Bitcoin Blockchain

Sameh El-Ansary, PhD

NOVELARI

INNOVATION ACCELERATOR

Bitcoin Blocks

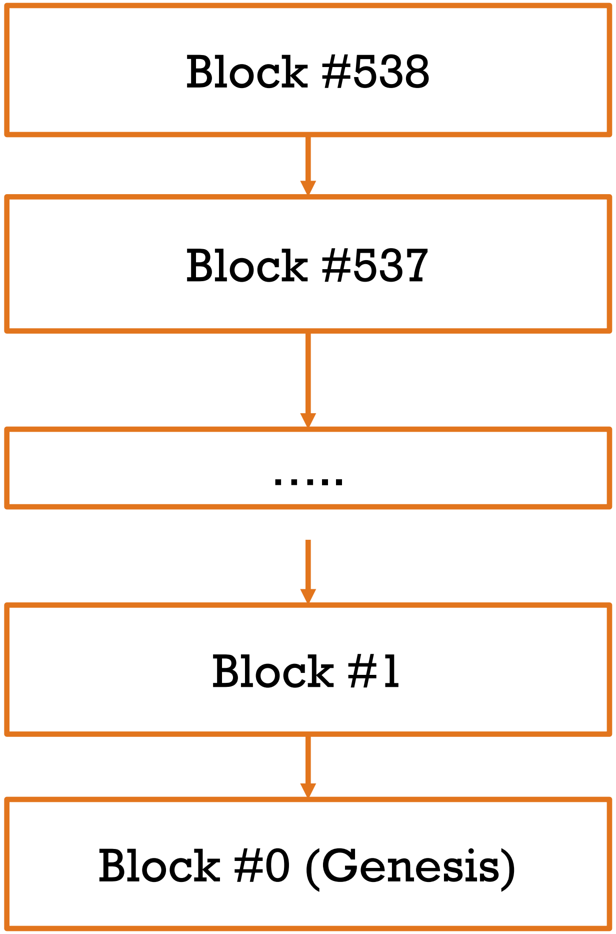
- A **block** is a set of transactions grouped together.
- Users issue transactions and send them to the network
- Miners:
  - Create blocks from received transactions
  - Propose a block to the network (after doing some work)
  - The network reaches an agreement on the acceptance/rejection of the block
- Each "accepted" blocks is added to an ordered list of blocks called the **Blockhain**

Blockchain

The bitcoin blockchain is a **global**, **replicated**, **public** ledger (list) of all transactions, which everyone in the bitcoin network accepts as the **authoritative record of ownership**

The Blockchain Data Structure

- The blockchain is an ordered, back-linked list
- Each block is of a variable size (# of TXs)
- Can be stored as a flat file, or in a simple database, Bitcoin Core uses Google's LevelDB.



Block #538

Block #537

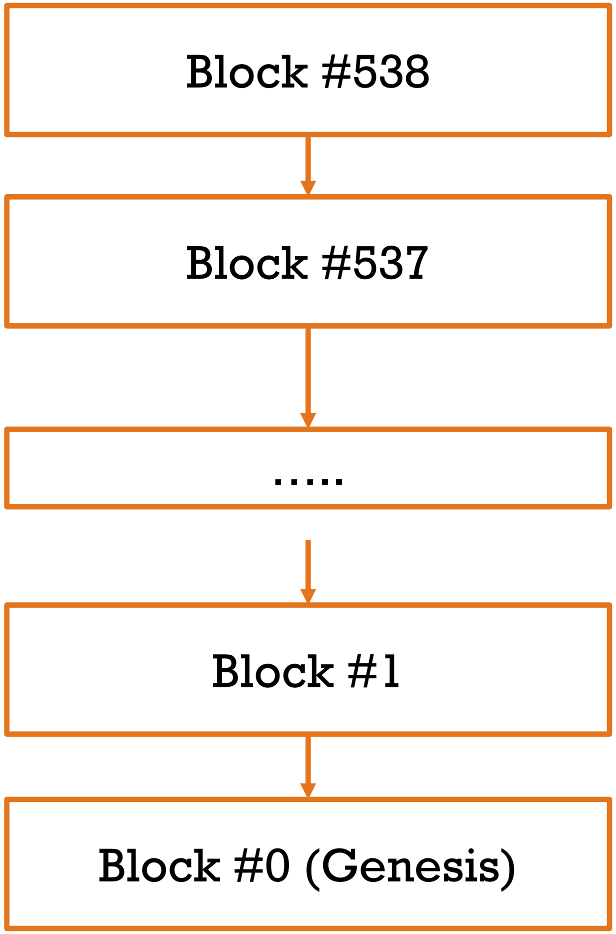
…..

