Execution Layer

Blockchain @ uninsubria

Roberto Vicario

2024/2025

Contents

1 Execution Layer

The *Execution Layer* is a critical component of blockchain systems, responsible for executing transactions and maintaining the state of the blockchain. It operates on top of the consensus layer, which ensures that all nodes agree on the order of transactions.

2 UTXO (Unspent Transaction Output) Model

The *UTXO* model is used in Bitcoin. It represents the state of the blockchain as a set of unspent transaction outputs, which can be used as inputs for new transactions.

$\boxed{DEFINITION}$

Given a UTXO block U_i in the blockchain, and let $TX_i = \{tx_1, ..., tx_n\}$ be the set of transactions included in the block, organized in a Merkle tree with root hash h_{root}. The block U_i can be defined as:

$$U_i = (H_{i-1}, MT(h_{\text{root}})) \tag{1}$$

2.1 Merkle Tree

A *Merkle Tree* is a data structure that allows efficient verification that a transaction is included in a block, without needing all the data.

$\boxed{SEARCHING}$

1. **Initialization:** Client stores the root hash of the Merkle tree h_{root}.
2. **Forwarding:** Prover sends to the client the transaction hash TX_i and the Merkle proof:

   $$\Pi = \{h_1, h_2, ..., h_k\}$$

   Where each h_i is a hash at some level of the tree.
3. **Verification:** Starting from tx_i, the client combines it with each h_i, following the tree path:

   $$h' = H(H(H(tx_i \parallel h_1) \parallel h_2) \parallel ... \parallel h_k)$$

4. **Termination:** The client accepts if the final hash equals the stored Merkle root:

$$h' = h_{\text{root}}$$

3 Account-based Model

The *Account-based Model* is used in Ethereum. It represents the state of the blockchain as a set of accounts, each with its own metadata.

The two main types of accounts in the account-based model are:

- **Externally Owned Account (EOA):** Controlled by a private key, can send transactions.
- **Contract Account:** Contains code and storage, can execute smart contracts.