MASTER BITCOIN

Chapter9 - Blockchain

Cheng Ting Tsai

2018.08.27

Items and Definition (1/2)

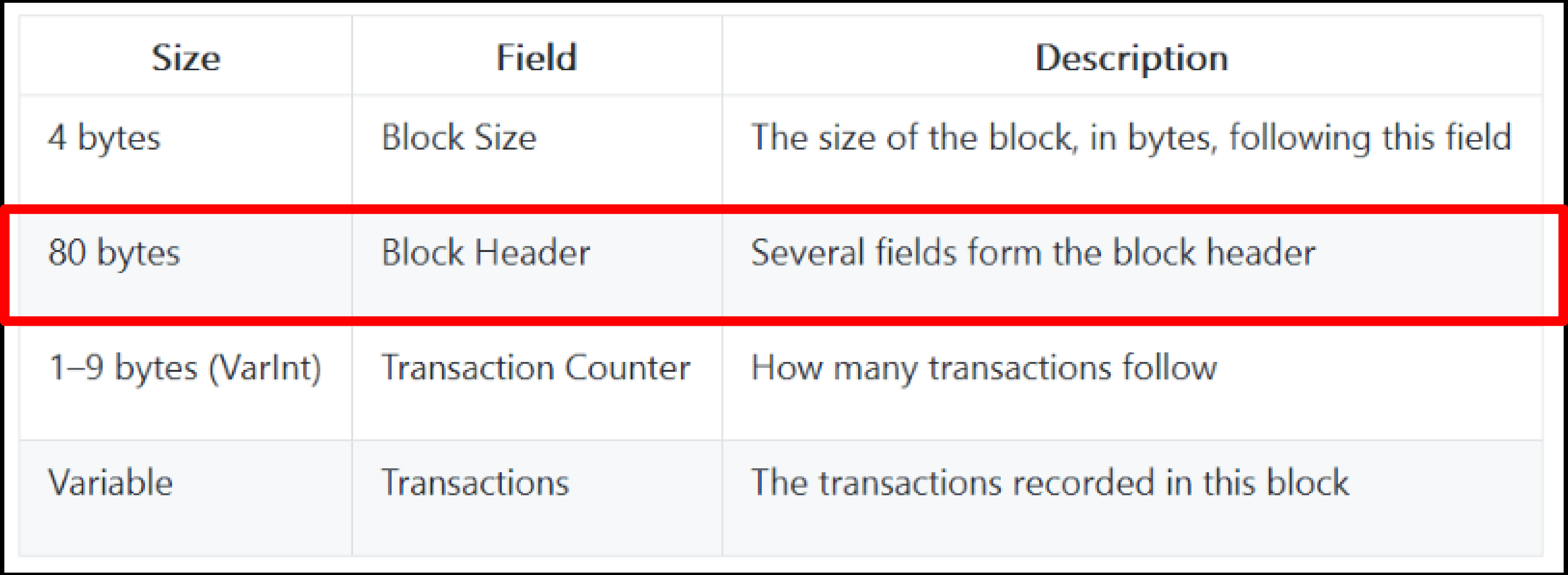
- **Chain Data:** Google LevelDB
- **Genesis Block:** The first block
- **Height:** Distance between a block and genesis block
- **Top:** New block added to the chain
- **Header:** Information of a block (see “*Header and Chain*”)
- **Parent Block:** Previous block
- **Child Block:** Next block

Items and Definition (2/2)

- Each block allows:
  - Multiple child block (Fork, Chapter10)
  - Only **one** parent block

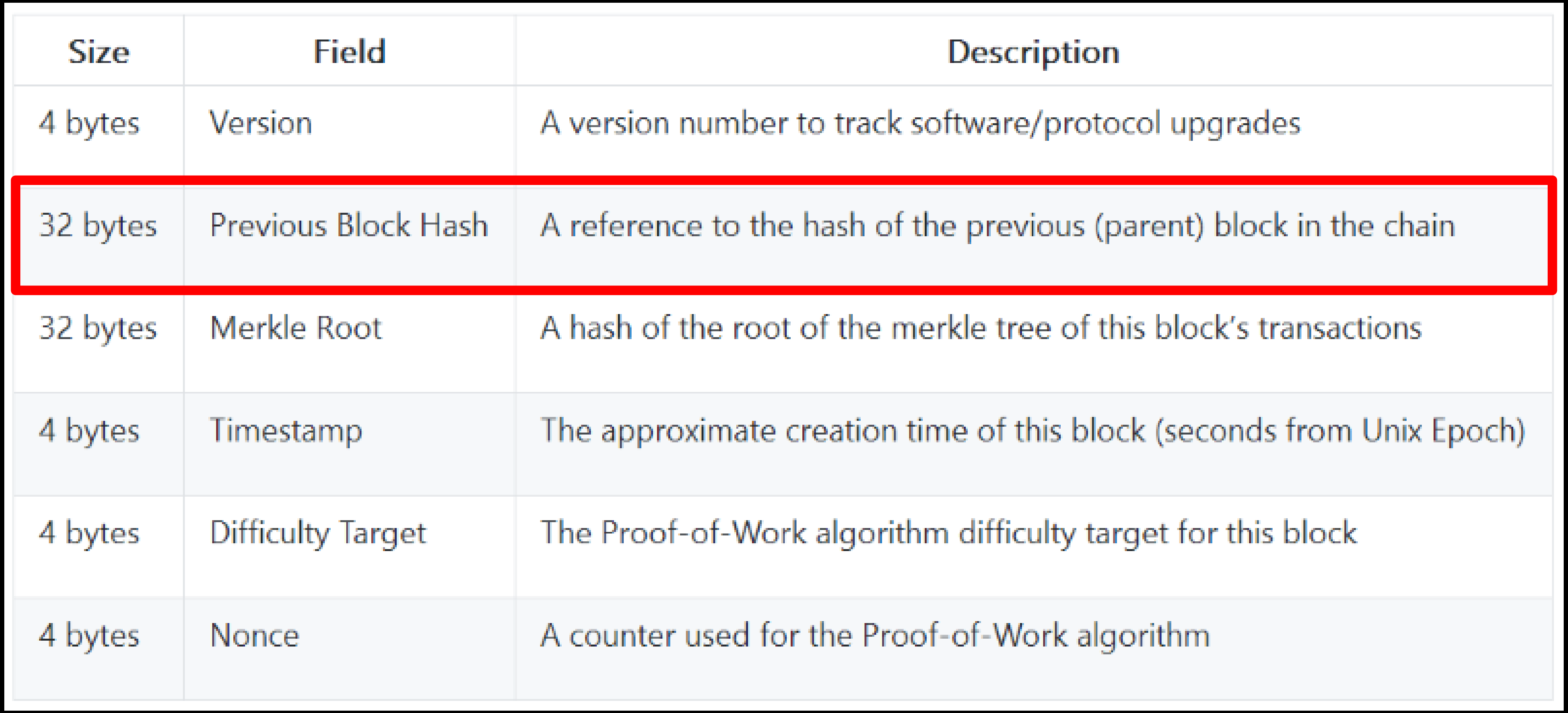
- Block Chain
  - Hash of parent block header
  - No hash conflict
  - A block with children is unchangeable