Block #1

Block #0 (Genesis)

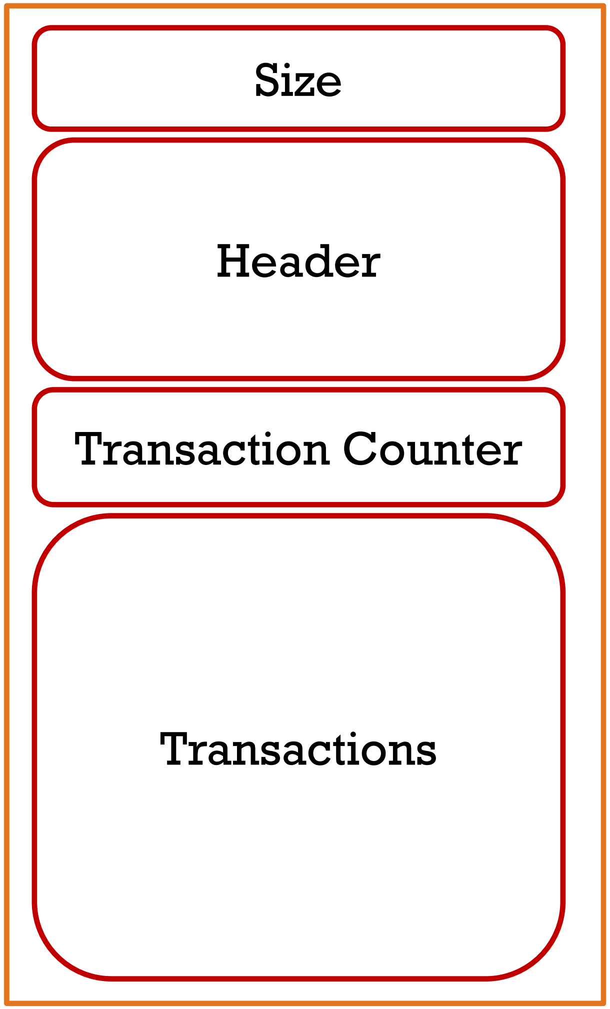
The Blockchain Data Structure

- Blocks refer to the previous block in the chain.
- "**height**" refers to distance from first block,
- "**tip**"/"head" refer to the most recently added block.
- "Genesis" block is the first block ever created i.e. #0



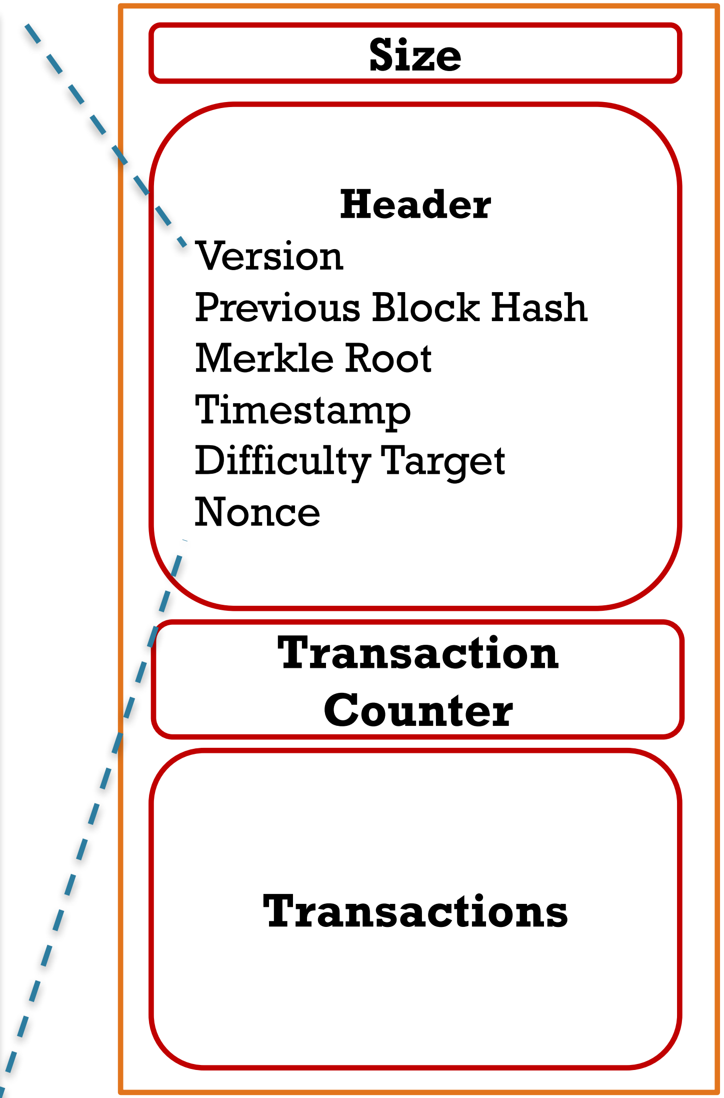
Structure of a Block

Size	Field	Description
4 bytes	Block Size	size of 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



