



# **polygon zkEVM**

**Knowledge Layer**

**Concepts**

**Ethereum State**

**Version: 311a75456c7ba5065a20ba1a381783f45df27c54**

January 9, 2024

# 1 Ethereum State

The **Ethereum World State** refers to a data structure designed to maintain a record of the Ethereum blockchain's current status. It contains all the data from the Ethereum accounts such as balances or nonces. The concrete data structure used to store the Ethereum state is called Ethereum Patricia Trie. Next, we provide the specification of account's data elements tracked by the Ethereum state, distinguishing between *Externally Owned Accounts (EOAs)* and *Contract Accounts*.

**Externally Owned Accounts (EOAs)** These accounts are controlled by users who know the associated private keys. The state of an EOA is defined by the values of the following parameters:

- **balance:** The balance of an EOA represents the amount of Ether (ETH), or more correctly, the amount of Wei with  $1 \text{ Wei} = 10^{-14} \text{ ETH}$  that the account holds. This information is vital for conducting transactions, as it ensures that the account has the necessary funds to do Ether transfers or pay the transaction fees.
- **nonce:** The nonce associated with an EOA serves as a transaction counter, tracking the number of transactions initiated from the account. This counter serves as a preventive measure against **replay attacks**, ensuring that previous transactions are not re-executed.

**Contract Accounts** A contract account is managed by code executed by the Ethereum Virtual Machine (EVM). It is also referred to as a Smart Contract. Contract accounts have associated code and data storage, but not private keys. The state of a contract account is defined by the values of the following parameters:

- **balance:** Similar to EOAs, contract accounts maintain a balance, which denotes the amount of Wei held within the contract.
- **nonce:** Contract accounts have their own nonce. The nonce of a contract account works as in EOAs.
- **codeHash:** For each Contract account, the Ethereum state includes the deployed bytecode of the contract. This code is immutable once deployed and can be executed by sending transactions to the contract's address. All such code fragments are contained in the state database under their corresponding hashes for later retrieval. This hash value is known as a **codeHash**.
- **storageRoot:** Smart contracts can store persistent data in their storage space. This storage space is organized as a key-value store and is specific to each contract. All the contracts storage key-values form part of the Ethereum World State. This key-value structure is contained in the state database storing only the root of a Merkle Patricia trie that encodes it.

As we have said before, the Ethereum World State is implemented using a data structure known as a Merkle Patricia Trie, which is a compact way to organize and store the data of all Ethereum accounts, permitting efficient data look ups. The root hash of the World State Tree is included in each block's header, allowing for quick verification of the state at a particular block. It ensures the integrity and consistency of the state throughout the blockchain.