Structure



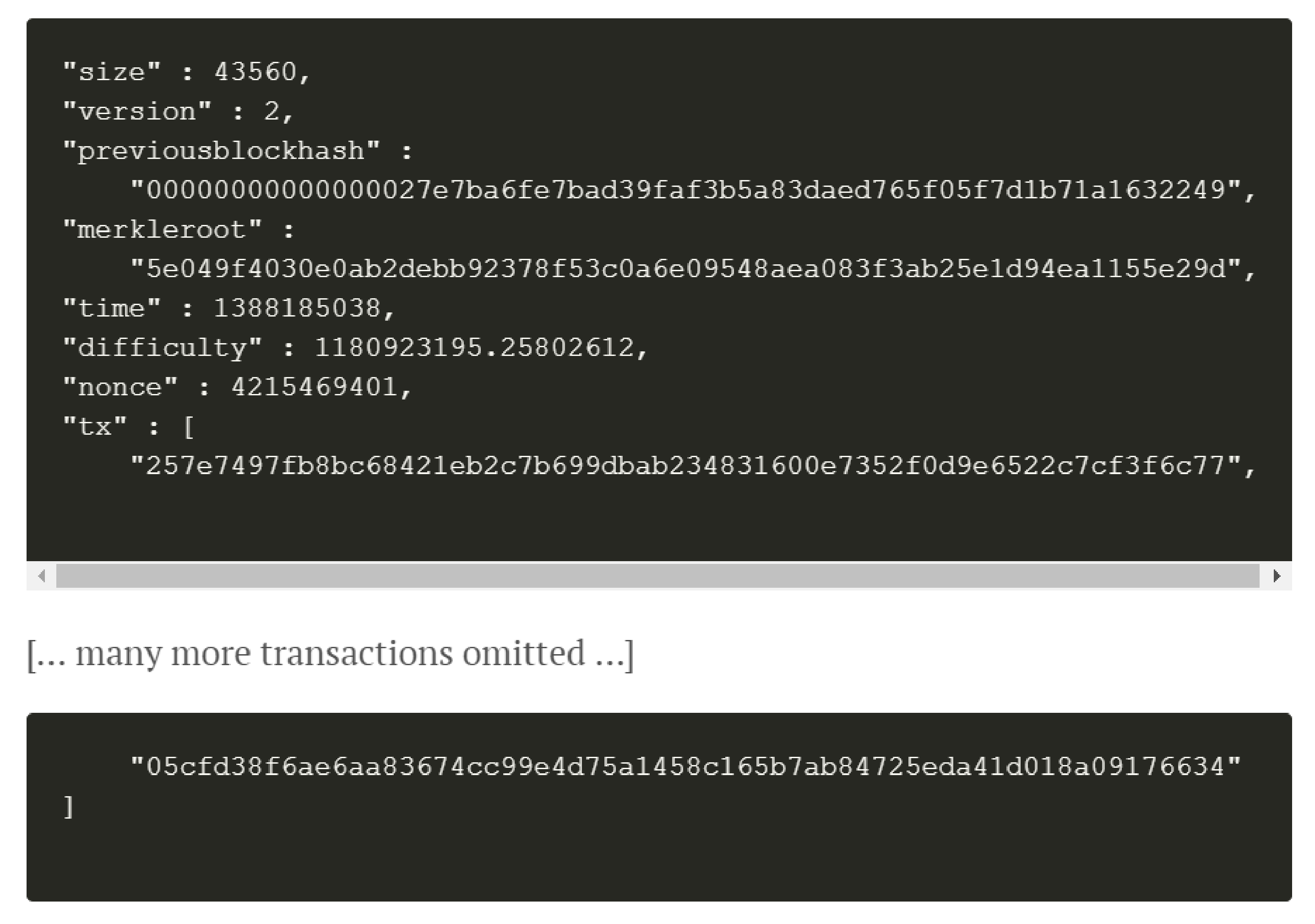
Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1–9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Header and Chain (1/3)



Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

Header and Chain (2/3)



```
"size" : 43560,
"version" : 2,
"previousblockhash" :
    "00000000000000027e7ba6fe7bad39faf3b5a83daed765f05f7d1b71a1632249",
"merkleroot" :
    "5e049f4030e0ab2debb92378f53c0a6e09548aea083f3ab25e1d94ea1155e29d",
"time" : 1388185038,
"difficulty" : 1180923195.25802612,
"nonce" : 4215469401,
"tx" : [
    "257e7497fb8bc68421eb2c7b699dbab234831600e7352f0d9e6522c7cf3f6c77",
```

[... many more transactions omitted ...]

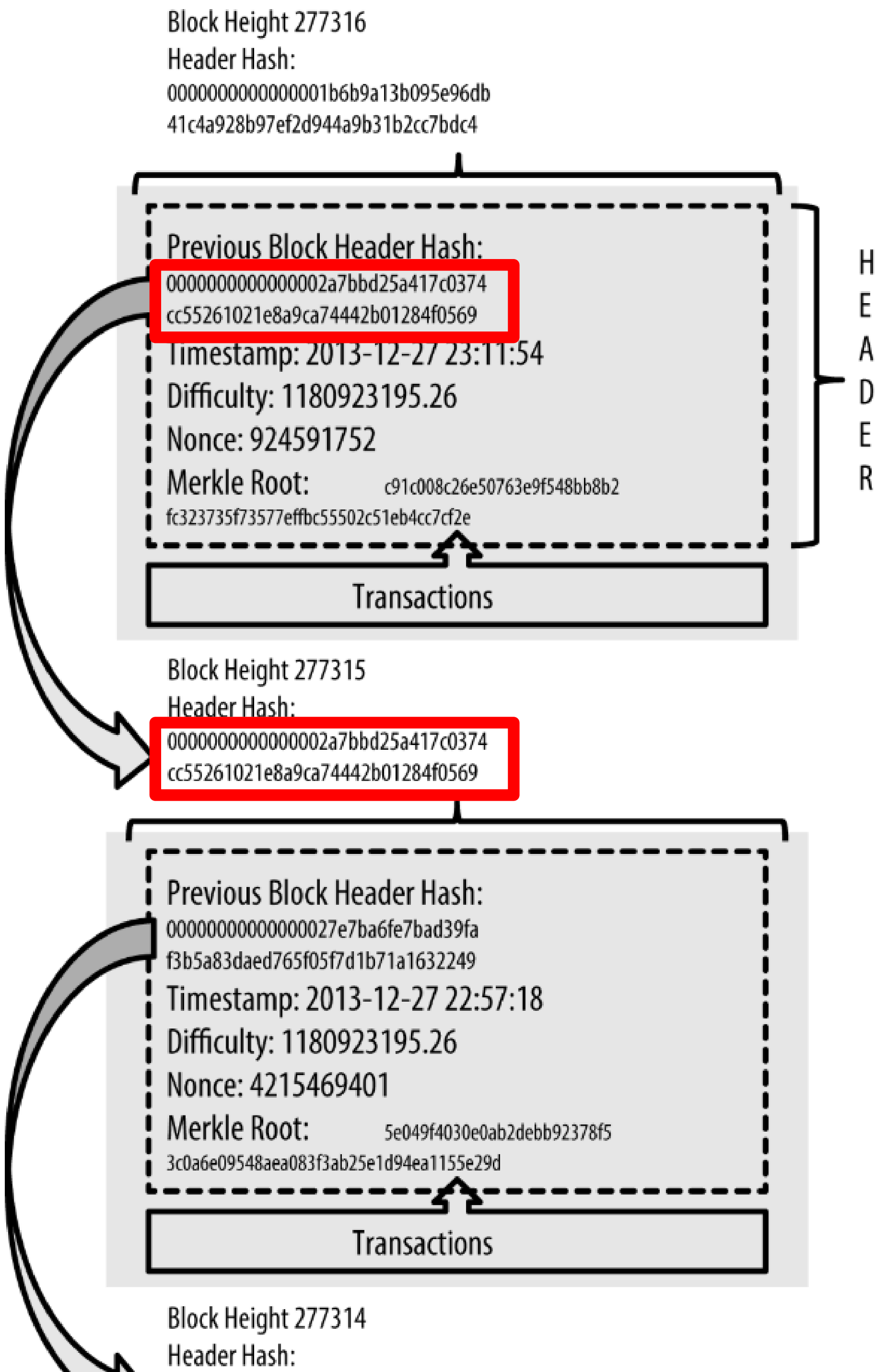
```
    "05cfd38f6ae6aa83674cc99e4d75a1458c165b7ab84725eda41d018a09176634"
]
```

Header and Chain (3/3)

- Block hash = hash of block header

- Previous block hash
  - Hash of Parent block header

- **Assume no hash confliction**
  - Same header can be made iif same information is given
    - Parent block
    - Current block



Block Height 277316
Header Hash:
0000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4

Previous Block Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Timestamp: 2013-12-27 23:11:54
Difficulty: 1180923195.26
Nonce: 924591752
Merkle Root: c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e