Block Header

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



Block Identifiers:
Block Header Hash & Block Height

Block Header Hash

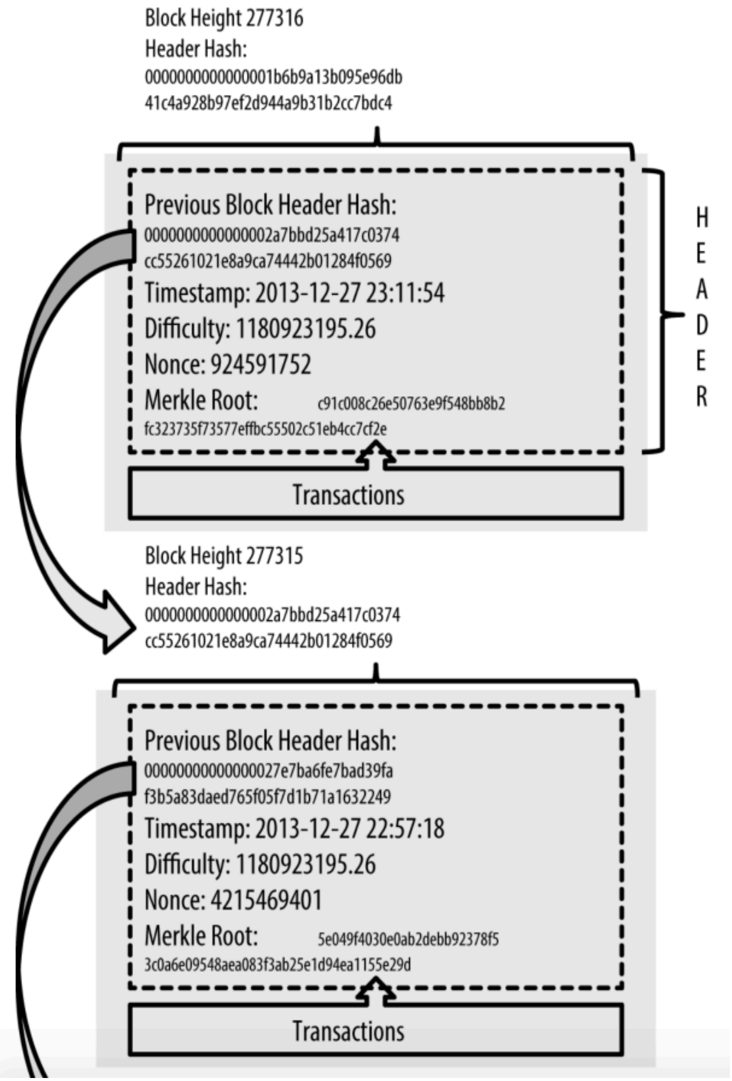
- Not written anywhere inside a block or its header
- Appears only in the "parent/previous" field of its child

Block Height

- Can be used to identify a block
- Also Not written anywhere

Uniqueness

- When 2 blocks compete for the tip of the blockchain
  - Hash is a unique id of the block
  - Height is not



