Quiz: best 80%

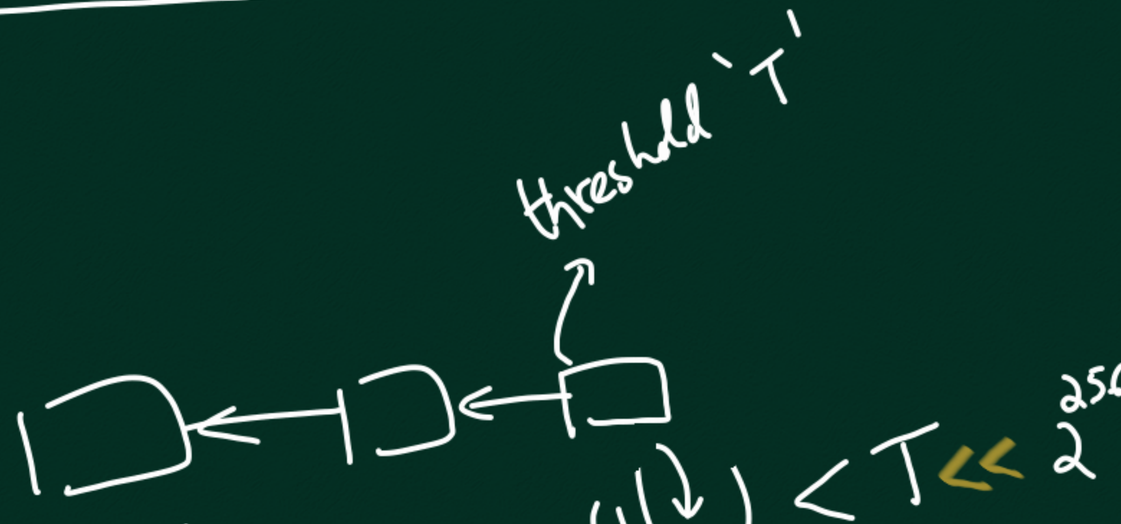
Attendance: 7 marks

Ex: missed 5 lec
⇒ 5 marks

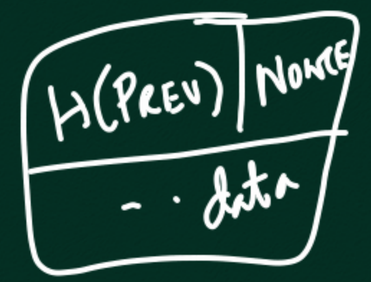
Hash Function

Attendance

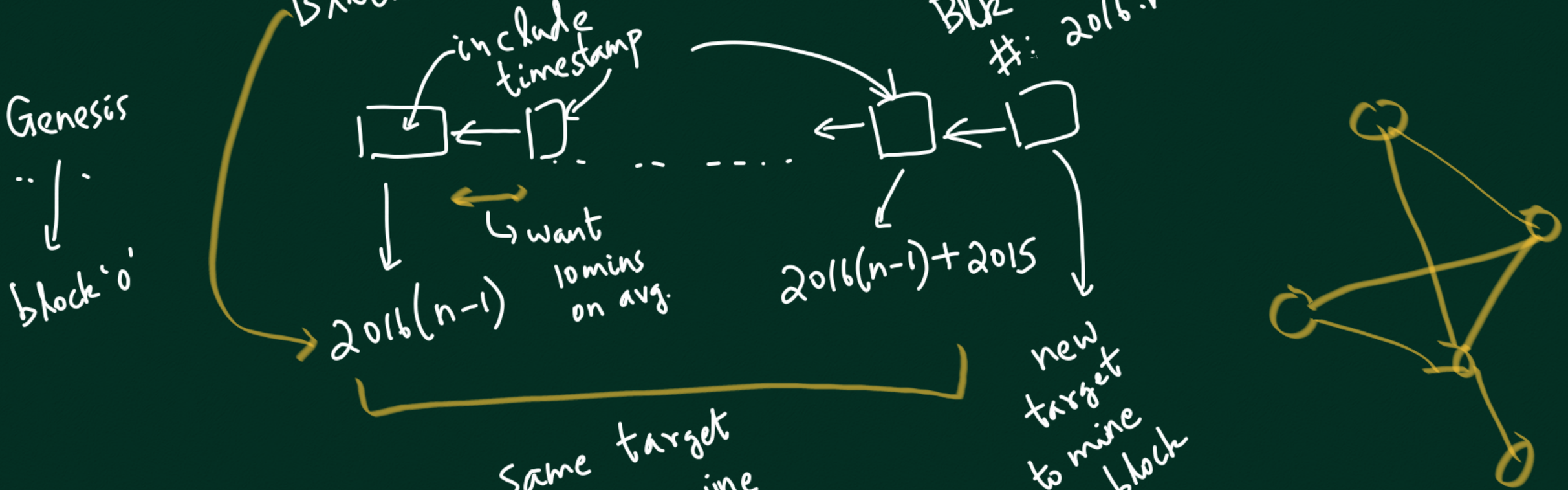
- ref. to txns
- Hiding & timestamping
- Puzzles & PoW



