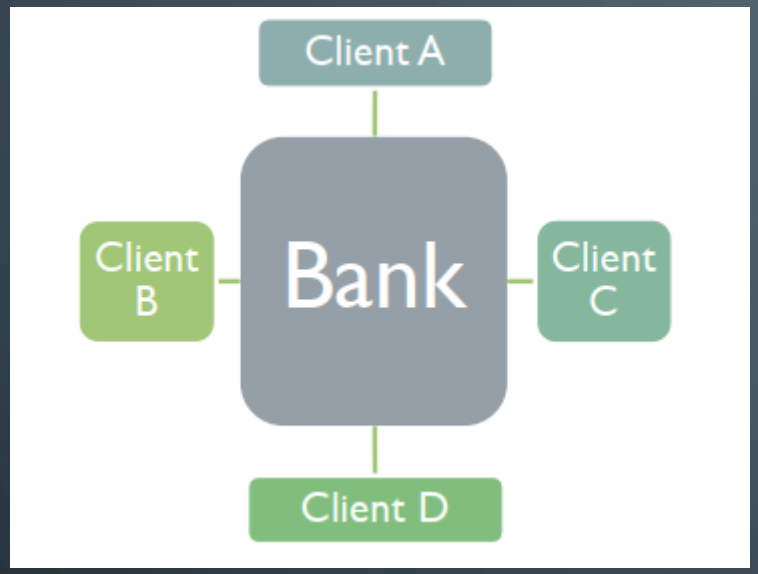
BLOCKCHAIN CONCEPTS

WHAT IS BLOCKCHAIN

- A distributed database
  - Protected against modifications or deletions
  - Can only grow with new data (ledger)
  - It's organized as a chain of data blocks
- Data recorded in a blockchain are transactions
- The ledger is accessed and stored by different servers, organized as a peer-to-peer network
- Blocks of transactions are cryptographically chained at chronological order
- Transactions can be verified by anyone and bound cryptographically (non-repudiation) to the emitter
- Transactions, usually, transfer the ownership of something

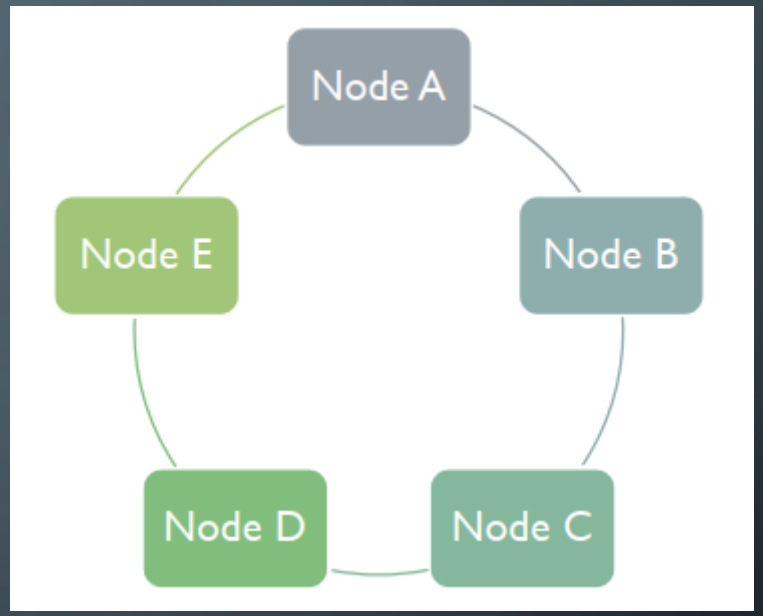
CENTRALIZED VS DISTRIBUTED

Centralized



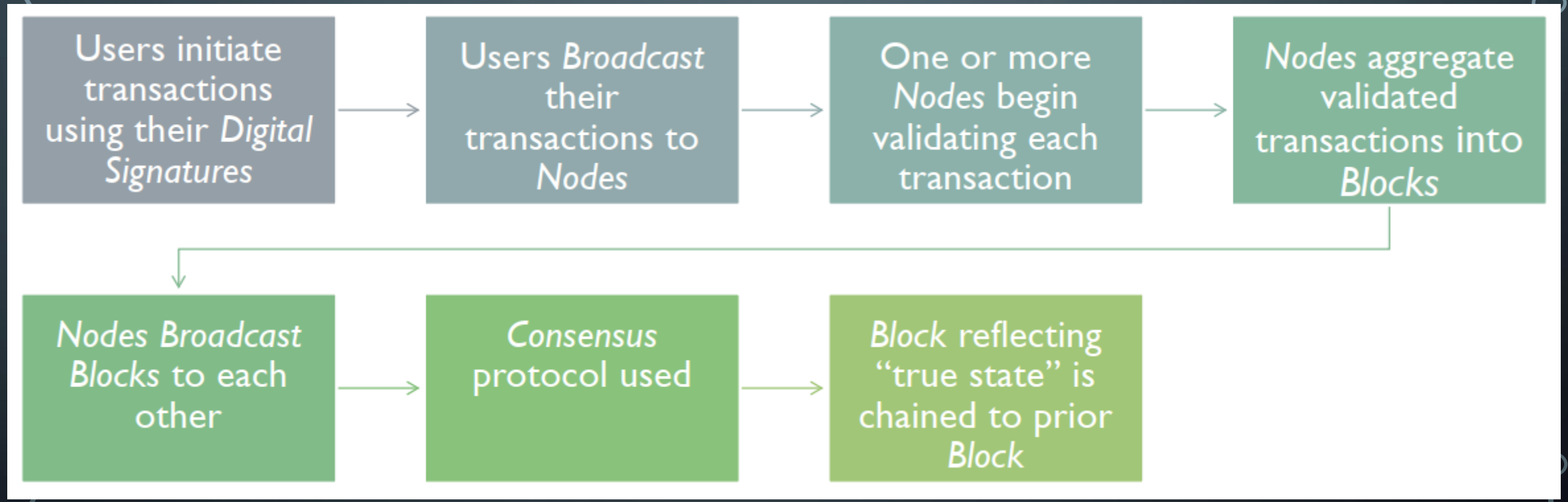
All clients access and request transactions to a single server holding and the data considered the 'true state' and the 'golden record'

Distributed



There is only one ledger, but it can be replicated and all nodes have some level of access to it. All nodes agree on a protocol to determine the 'true state' and to add verified transactions. This protocol is called 'achieving consensus'.