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

HEADER

Block Height 277315
Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

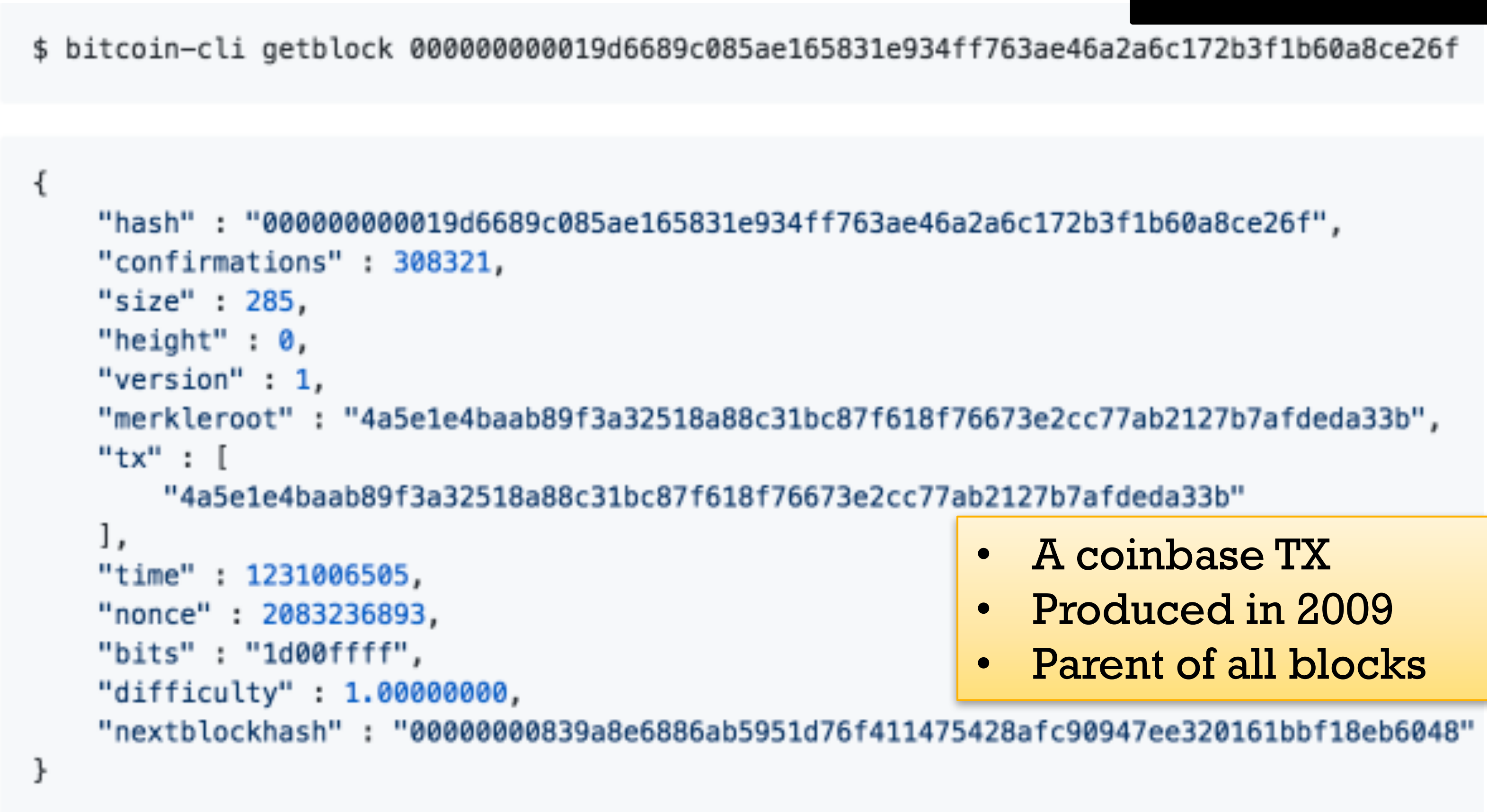
Previous Block Header Hash:
0000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
Timestamp: 2013-12-27 22:57:18
Difficulty: 1180923195.26
Nonce: 4215469401
Merkle Root: 5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d

Transactions

Why many zeroes in the block hash?

Genesis Block

How is this diferent from transactions we saw earlier? Is this the header only or the full block? Can you guess where is the hidden message.



```
$ bitcoin-cli getblock 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
```

```
{
    "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"
}
```

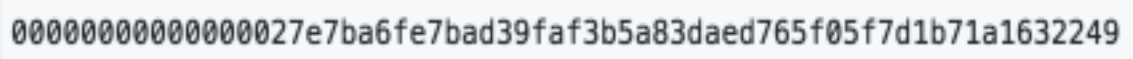
- A coinbase TX
- Produced in 2009
- Parent of all blocks

Had a hidden message irony as well as a proof of release date. It is the headline of the Times newspaper on Jan 3rd 2009:

"*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”*

Linking Blocks in the Blockchain

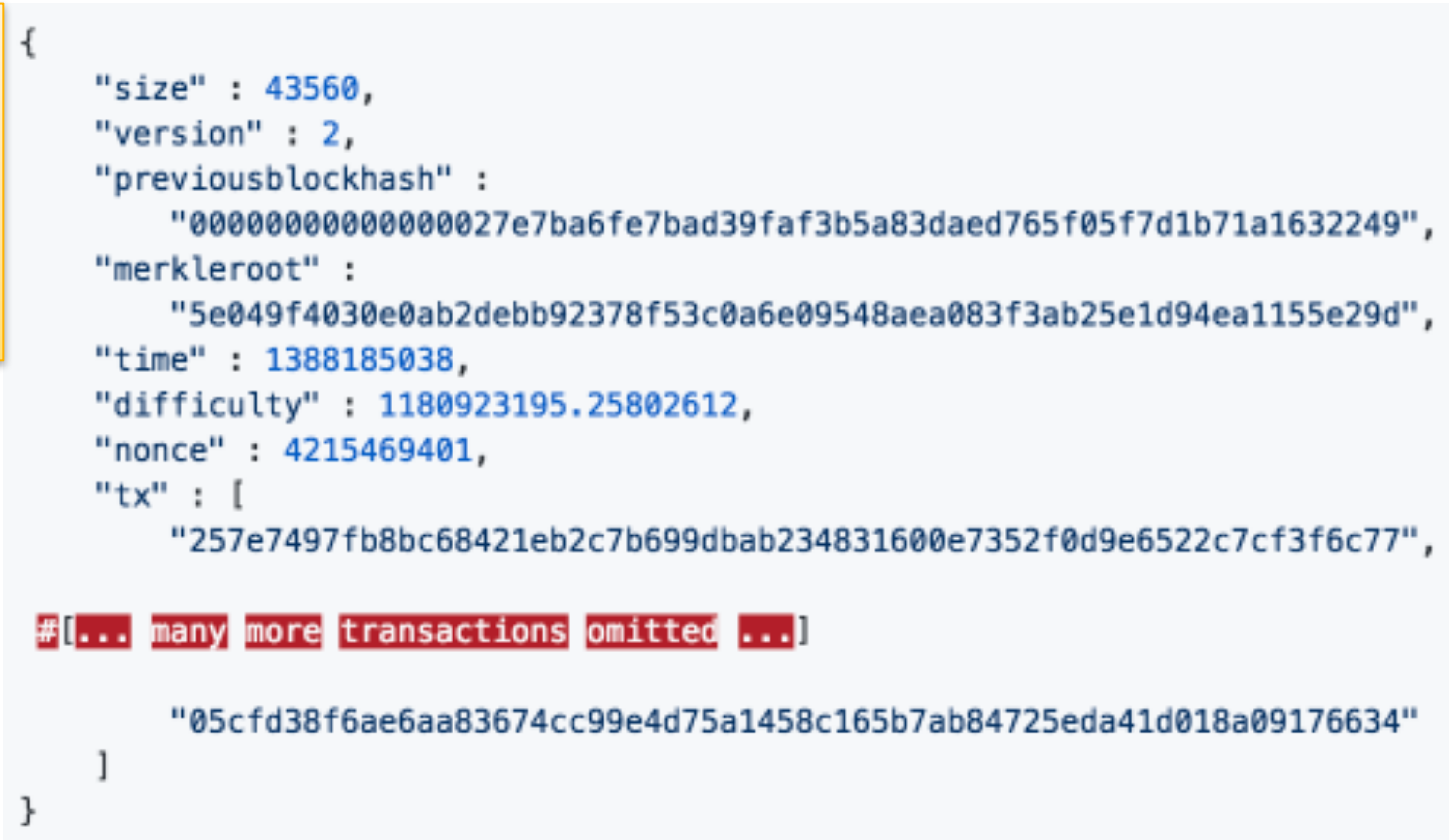
Tip, @height:
277314



```
000000000000000027e7ba6fe7bad39faf3b5a83daed765f05f7d1b71a1632249
```