Avg. # tries = $\frac{2^{256}}{T}$



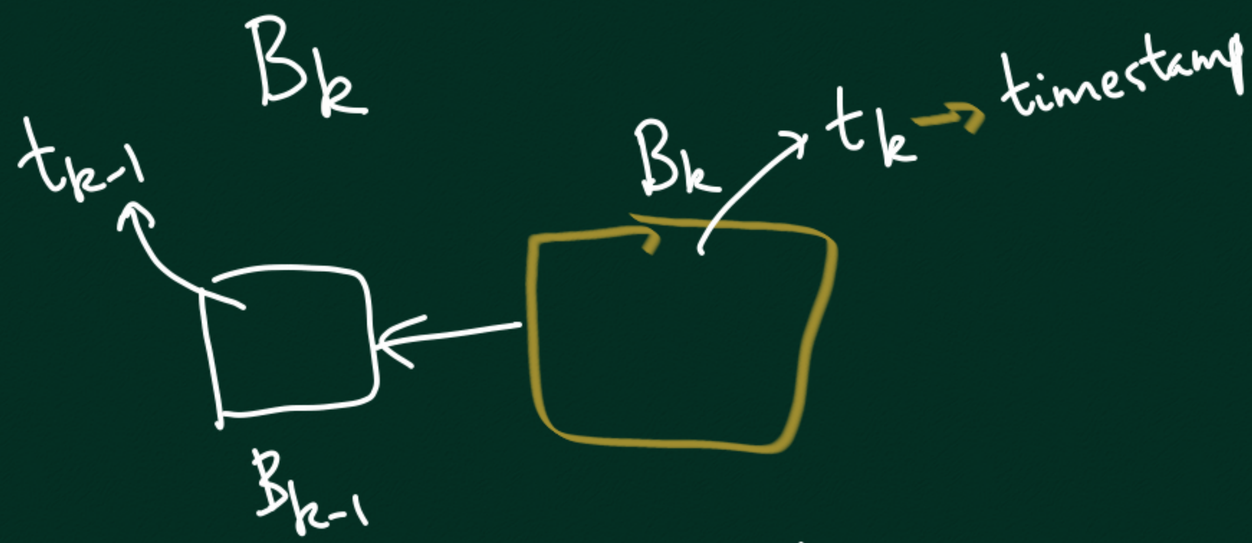
target threshold 'T' is updated every 2 weeks roughly (actually every 2016 blocks)



$$T = T_x \left[\frac{\text{timestamp in blk } 2016(n-1)+2015 \; - \; \text{timestamp in blk } 2016(n-1)}{1209600} \right]$$

new target in blk 2016·n

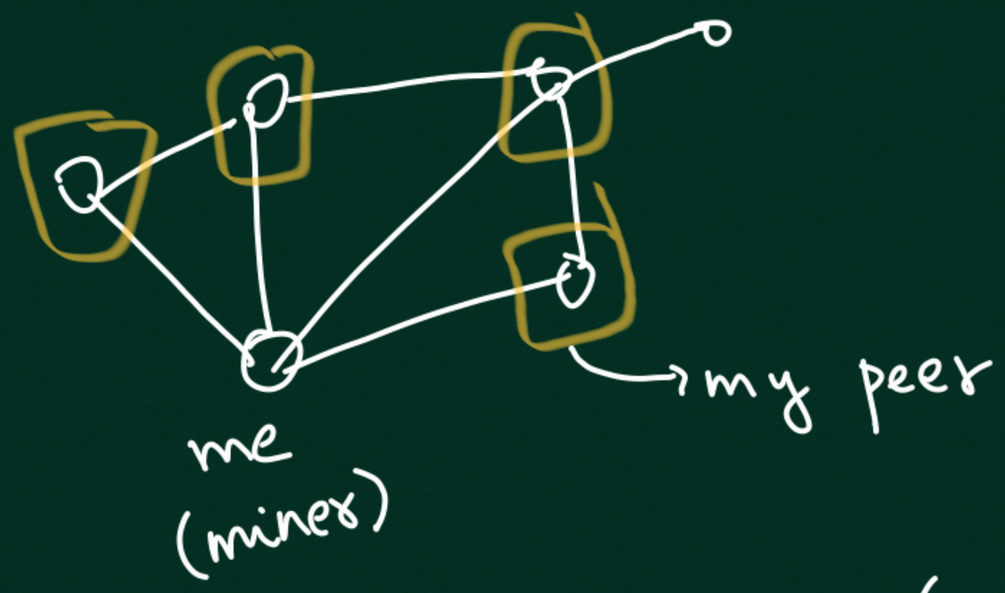
When a miner receives a block B_k



Accept B_k only if

$$t_k > \text{median}(t_{k-1}, t_{k-2}, \ldots, t_{k-11})$$

AND $t_k <$ 2 hours + "network adjusted time"



