COURSE CODE: (DJS22ADL7013)

COURSE NAME: Blockchain Technology Laboratory CLASS: B.Tech

EXPERIMENT NO. 2

CO/LO: Describe basic knowledge of Blockchain technology.

AIM / OBJECTIVE: To implement Merkle root from the transactions and verify the validity of transactions using it.

DESCRIPTION OF EXPERIMENT:

This experiment demonstrates the construction of a Merkle Tree from a set of transactions.
It computes the Merkle Root, which uniquely represents all transactions in the block.
Finally, it verifies the validity of a transaction using Merkle Proof.

Overview of Libraries:

hashlib → Provides secure hash functions (e.g., SHA-256) to generate transaction hashes.

sys / os (optional) → Used for handling input/output or file-based transaction data.

random (optional) → Can be used to generate sample transaction data for testing.

EXERCISE

Example Walkthrough

Suppose transactions = `["Tx1", "Tx2", "Tx3", "Tx4"]`

1. **Hash level-1:**

```
H1 = sha256("Tx1" + "Tx2")
H2 = sha256("Tx3" + "Tx4")
```

Now: `[H1, H2]`

2. **Hash level-2:**

```
Merkle Root = sha256(H1 + H2)
```

Final output → Merkle Root

```python
import hashlib

def build_merkle_tree(transactions):
    if len(transactions) == 0:
        return None
    if len(transactions) == 1:
        return transactions[0]

    while len(transactions) > 1:
        # If odd number of transactions, duplicate the last one
        if len(transactions) % 2 != 0:
            transactions.append(transactions[-1])

        new_transactions = []
        for i in range(0, len(transactions), 2):  # step=2 to take pairs
            combined = transactions[i] + transactions[i+1]
            hash_combined = hashlib.sha256(combined.encode()).hexdigest()
            new_transactions.append(hash_combined)

        transactions = new_transactions

    return transactions[0]


# Example usage
transactions = ["Transaction 1", "Transaction 2", "Transaction 3", "Transaction 4", "Transaction 5"]
merkle_root = build_merkle_tree(transactions)
print("Vinit Pandey\n60019220126\nB039\n")
print("Merkle Root:", merkle_root)
```

Result:

```
Vinit Pandey
60019220126
B039
Merkle Root: a4a18941de1162b17a46c4f8c87d8a0850b46fad17ac881340061d9233785077
```

QUESTIONS:

1. Explain the concept of Markle Tree in detail.

REFERENCE:

Website References:

1.https://www.geeksforgeeks.org/software-engineering/blockchain-merkle-trees/
.