15/07/24

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

Om Shete
G1_07
2103163

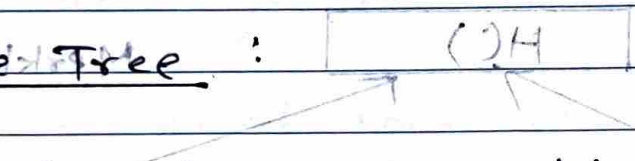
Experiment No : 1

Aim : Write a program to implement Merkle tree showing the cryptographic hash function in Blockchain.

Theory :

- A hash tree is also known as Merkle Tree. It is a tree in which each leaf node is labeled with hash value of data block and each non-leaf node is labeled with the hash value of its child node labels.

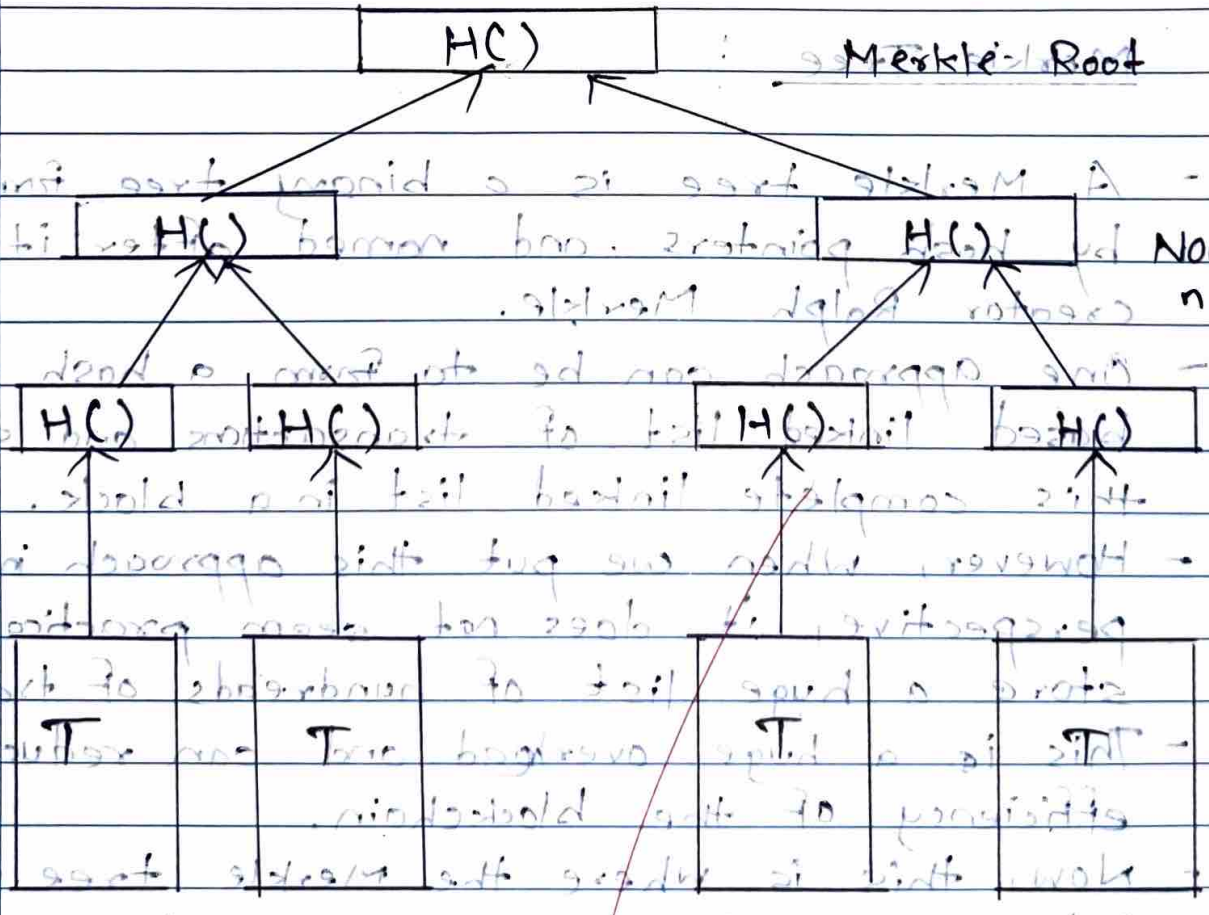
- **Merkle Tree** :



- A Merkle tree is a binary tree formed by hash pointers, and named after its creator Ralph Merkle.
- One approach can be to form a hash pointer-based linked list of transactions and store this complete linked list in a block.
- However, when we put this approach into perspective, it does not seem practical to store a huge list of hundreads of transactions
- This is a huge overhead and can reduce the efficiency of the blockchain.
- Now, this is where the Merkle tree comes into the picture. Merkle tree is a per-block tree of all the transactions that are included in the block.

- It allows us to hash of all transactions and proof of membership in a time-efficient manner.
- Hence, the blockchain is a hash-based linked list of blocks, where each block consists of a header and transactions.
- The transactions are arranged in a tree-like fashion, known as Merkle Tree.

Merkle Tree Structure



H() : Hash value
T : transaction

- A blockchain can potentially have thousands of blocks with thousands of transactions in each block. Therefore, memory space and computing power are two main challenges.
- It could be optimal to use as little data as possible for verifying transactions, which can reduce CPU processing and provide better security and this is exactly what Merkle tree offers.
- In a Merkle tree, transactions are grouped into pairs. The hash is computed for each pair and this is stored in the parent node.
- Now the parent nodes are grouped into pairs and their hash is stored in one level up in the tree. This continues till the root of the tree.
- The different types of nodes in Merkle tree is stored in root :-

1) Root node: The root of Merkle tree is known as the Merkle root and Merkle root is stored in the header of the block.

2) Leaf node: The leaf node contains the hash value of transaction data. Each transaction in the blocks has its data hashed and then this hash value is

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

stored in leaf nodes.

3) Non-leaf Node : The non-leaf nodes contain the hash value of transaction data of their respective children.

- Bitcoin uses the SHA-256 hash function to hash the transaction data continuously till the Merkle root is obtained.
- Further, a Merkle tree is binary in nature.

A+

29/7/24