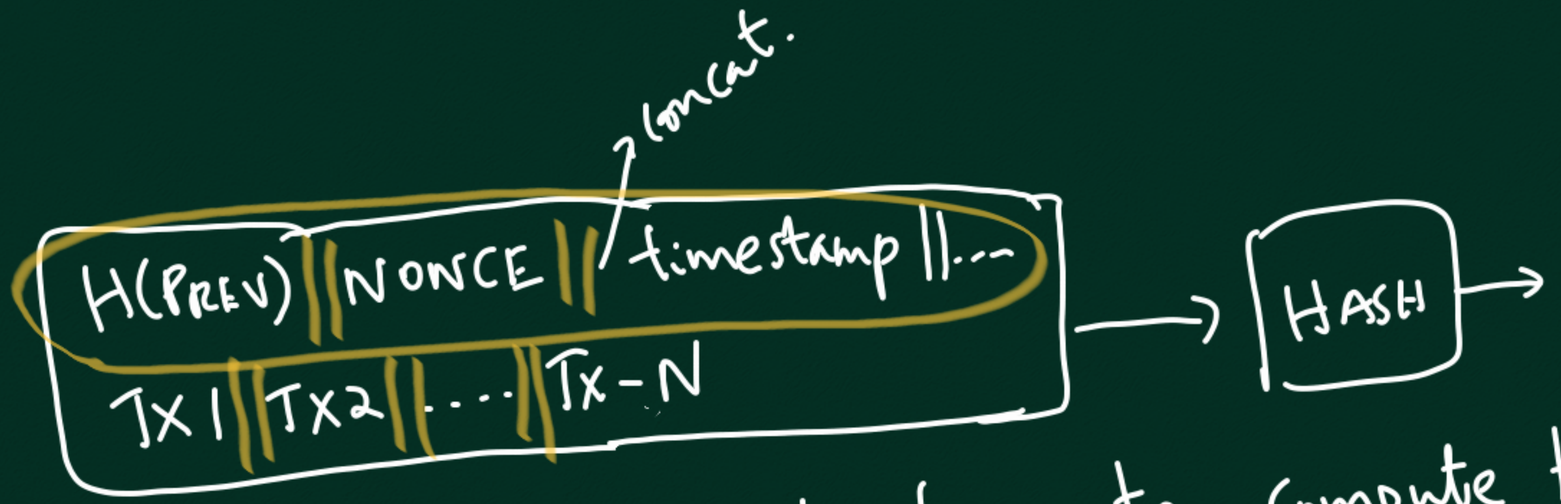
NAJ = my time + median (offsets of time with all Connected peers)

