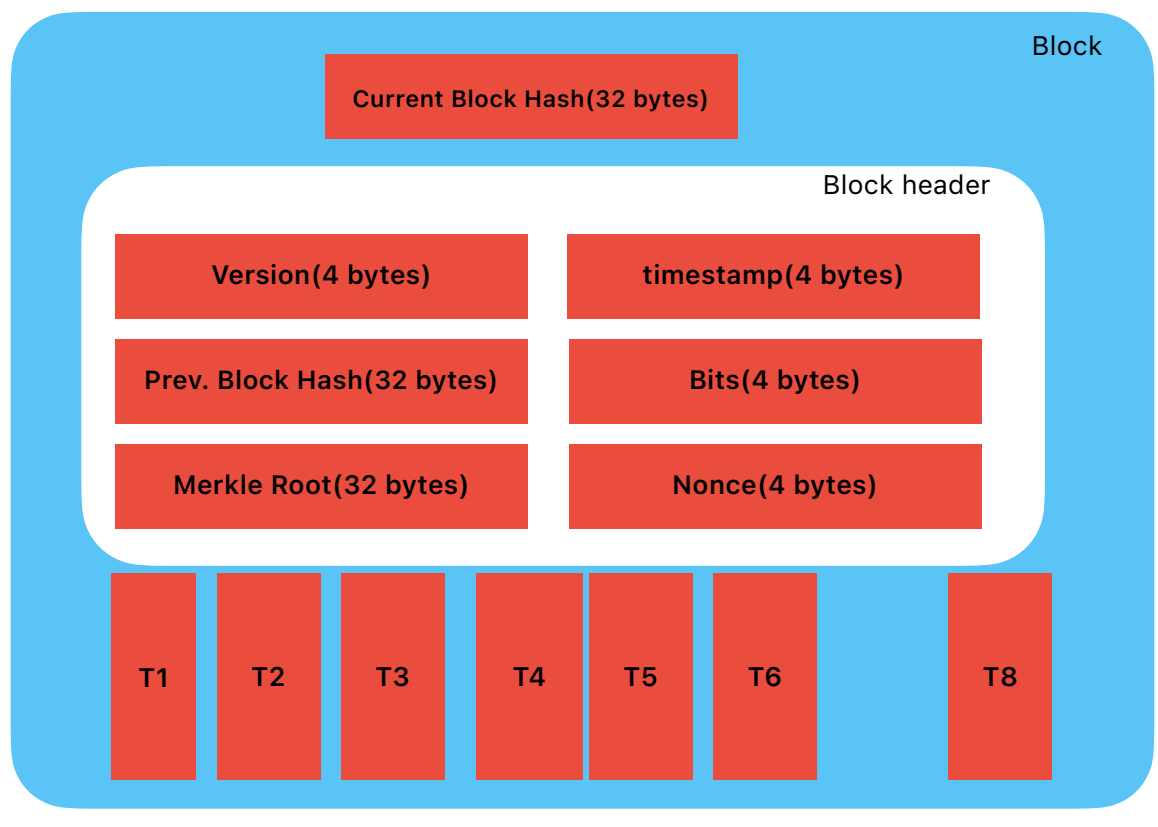
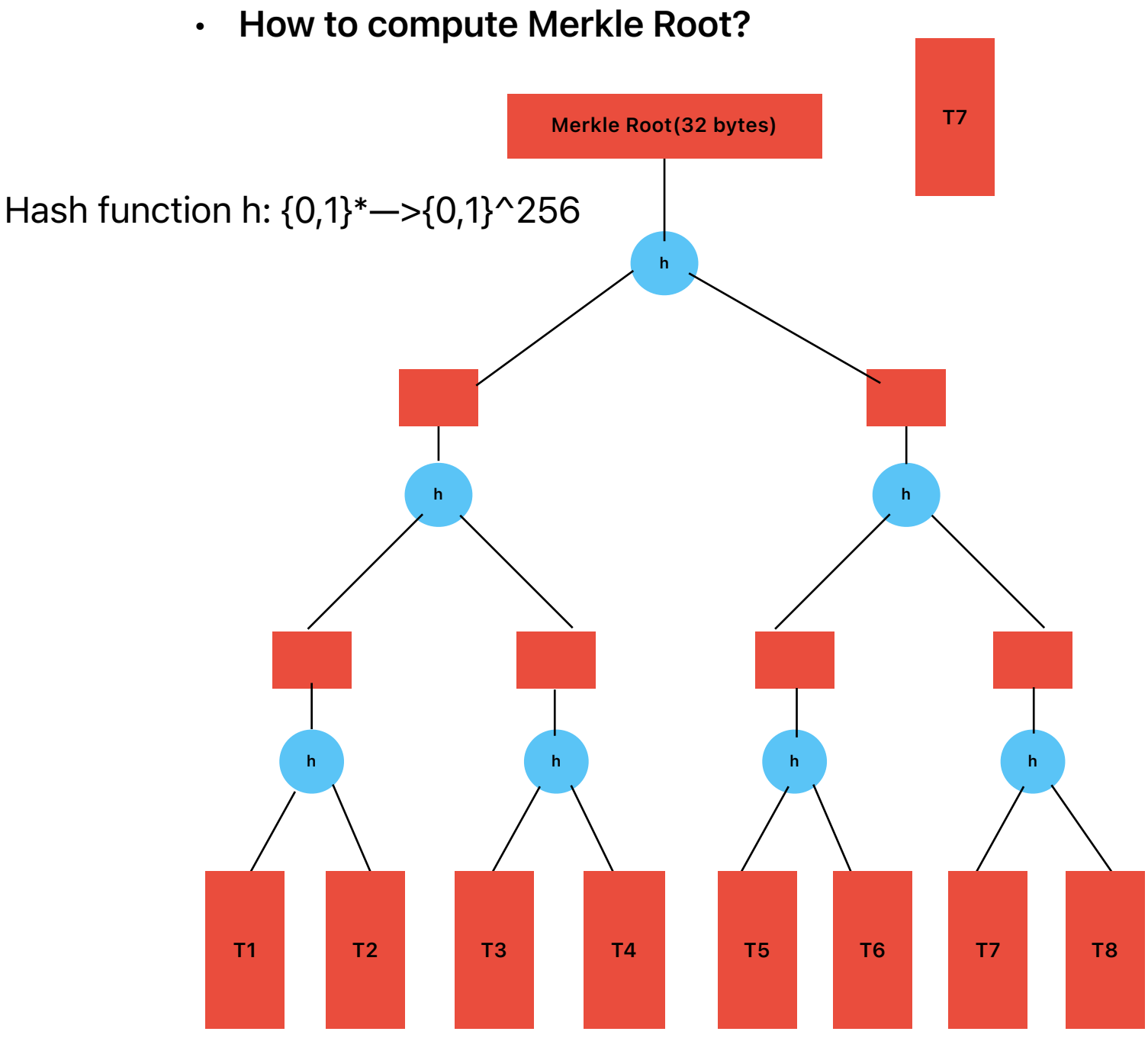


