d4b988d3c8a9fca5d4b5d88ac0000000000000000014395f5cf12900e99dd6192b6209b49b3450e566019ed408d99104dd200d41c590000000000000000045022100a4409279bcbae239067d4533ab66f60b814a7
c736e0e493138573f58733bbf1002204bed71dcb9c0e761d6c301c8358ed65081c60644a48efef6c37baf9729e6fc2701410432a325c210a4f9bb5d1522b81011a51bac208bba644eee54b2c9fbcbd748a53ca04f57acd052b2
47a1ace735c414958a3e1fded493f4128207e00ea058ceff87fffff024016750c000000001976a914cdc0d731b176c3aa8ba0ae0efdc27206afa08e7588acc0b060000000001976a914fc80396945a751a5dbc4b8ee682
993675e55533588ac00000000000000001c2ad61d37043de51542592378f2d0122d118ec78ebc4e9bb59e59a03d38432aa0000000008b48304502201837ae7e28ec87d59b44e3e86848762d827363d0164b02c62f108f9abc5f
c1d3022100fee05b2212e743bf8050fdd3e0cd19c8acba7fef1172678a909048a81fa18fbd014104ae588cbc9515b921f6f06e8fdcee9bb4276cfa3f7eee37afffcf3ac348e59323d959d720ffb0c4eb13cf8d8feebff39857a
f582181801f21bf13090c2d1fdb38fffffff6200e1f505000000001976a914cf1071894099f6ed178a9d3f8f736db0d9b8660b88ac4062b007000000001976a9144e60b49dcc9534d4700ab2bbea5880c221cab64488ac0000
00000100000003743c127e0cf6a849891792a6caec54cf4ef73681f423785c97d36aea27757fed00000008b48304502200f73796a8ef4f6b152485d2b5a81e6b077f50cc3535dbcd2e6bb4a72db6f1fb6022100ef9414edf55
3130a761380d85361301a3dd8747a6f26c454c3cd34b3e8a40b19014104da0b3696c878d3ef54b9b5ee21e2d6e1af534c5a8f6ab1cb7af342abd717aede2556b78813c02ccb98feb3bd4a88ff99e9e4c14f371caf9b4e175af1
9a70588dfffffff038ff9b434fd29a959006553c0af7e0bd60ab498c15b9cc5d5900859303bed48000000008b48304502210087beb550e5c32f1550c4d152bebb78fe95569f1bf0c6896bafef0d0e4cd1a6c902207a0449332
ee5f53ab5904b6e8849de39931350db8edb91ad0064f0d6d3f15b210141047aa5d5ba00d20563285e33599fb71af0657dd107c84bcdea3335ddac7b5b47f537a3a7c80ac22b295628cee7fb07938d85a440c17066a364480cc2
2679641671fffffffd4a590514aeace8e06d1bb2fb4ffc67a697d69d044d37f8f50c2c5dbc946b2ad010000008b483045022050d56ecf07775c47cc6937a8b87e45b6e37e22dabc421c91e62a776d727bb084022100fc93854
986173493926f1ab10958eec7c3ef6b040de91948848399fe66cb9a6d01410439c6bf25ca3de24d30353dc4a202670c4de1327fb5d3b56020bd76d51b17e4dac84001894904f2b426362b52f808901d8b2066d0eef6f753c834
105eeab9bf1affffff6240420f00000000001976a914328ea7ed3377be3c7fab0d09487309057a33f8c588ac8047a11900000001976a914c1773b304bb2f975623f01fa365fb55e86b340c488ac000000000100000001c20
a545d9df9f6b0f58eae2eec1cfe76ddb49d705a11dcb44a24cb464197e7e3010000008c493046022100b422fdc92aa6a86af349b826c033ecc2139ddf79ad7d215a0c00701cde4ce1d3022100a1017fc5c88b70900b56bbfb67
eb0f45e47a4b4d28f63674fc7dff7f6fb1328f0141043f6b33e5101c289c5c760cb35f77c43ab8f4f2ebce622b68f7105e166ee7ceb2d3a8562a094038452d702c0ddde1fd089bceb84c0eb8c4584d116c040c49f6b3fffffff
f02808d5b000000000001976a91420782923b21b1dd5b6b64d5069f7b01168288e0b88ac00e1f505000000001976a914ae214baa6cd56a0d50c9b60aea2352a56236207688ac00000000000016a0581837861fbce6253b8
e950eb606e0ba879bf9e6a5cd9cadb919fd376be38000000008a47304402206c7308a8fa8d45c082da032880270c10d436d2a4623ba6e13819d45eecf0f3b90220356f4e9855a101487b680d0b4e69b10c509015293236f2cfb
af9da6cb6791466014104cfd5868f564bae61bf22479e8d22e030fbdbf9a01a9a0b61ddfb580a9552b47b15f8a28e7c40b8fe73d6b9c0e0cdd1527266602b327dcc272bd8c1a33b87e4defffffff024864780000000001976
a914ceb552bdf23d002aed04c317c92cf8987e550df988ac40420f0000000001976a914586ce63c59b47a3ad08ccac6f132dc04ccbea0e288ac00000000
```

BLOCOS EM PYTHON

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

ATIVIDADE: BLOCOS

GitHub Classroom

./02-blocks/