↓ When I received B_k

bounded by ±70 mins

Block Header

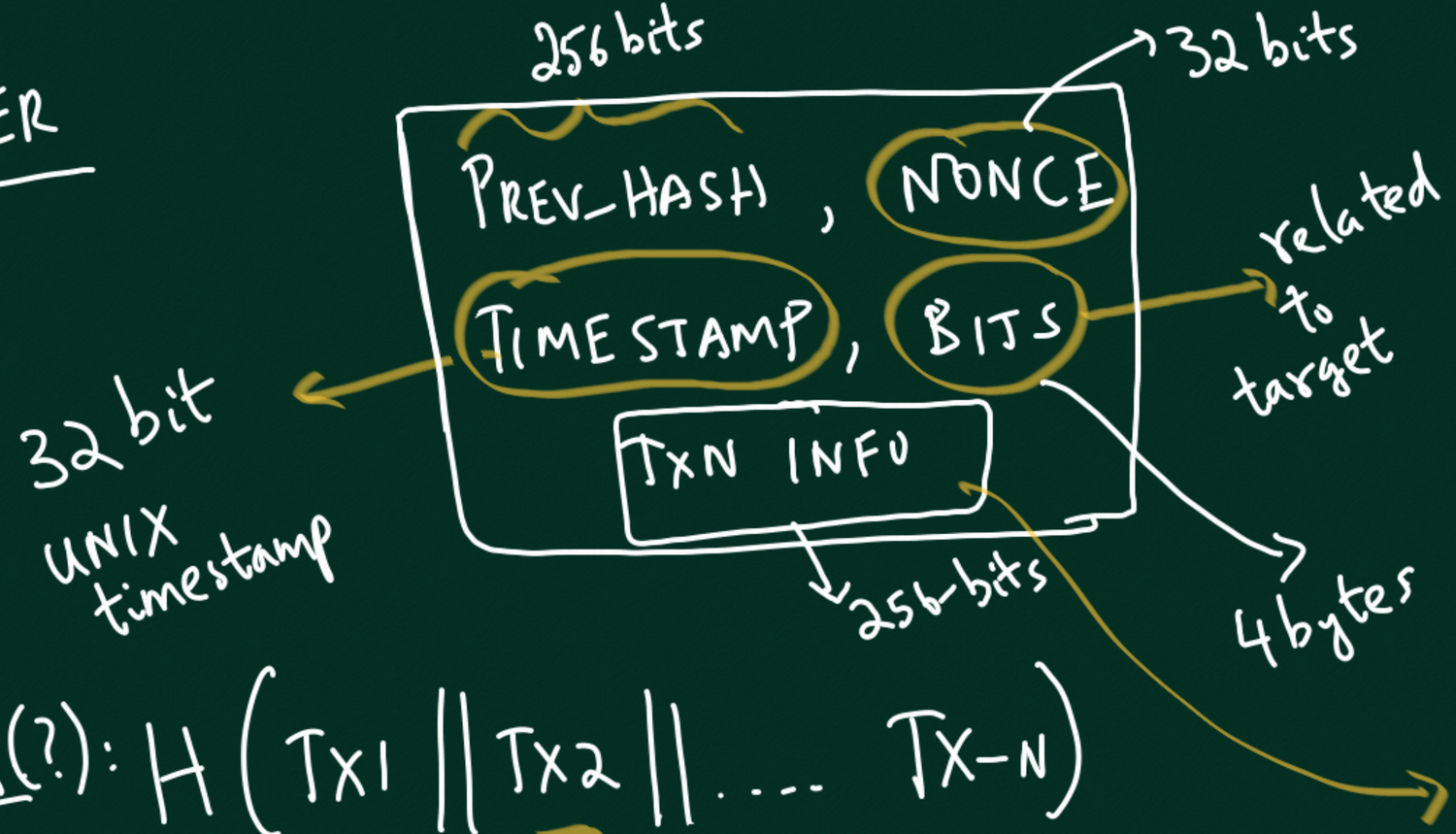
Naive



N = 1000,

Want time to compute Hash of blk to be indep. of # txns

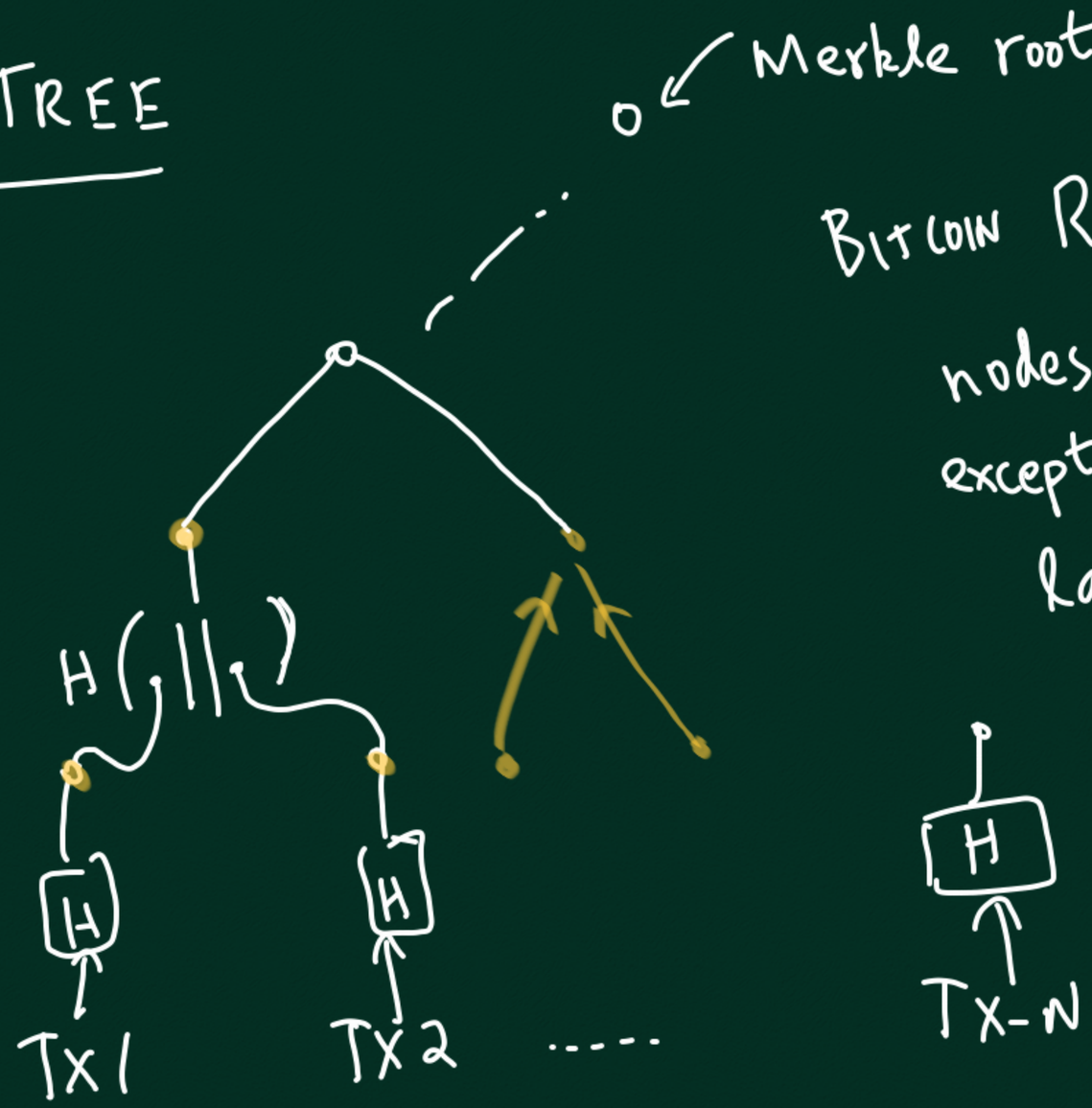
HEADER



IDEA(?): $H(TX1 \,||\, TX2 \,||\, \ldots \; TX\text{-}N)$

BITCOIN Rule: $H(\text{BLK HEADER}) < T$

MERKLE TREE



BITCOIN RULE: If odd # of nodes in tree (at any level except last level), repeat last node once and proceed upward in tree