Transactions

Block Height 277315
Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

Previous Block Header Hash:
00000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
Timestamp: 2013-12-27 22:57:18
Difficulty: 1180923195.26
Nonce: 4215469401
Merkle Root: 5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d

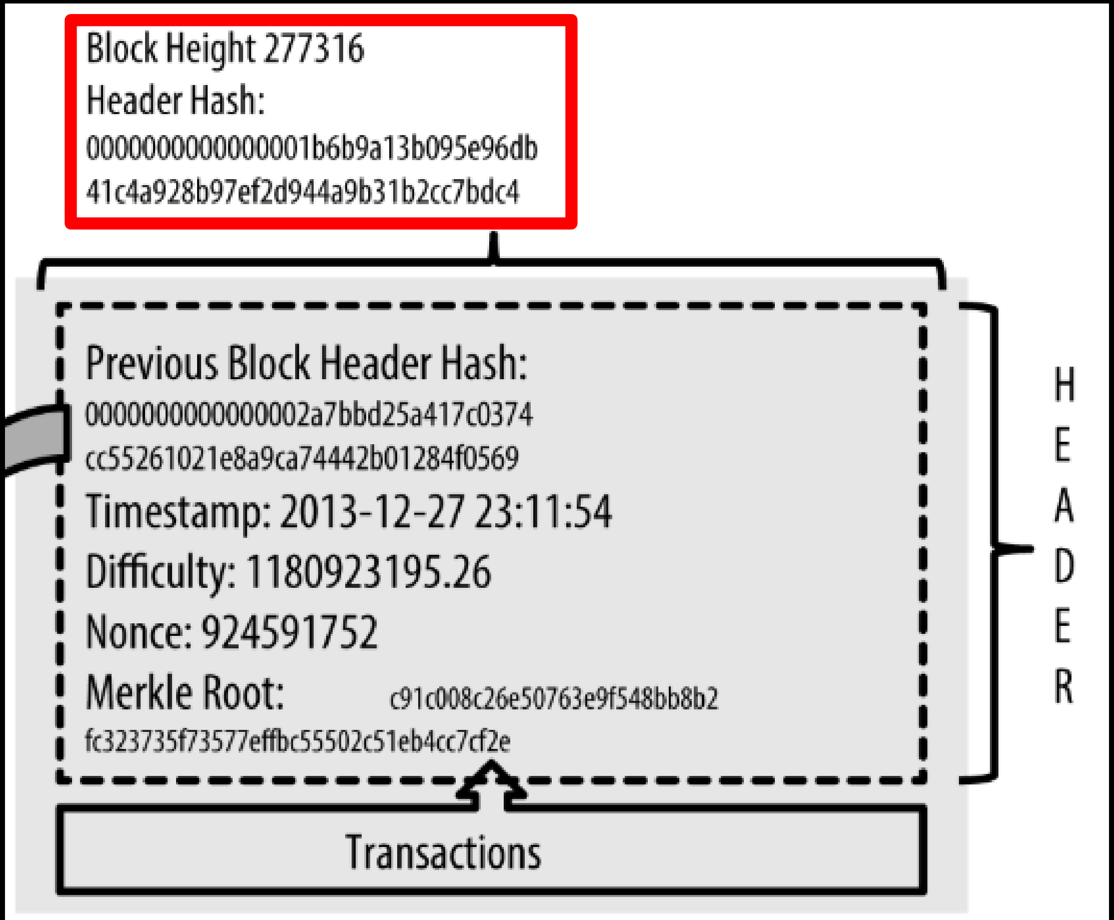
Transactions

Block Height 277314
Header Hash:

Block ID

- Block Hash (Block Header Hash)
  - Hash of block header

- Block Height
  - The order of the block in chain



Block Height 277316
Header Hash:
0000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4

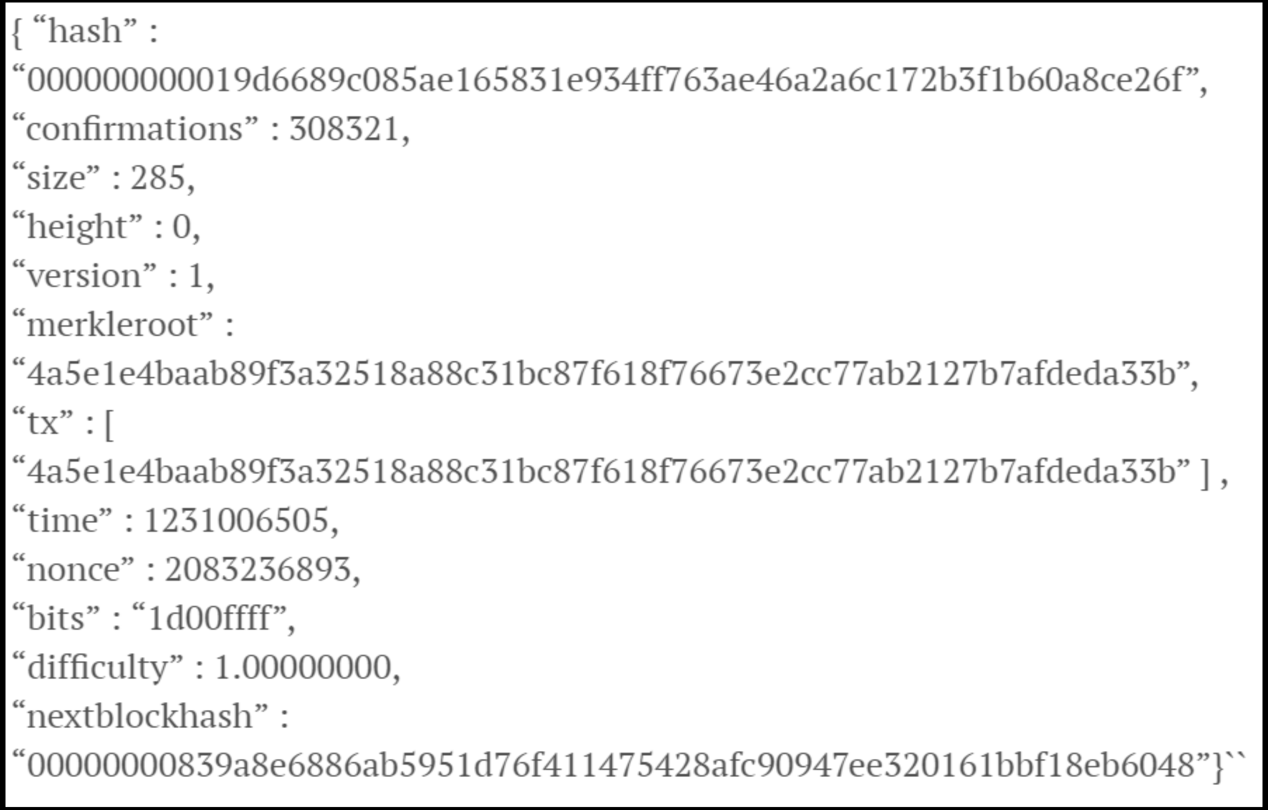
Previous Block Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Timestamp: 2013-12-27 23:11:54
Difficulty: 1180923195.26
Nonce: 924591752
Merkle Root: c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e

