Experiment No.3
To implement the concept of Merkle root
Date of Performance:
Date of Submission:

AIM: To implement the concept of Merkle root.

Objective: To develop a program to create a cryptogrphich hash using the concept of merkle tree.

Theory:

A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. It allows the user to verify whether a transaction can be included in a block or not.

Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. This hash is called the Merkle Root, or the Root Hash. The Merkle Trees are constructed in a bottom-up approach

Every leaf node is a hash of transactional data, and the non-leaf node is a hash of its previous hashes. Merkle trees are in a binary tree, so it requires an even number of leaf nodes. If there is an odd number of transactions, the last hash will be duplicated once to create an even number of leaf nodes.

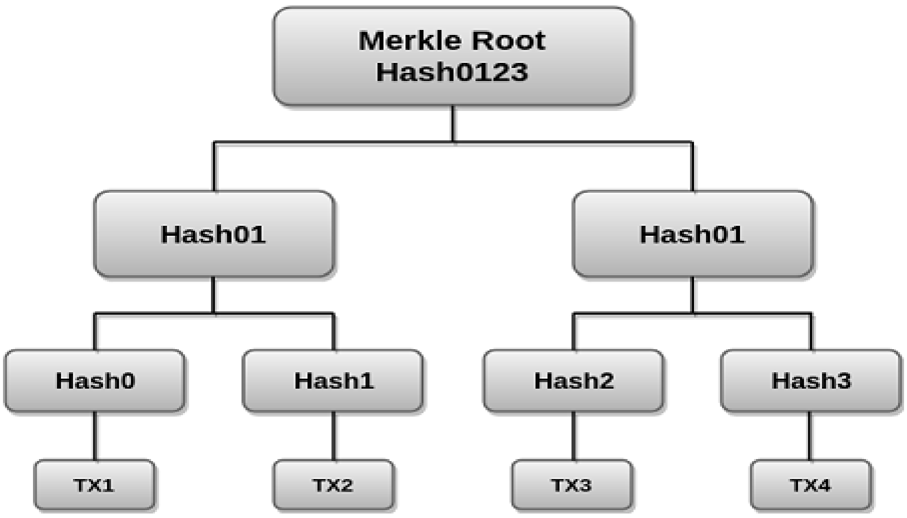

Fig.3.1 Merkle Root Tree Structure

The above example is the most common and simple form of a Merkle tree, i.e., Binary Merkle Tree. There are four transactions in a block: TX1, TX2, TX3, and TX4. Here you can see, there is a top hash which is the hash of the entire tree, known as the Root Hash, or the Merkle Root. Each of these is repeatedly hashed, and stored in each leaf node, resulting in Hash 0, 1, 2, and 3. Consecutive pairs of leaf nodes are then summarized in a parent node by hashing Hash0 and Hash1, resulting in Hash01, and separately hashing Hash2 and Hash3, resulting in Hash23. The two hashes (Hash01 and Hash23) are then hashed again to produce the Root Hash or the Merkle Root.

Merkle Root is stored in the block header. The block header is the part of the bitcoin block which gets hash in the process of mining. It contains the hash of the last block, a Nonce, and the Root Hash of all the transactions in the current block in a Merkle Tree. So having the Merkle root in block header makes the transaction tamper-proof. As this Root Hash includes the hashes of all the transactions within the block, these transactions may result in saving the disk space.