MEMPOOL → Pending txns, not yet in any block

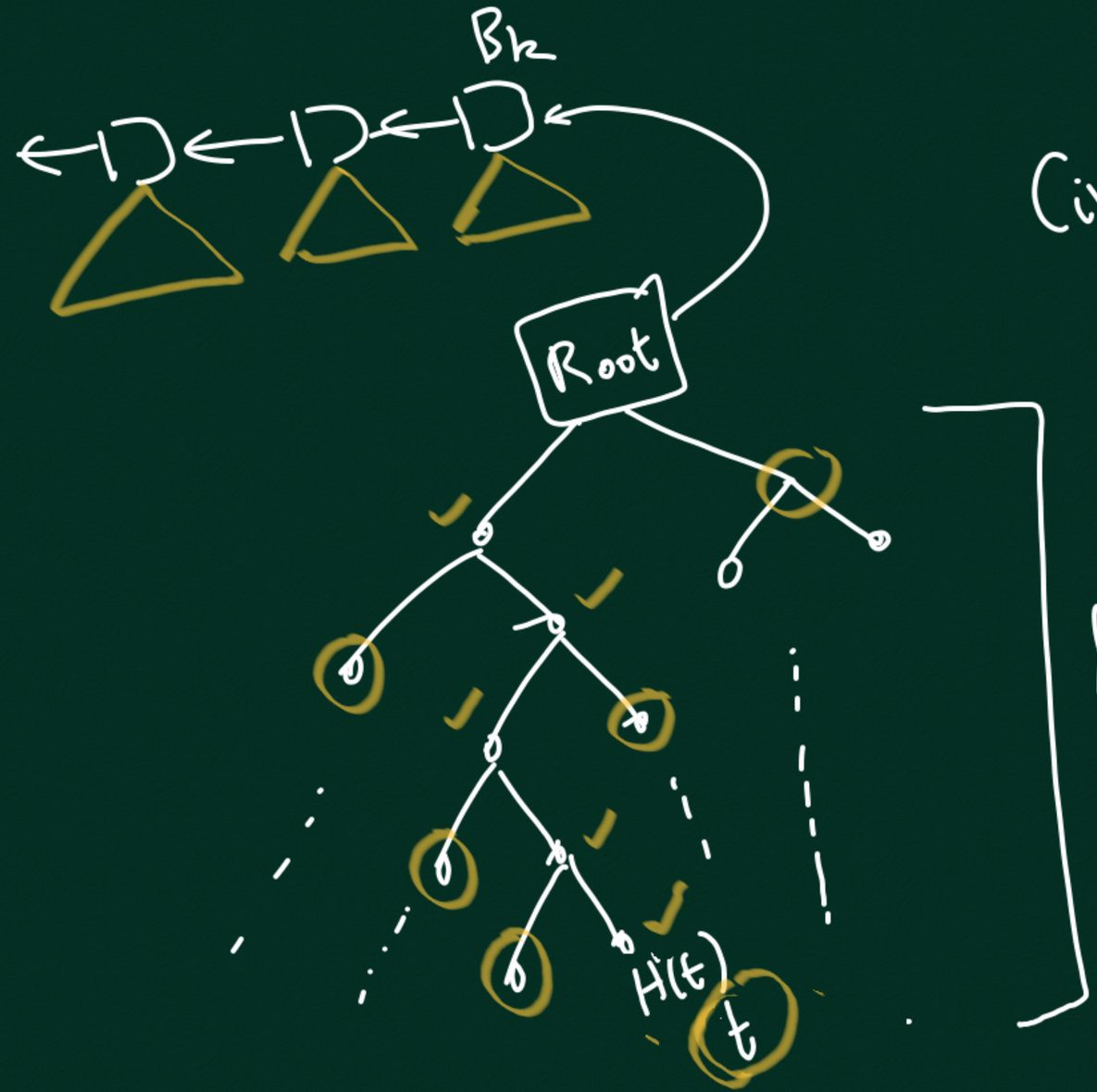
Advantages of using Merkle Roots

(1) Light Nodes & Merkle Proofs

Full Node: Has all info from Gen. blk to latest blk

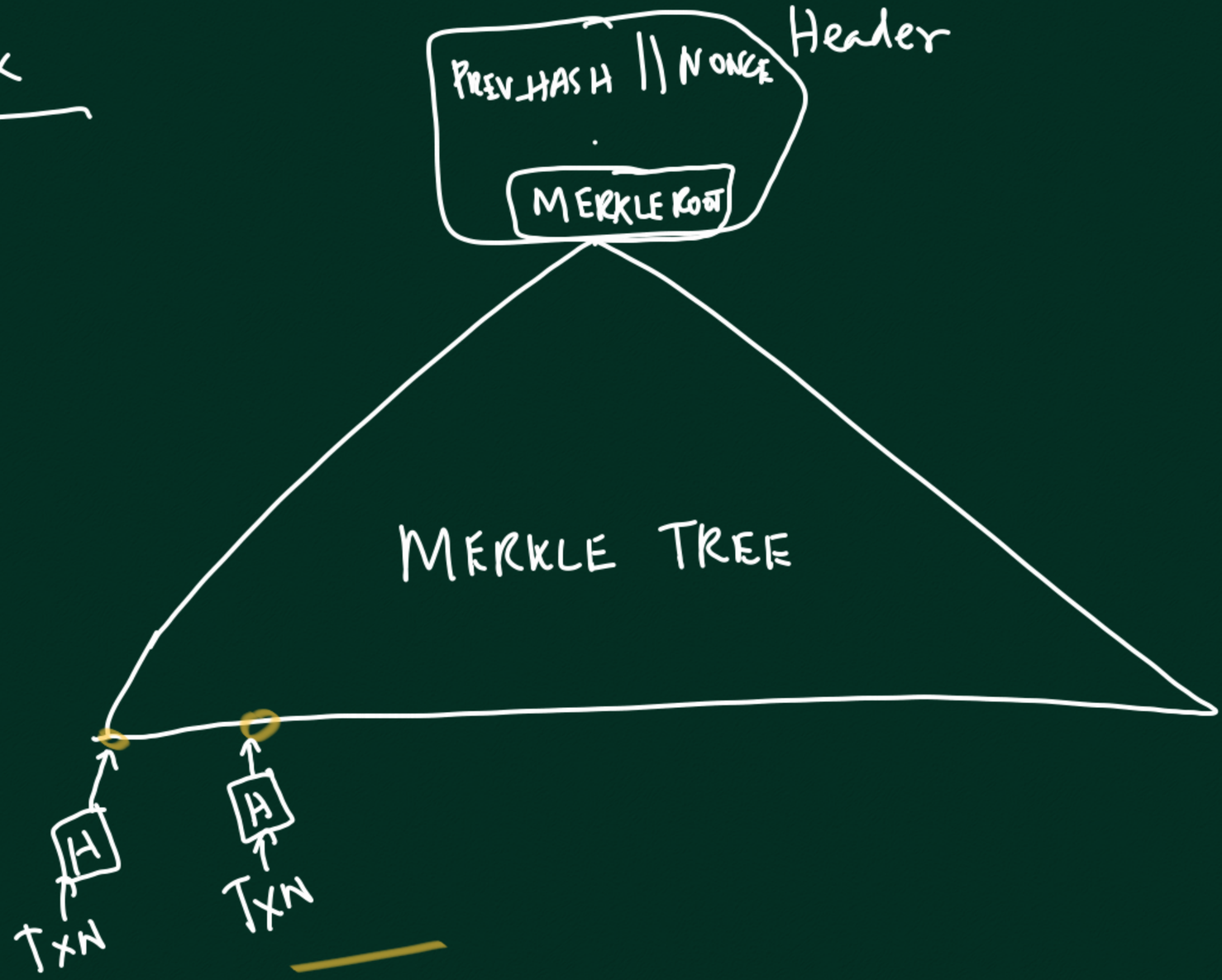
Light Node: Has all blk Headers only
(80 bytes/hdr)
(block size: 1MB → Satoshi)