Transactions

Genesis Block

- First block in chain
  - Height: 0

- Every node
  - Has the same Genesis Block



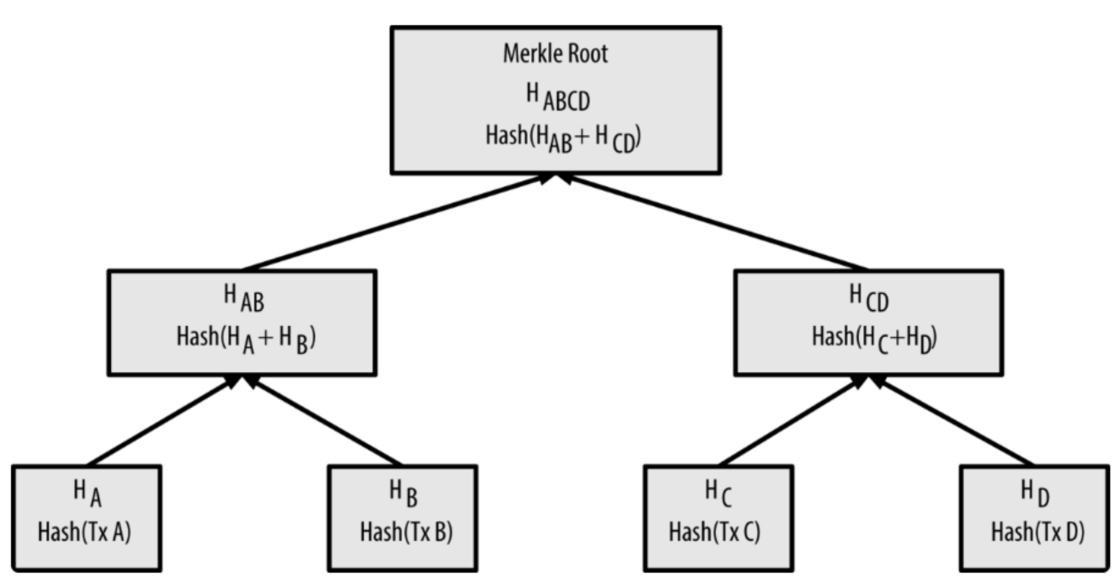
```
{ “hash” :
“000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f”,
“confirmations” : 308321,
“size” : 285,
“height” : 0,
“version” : 1,
“merkleroot” :
“4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b”,
“tx” : [
“4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b” ] ,
“time” : 1231006505,
“nonce” : 2083236893,
“bits” : “1d00ffff”,
“difficulty” : 1.00000000,
“nextblockhash” :
“00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048”}``
```

- The input of Coinbase in Genesis Block
  - *The Times 03/Jan/2009 Chancellor on brink of second bailout forbanks.*

Merkle Tree (1/7)

- Structure: Binary Search Tree (BST)

- Store transactions (tx)
- Increase search efficiency
- Verify existence of transactions