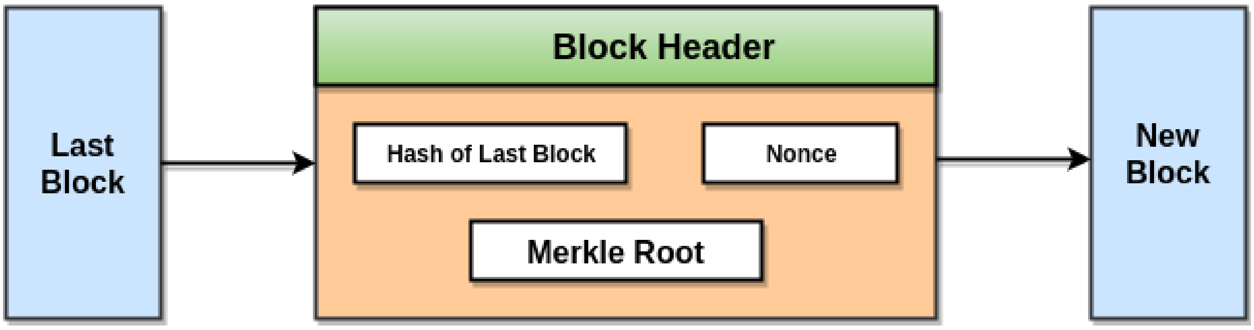

Fig.3.2 Merkle Root in Block

The Merkle Tree maintains the **integrity** of the data. If any single detail of transactions or order of the transaction's changes, then these changes reflected in the hash of that transaction. This change would cascade up the Merkle Tree to the Merkle Root, changing the value of the Merkle root and thus invalidating the block. So everyone can see that Merkle tree allows for a quick and simple test of whether a specific transaction is included in the set or not.

Process:

Step 1. The transaction represents the original data blocks which are hashed to produce transaction hashes (transaction id) which form the leaf nodes.

Step 2. The leaf nodes have to be even in number for a binary hash tree to work so if the number of leaf nodes is an odd number, then the last leaf node is duplicated to even the count.

Step 3. Each pair of leaf nodes is concatenated and hashed to form the second row of hashes.

Step 4. The process is repeated until a row is obtained with only two hashes

Step 5. These last two hashes are concatenated to form the Merkle root.

Output:

```
--- exec:3.1.0:exec (default-cli) @ MerkleTree ---
Transaction List[a, b, c, d, e]
Left-->         a       Right-->        b
sha2HexValue    fb8e20fc2e4c3f248c60c39bd652f3c1347298bb977b8b4d5903b85055620603
Left-->         c       Right-->        d
sha2HexValue    21e721c35a5823fdb452fa2f9f0a612c74fb952e06927489c6b27a43b817bed4
Left-->         e       sha2HexValue    3f79bb7b435b05321651daefd374cdc681dc06faa65e374e38337b88ca046dea
Left-->         fb8e20fc2e4c3f248c60c39bd652f3c1347298bb977b8b4d5903b85055620603        Right-->        21e721c35a5823fdb452
sha2HexValue    12a40550c10c6339bf6f271445270e49b844d6c9e8abc36b9b642be532befe94
Left-->         3f79bb7b435b05321651daefd374cdc681dc06faa65e374e38337b88ca046dea        sha2HexValue    ef5960718ca91ca07e63
Left-->         12a40550c10c6339bf6f271445270e49b844d6c9e8abc36b9b642be532befe94        Right-->        ef5960718ca91ca07e63
sha2HexValue    3b7e1e6ba3b82975d7802511d8c7fabbe7a5d112d0dd112fbcfbb7e6417a3214
root : 3b7e1e6ba3b82975d7802511d8c7fabbe7a5d112d0dd112fbcfbb7e6417a3214
------------------------------------------------------------------------
BUILD SUCCESS
------------------------------------------------------------------------
Total time:  1.816 s
Finished at: 2023-09-12T21:42:26+05:30
------------------------------------------------------------------------
```

Conclusion: The Merkle root is vital for maintaining the integrity of transaction details within a block in a blockchain for several reasons:

Data Integrity: It serves as a condensed representation of all transactions in a block. Any change in even a single transaction would result in a completely different Merkle root, immediately detecting tampering or errors.

Efficiency: Instead of hashing all transactions individually, the Merkle root allows quick verification of the entire block's integrity using a fixed-size hash.

Scalability: As the number of transactions in a block grows, the Merkle root remains a constant size, ensuring efficient verification even as the blockchain expands.

Quick Verification: It enables rapid verification of a transaction's presence in a block without the need to download the entire block, enhancing the efficiency of lightweight clients.

Security: The Merkle root's cryptographic properties ensure that it is practically impossible to find two different sets of transactions that yield the same root hash, safeguarding the blockchain against malicious alterations.

Consensus Mechanism: Miners in proof-of-work and validators in proof-of-stake use the Merkle root in the process of block validation, ensuring that only valid transactions are included in the blockchain.

Chain of Trust: The Merkle root, combined with previous block hashes, forms a chain of trust throughout the blockchain, reinforcing the validity of all transactions back to the genesis block.

Pruning: Full nodes can prune older transactions, retaining only block headers with Merkle roots, saving storage space while still verifying the integrity of the entire blockchain.