Q. How to prv. to LN that a txn (t) is in block B_k

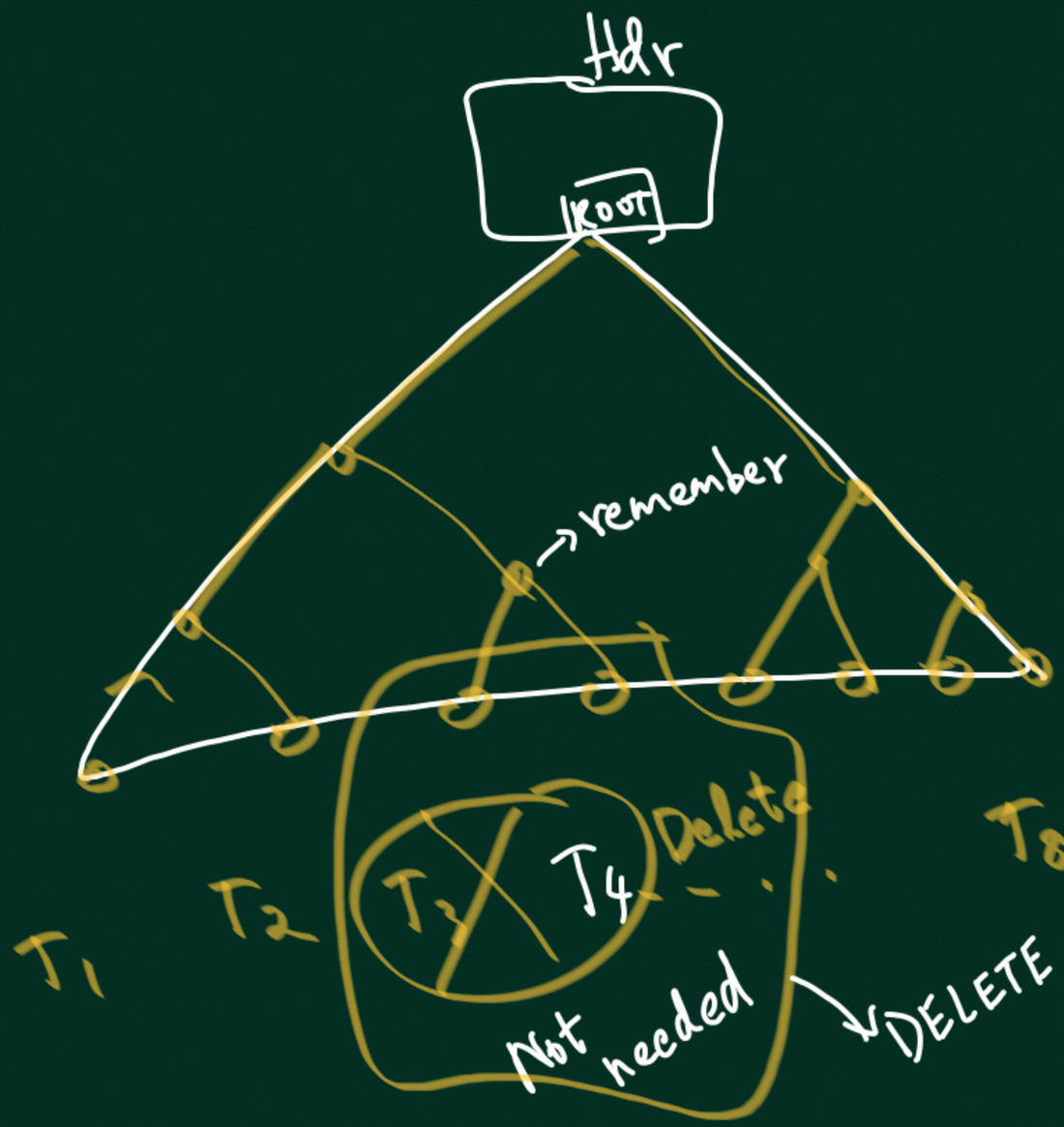


Circled info is Merkle Proof of inclusion of txn 't' in a block

BLOCK



PRUNING (2nd Advantage of Merkle tree)



$H(T_1 || T_2 || T_3 || T_4 \ldots T_8)$

X

missing deleted ??