New block:
Direct Child?
Yes

Add @height:
277314

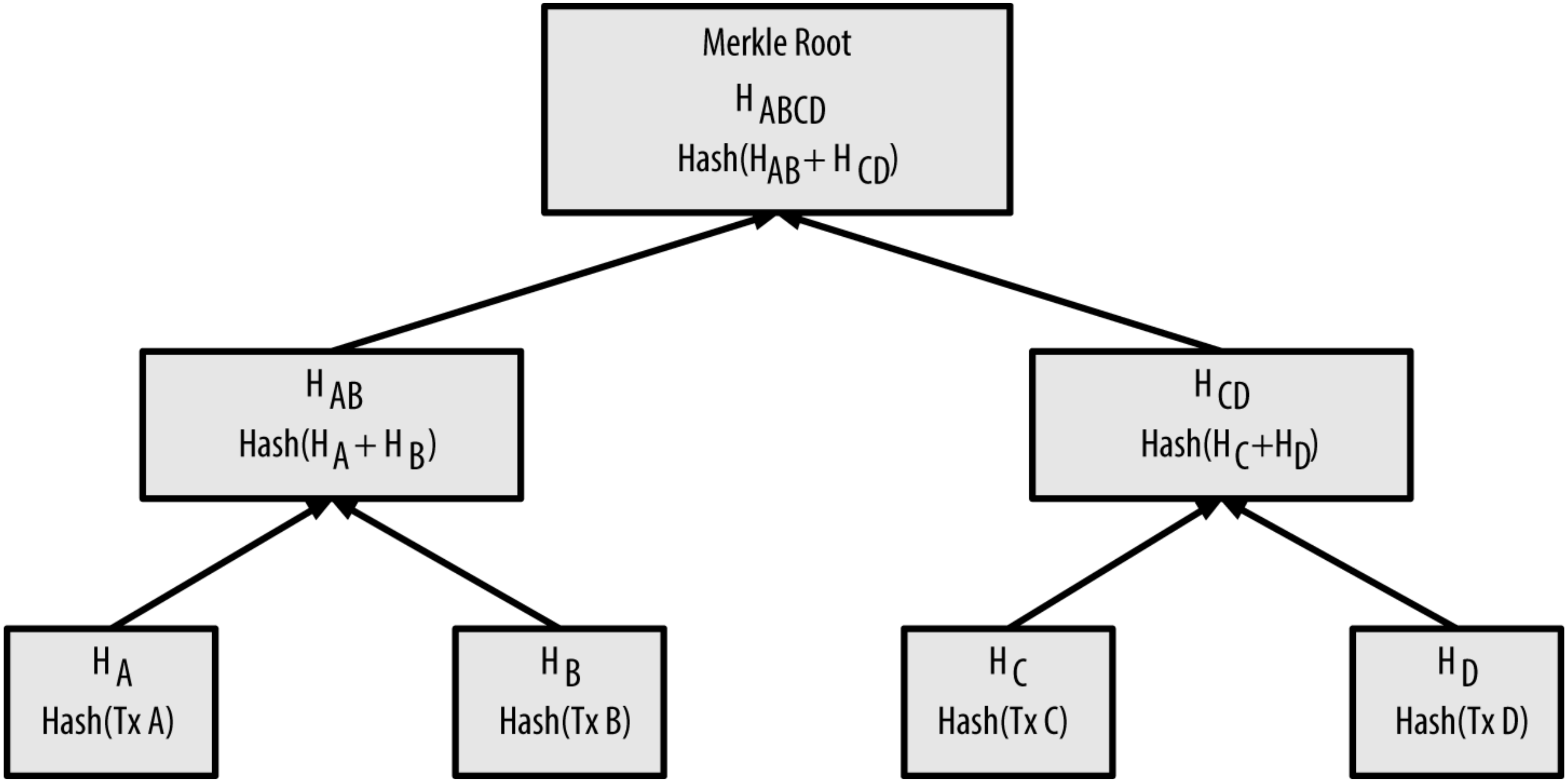


```
{
    "size" : 43560,
    "version" : 2,
    "previousblockhash" :
        "000000000000000027e7ba6fe7bad39faf3b5a83daed765f05f7d1b71a1632249",
    "merkleroot" :
        "5e049f4030e0ab2debb92378f53c0a6e09548aea083f3ab25e1d94ea1155e29d",
    "time" : 1388185038,
    "difficulty" : 1180923195.25802612,
    "nonce" : 4215469401,
    "tx" : [
        "257e7497fb8bc68421eb2c7b699dbab234831600e7352f0d9e6522c7cf3f6c77",

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

        "05cfd38f6ae6aa83674cc99e4d75a1458c165b7ab84725eda41d018a09176634"
    ]
}
```