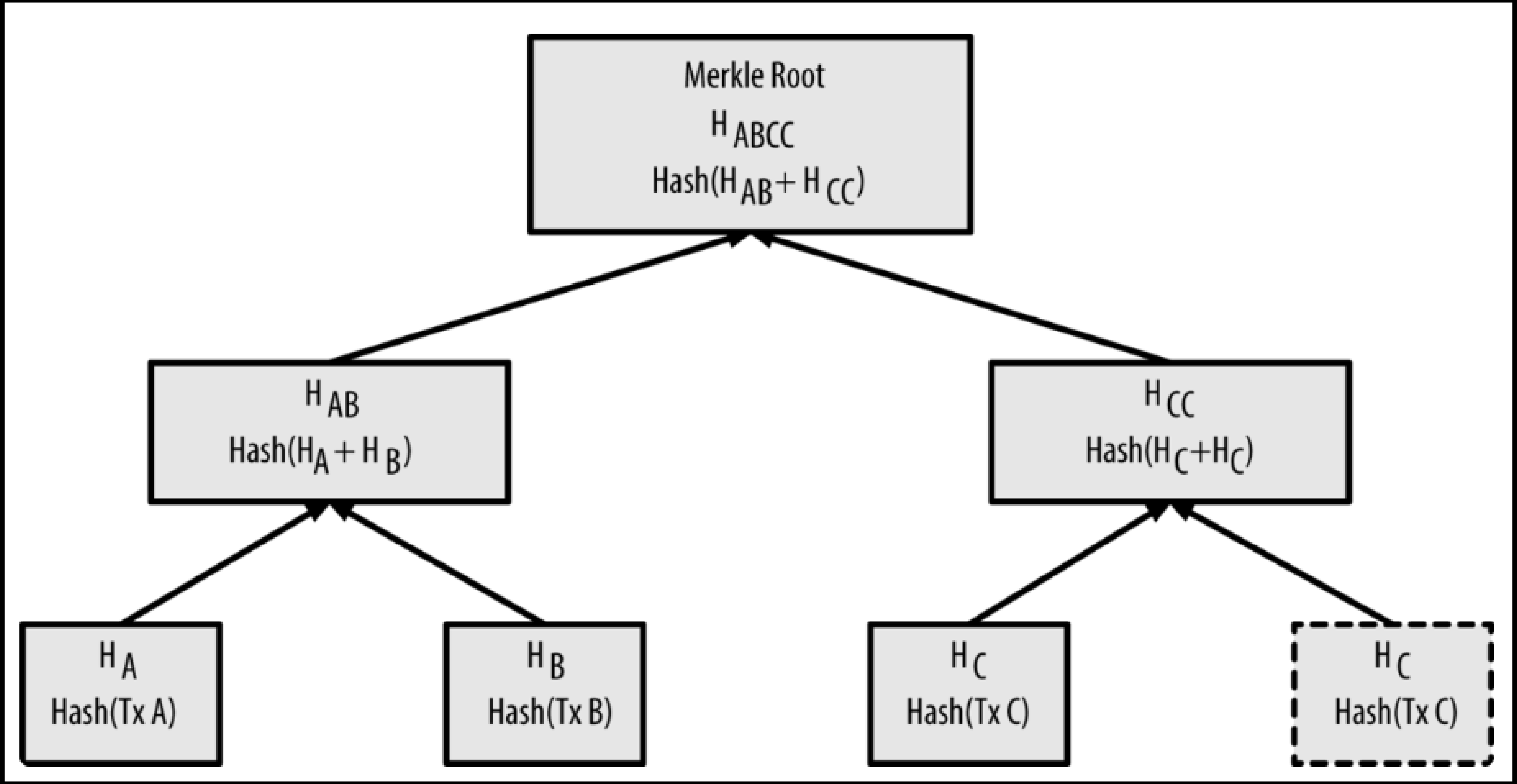


Merkle Tree (2/7)

- Tree node
  - **Root:** stored in block header, calculate by its leaves
  - **Node with leaves:** calculate by its leaves
  - **Node without leaves:** transactions

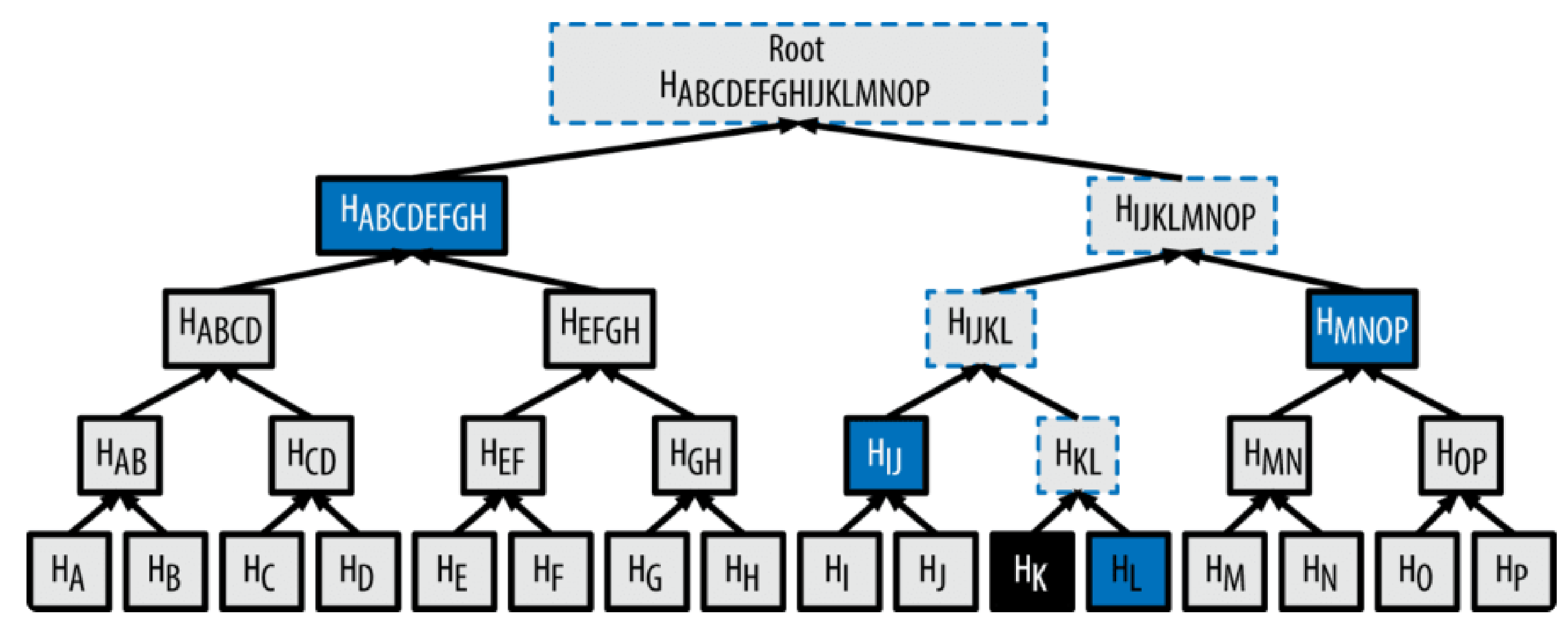
- Rule
  - The number of each node must be **even**
  - Ex: Given transaction A, B, C, the C will the duplicated to fill the right leave of node H_{CC} (See next page.)