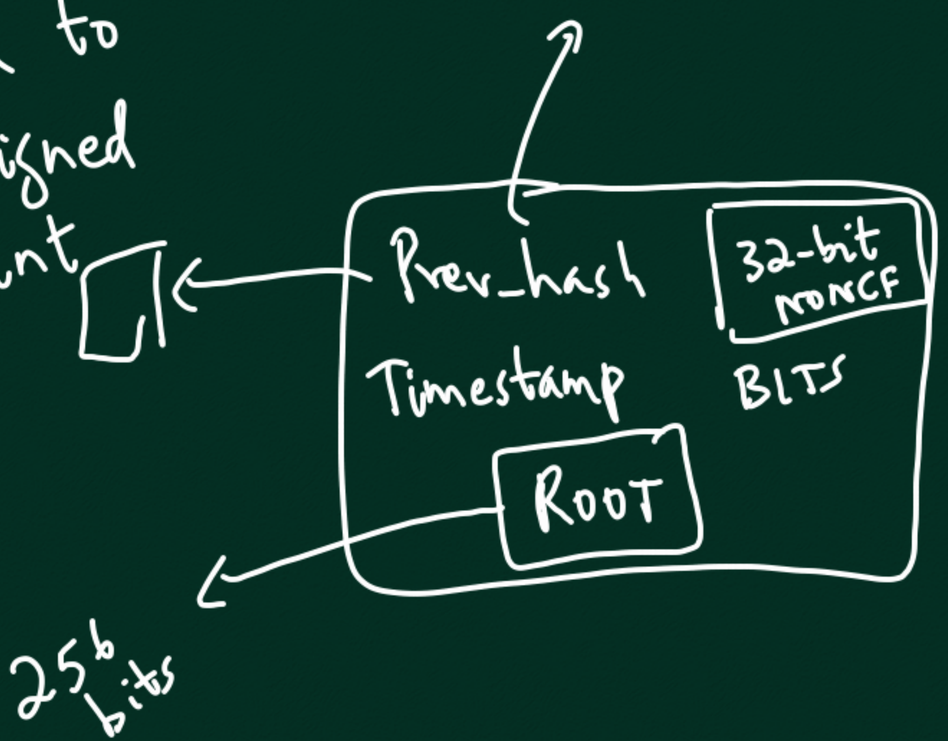
BITS : b_1 b_2 b_3 b_4

4 bytes

target $T = b_2 b_3 b_4 \times (256)^{b_1 - 3}$

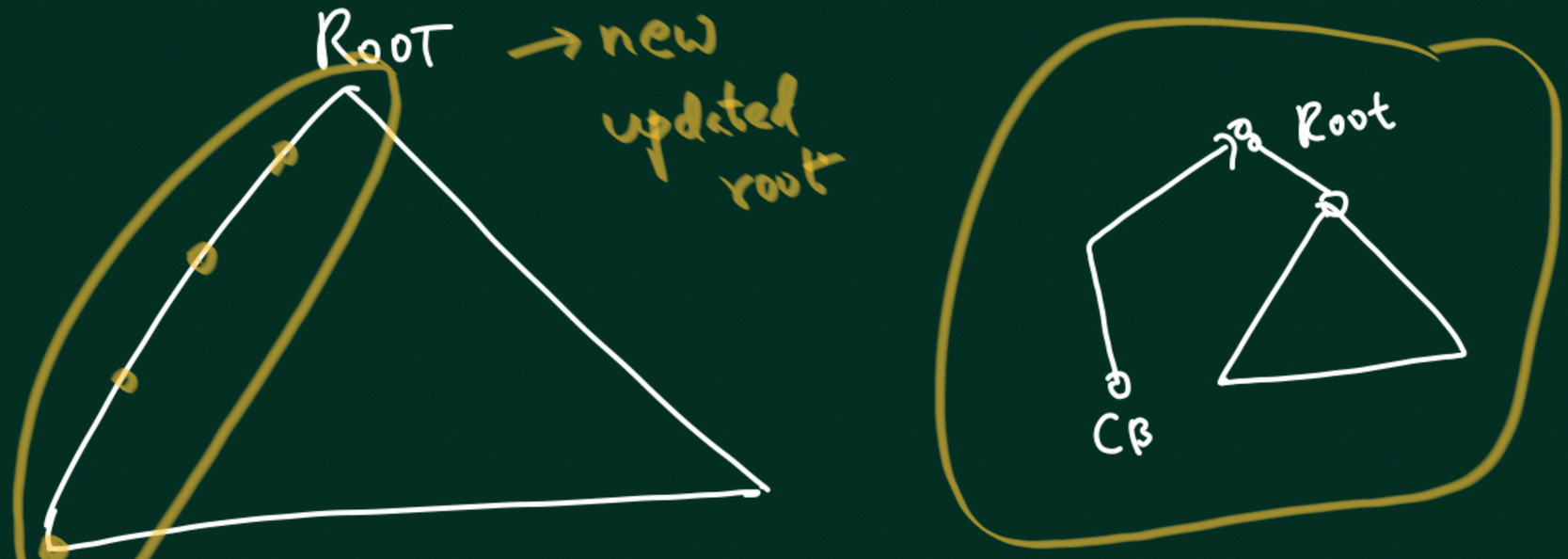
Considered to be unsigned int

NONCE: 32 bits



Coinbase txn: 1st txn in a blk

↳ Spl. txn : miner gets mining reward



Coinbase → has field where any text can be put