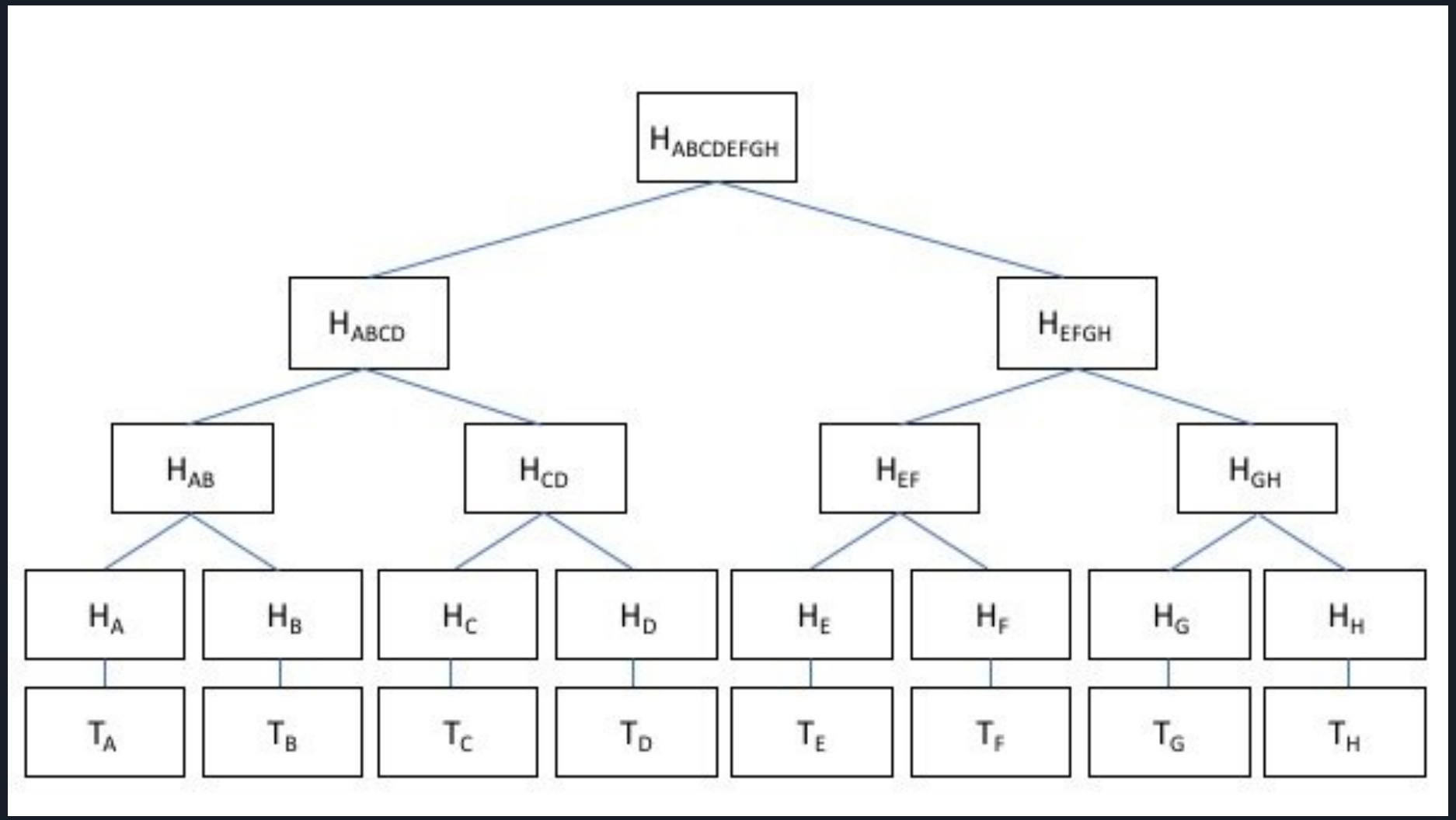
LimeChain

Merkle tree

Fingerprinting off chain data

What is Merkle Tree?


$H_{ABCDEFGH}$
H_{ABCD}
H_{EFGH}
H_{AB}
H_{CD}
H_{EF}
H_{GH}
H_A
H_B
H_C
H_D
H_E
H_F
H_G
H_H
T_A
T_B
T_C
T_D
T_E
T_F
T_G
T_H

Why merkle tree?

Why Merkle tree?

- Quick check of data tampering
- Quick check of existence

How?

- Store the Merkle tree root in smart contract
- Update it regularly
- Provide mechanisms for verification

Let’s code