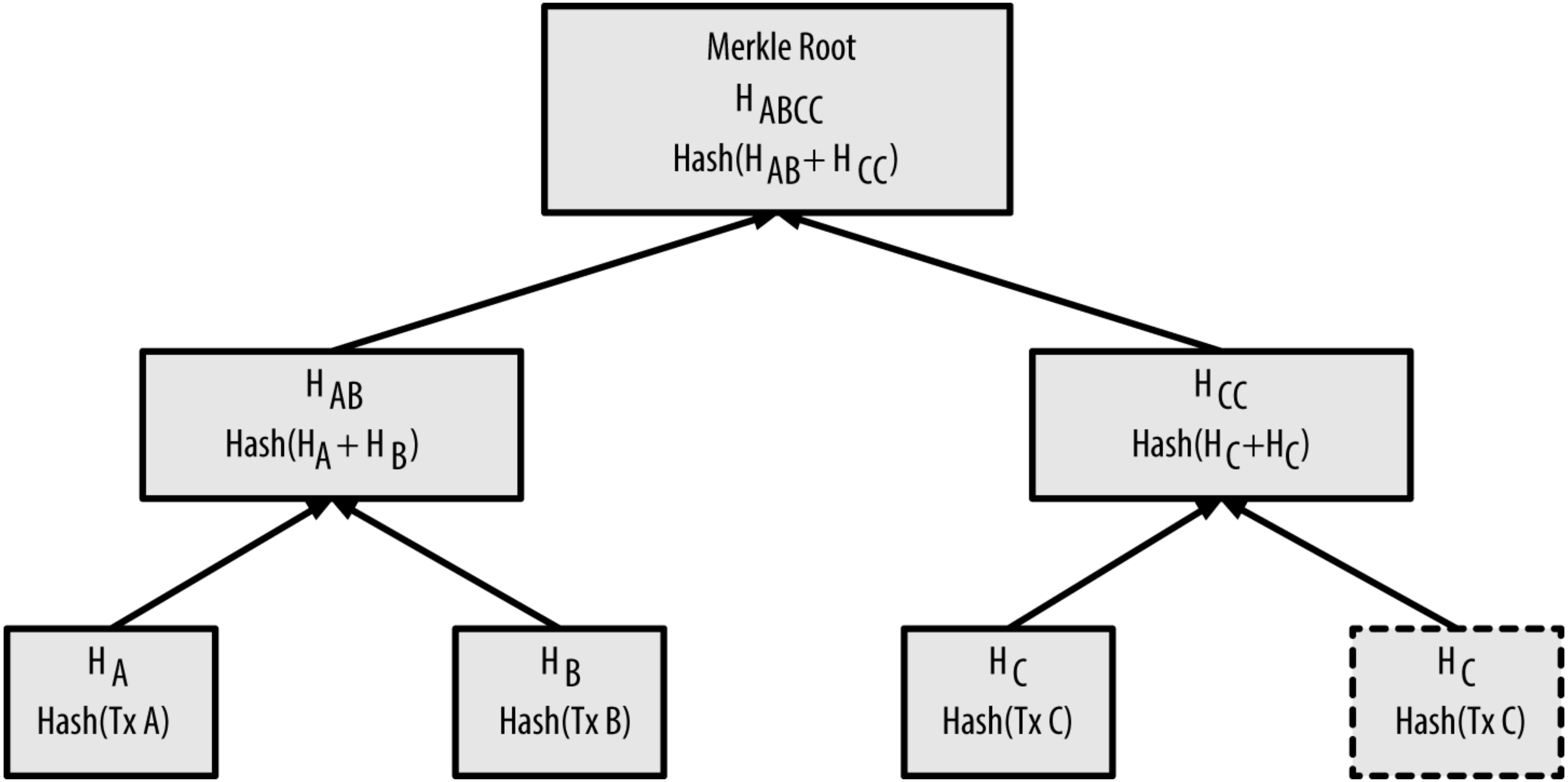
Merkle Tree

- AKA Binary Hash Tree
- Efficiently summarizes and verifies large sets of data.
- Given N data elements, you can check whether any element is in the list in at most $2\log_2(N)$ steps.
- Used to know if a transaction belongs to a block without downloading the whole block (Needed by SPV nodes)