- **How to compute Merkle Root?**



- **How to compute *Current Block Hash* and *nonce* ?**

Choose a *nonce* such that x :=H(Block_header) is less than the *target* then x = Current hash block

Note, Block_hash = (***Nonce***, ***MR***, B, Time, V, PB)

Hash function H: {0,1}*—>{0,1}^256

- **How to compute 32-bit Bits and 256-bit Target?**

Step: 1

Difficulty = Prev_Difficulty*2016*10/(time to mine 2016 last blocks)

Initial Difficulty = 1

Step: 2

Target = 2**224/Difficulty

Step: 3

Bits=Index(8 bits)||Coefficient(24 bits)

Compute *Bits* such that:

Target = Coefficient*2**(8*Index-3)

Exercise 1:
A.Compute Target and Bits, when Difficulty = 8.
B. Suppose, #of nodes=2^50, hashrate = 2^30/node_hour
Determine the expected time taken by the network to generate 1 block.

Exercise 2:

As discussed values of Target and Bits in Bitcoin are adjusted every 2016 Blocks, so that the average Block generation/ mining time remains 10 minutes. Suppose, For Blocks B1, B2, …. B2016, Difficulty = 8, average block generation time is 20 mins.

Compute Target and Bits, for B2017, B2018,…,B4032.

Exercise 3: Is it okay that nonce size is 32-bit, but output of H is 256-bit?