Merkle Tree (3/7)



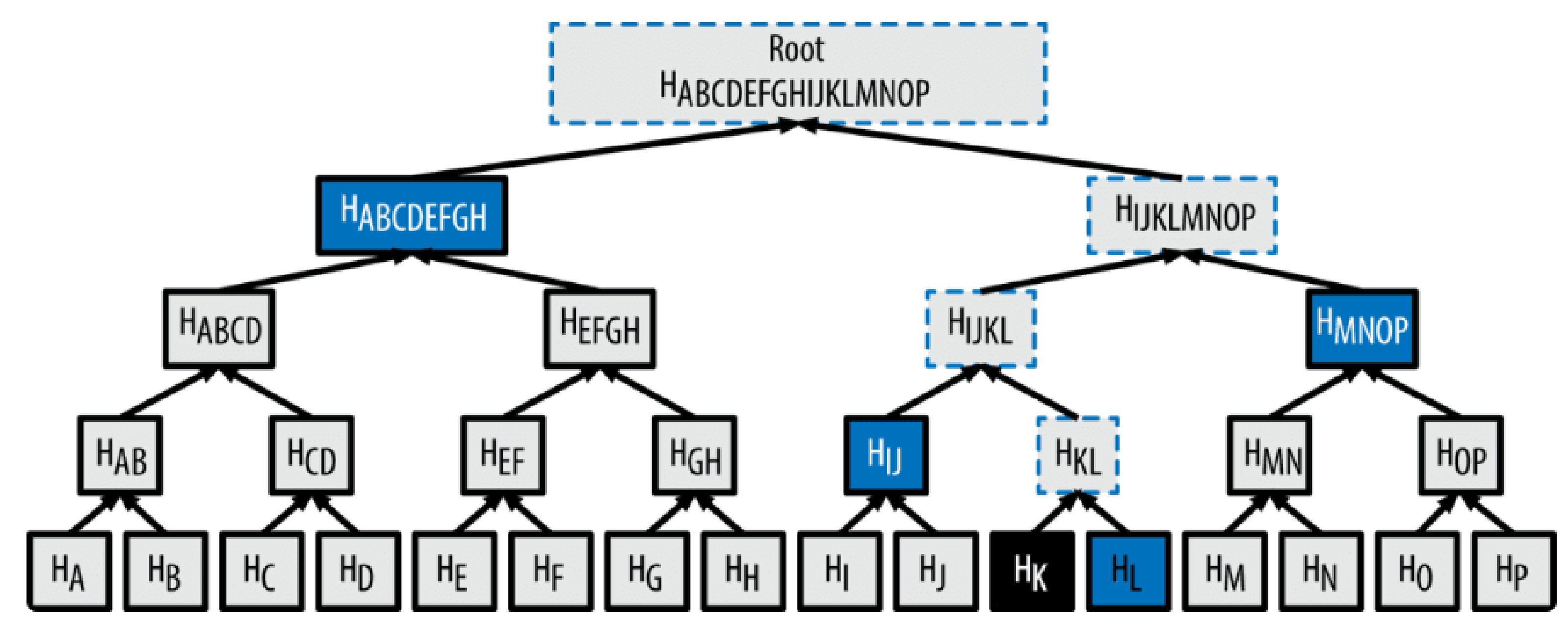
Merkle Tree (4/7)

- Verify existence of a transaction
  - Path: combination of tree node hashes that used to calculate the parents of the transaction