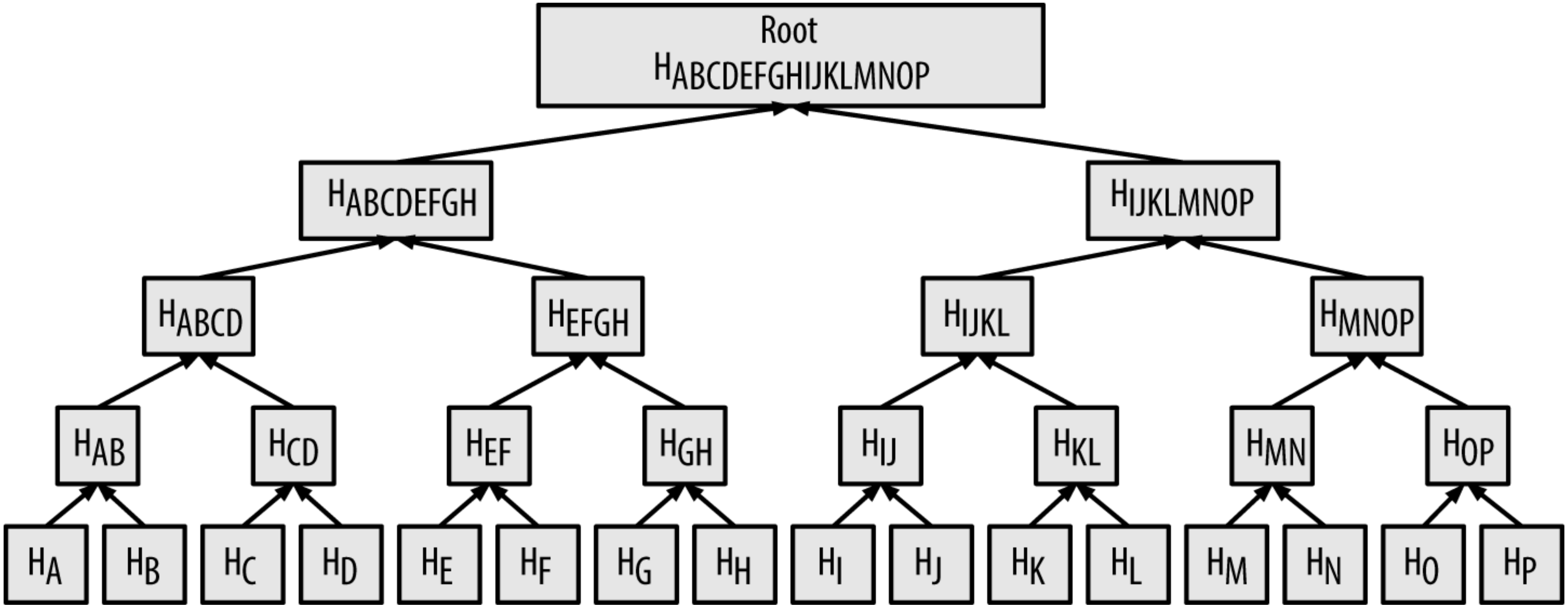
Merkle Tree for a Block with 4 TXs



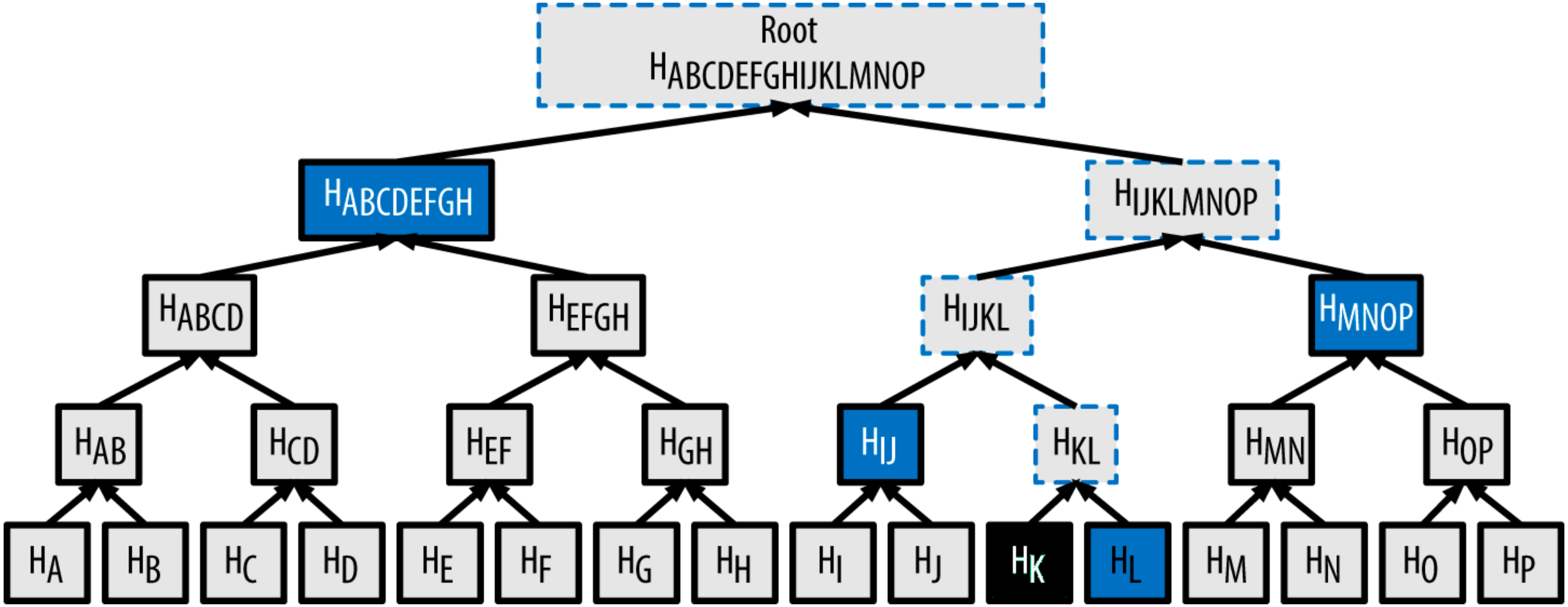
Merkle Tree for a Block with 3 TXs



Merkle Tree for a Block with 16 TXs



Merkle Path



A node can prove that a transaction K is included in the block by producing a Merkle path that is only four 32-byte hashes long (128 bytes total). The path consists of the four hashes HL, HIJ, HMNOP, and HABCDEFGH.

Merkle Tree Efficiency

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

Bitcoin Networks

Network	Purpose
Mainnet	The real network
Testnet	For testing purposes Testnet 1 Testnet 2 Testnet 3
Segnet	For helping in Segregated Witness 3 (now merged in Testnet3)
Regtest	Local blockchain

Lab

- Play with regtest:
  - https://bitcoin.org/en/developer-examples#regtest-mode

Knowledge Checklist

- Block
- Blockchain
- Block Header
- Block identifiers: hash & height
- Blockchain Tip
- Genesis Block
- Merkle Tree