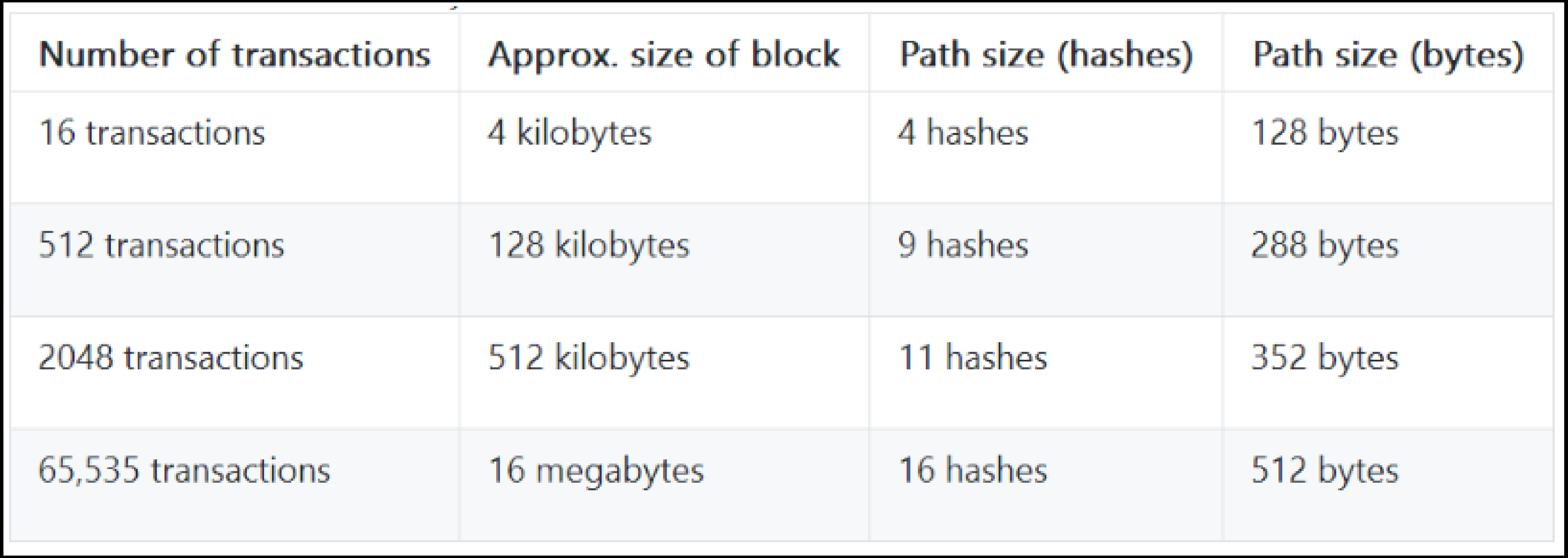


Merkle Tree (5/7)

- In this case, to verify Hk:
  - Parent: H_{KL}, H_{IJKL}, $H_{IJKLMNOP}$, $H_{ABCDEFGHIJKLMNOP}$
  - Path = [H_L | H_{IJ} | H_{MNOP} | $H_{ABCDEFGH}$]



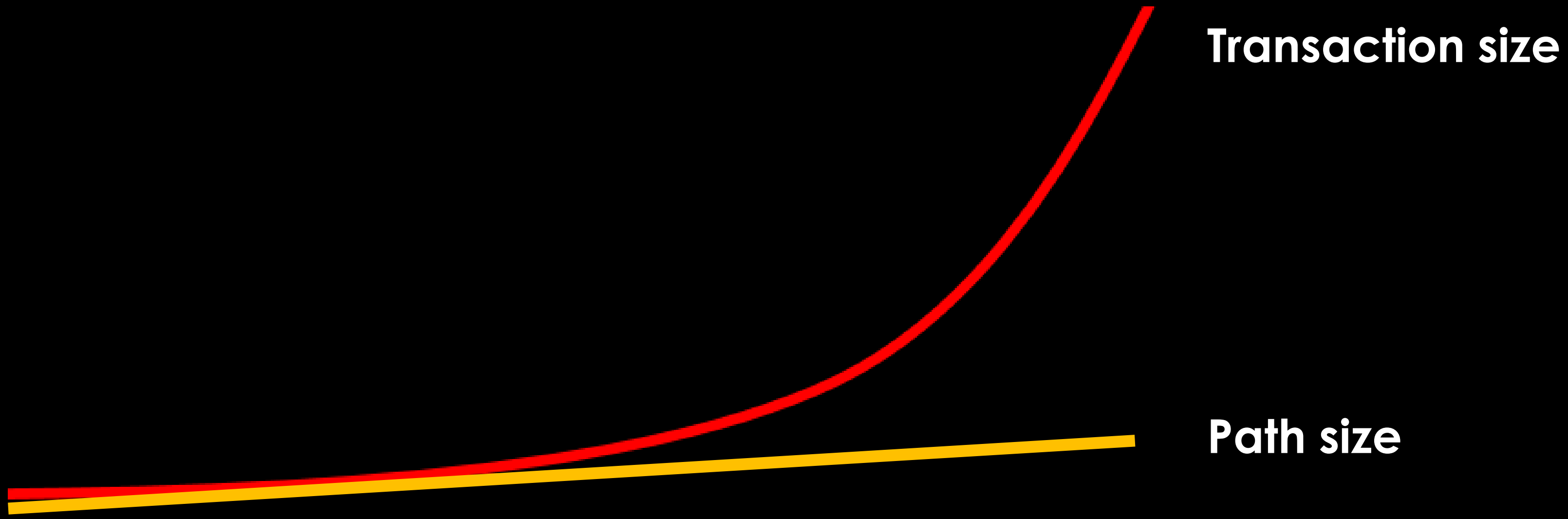
Merkle Tree (6/7)



Number of transactions	Approx. size of block	Path size (hashes)	Path size (bytes)
16 transactions	4 kilobytes	4 hashes	128 bytes
512 transactions	128 kilobytes	9 hashes	288 bytes
2048 transactions	512 kilobytes	11 hashes	352 bytes
65,535 transactions	16 megabytes	16 hashes	512 bytes

Merkle Tree (7/7)

- Advantage
  - BST: $\log_2(N)$
  - Small data size require for verifications
  - Suitable for nodes with limited hardware device (SPV node)


Transaction size
Path size