HOW A BLOCKCHAIN WORK?



BLOCKCHAIN USE OF CRYPTOGRAPHY

Initiation and Broadcasting of Transaction	• *Digital Signatures* • *Private/Public Keys*
Validation of Transaction	• *Proof of Work and certain alternatives*
Chaining Blocks	• *Hash Function*

BLOCKCHAIN PROPERTIES

It *can be used* without a central authority by individuals or entities with no basis to trust each other

It *can be used* to create value or issue assets

It *can be used* to transfer value or the ownership of assets

- A human being or a Smart Contract can initiate the transfer

It *can be used* to record those transfers of value or ownership of assets

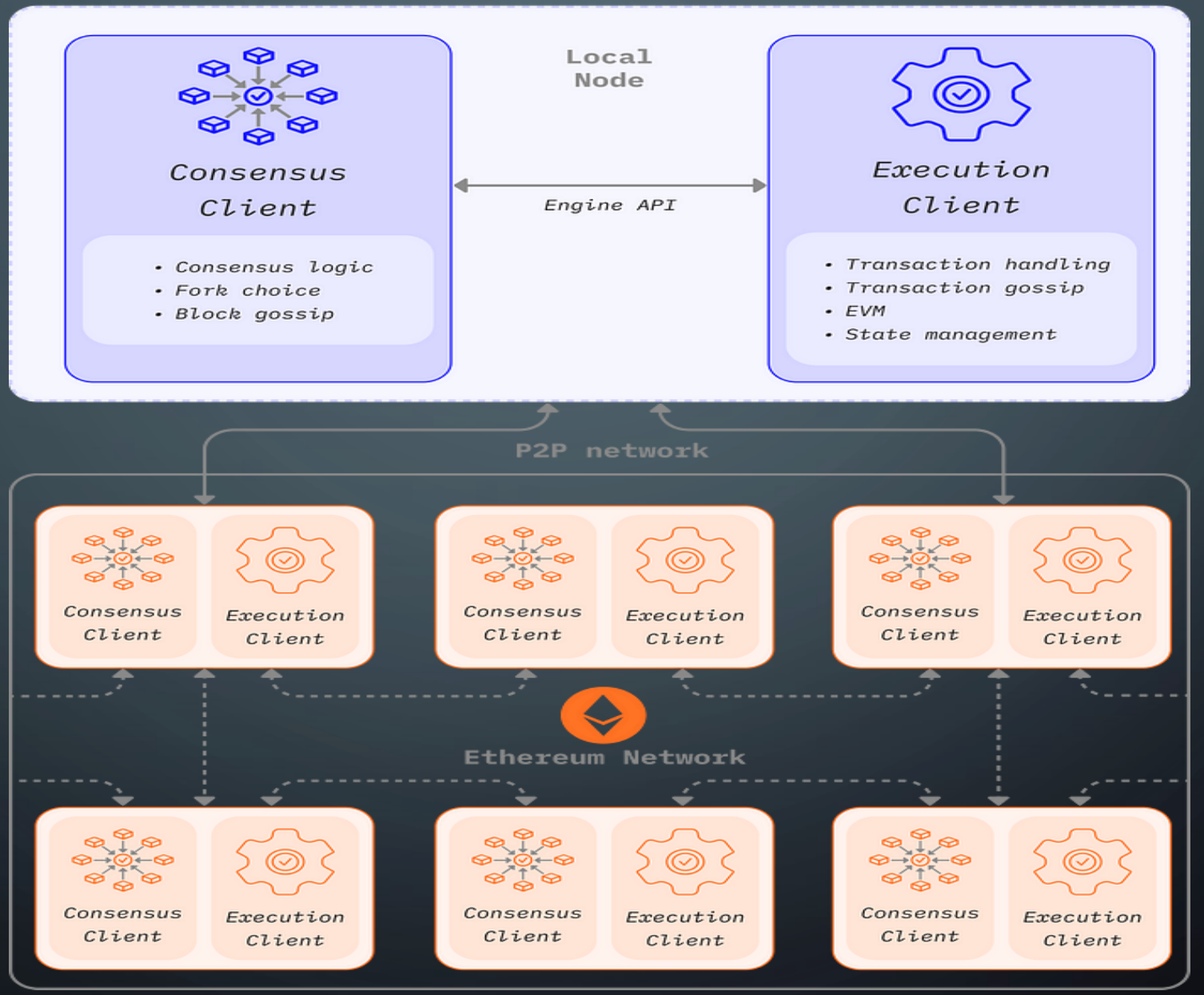
- These records may be very difficult to alter, such that they are sometimes called effectively immutable

It *can be used* to allow owners of assets to exercise certain rights associated with ownership, and to record the exercise of those rights.

- Proxy Voting

BLOCKCHAIN APPLICATIONS

ETHEREUM BLOCKCHAIN

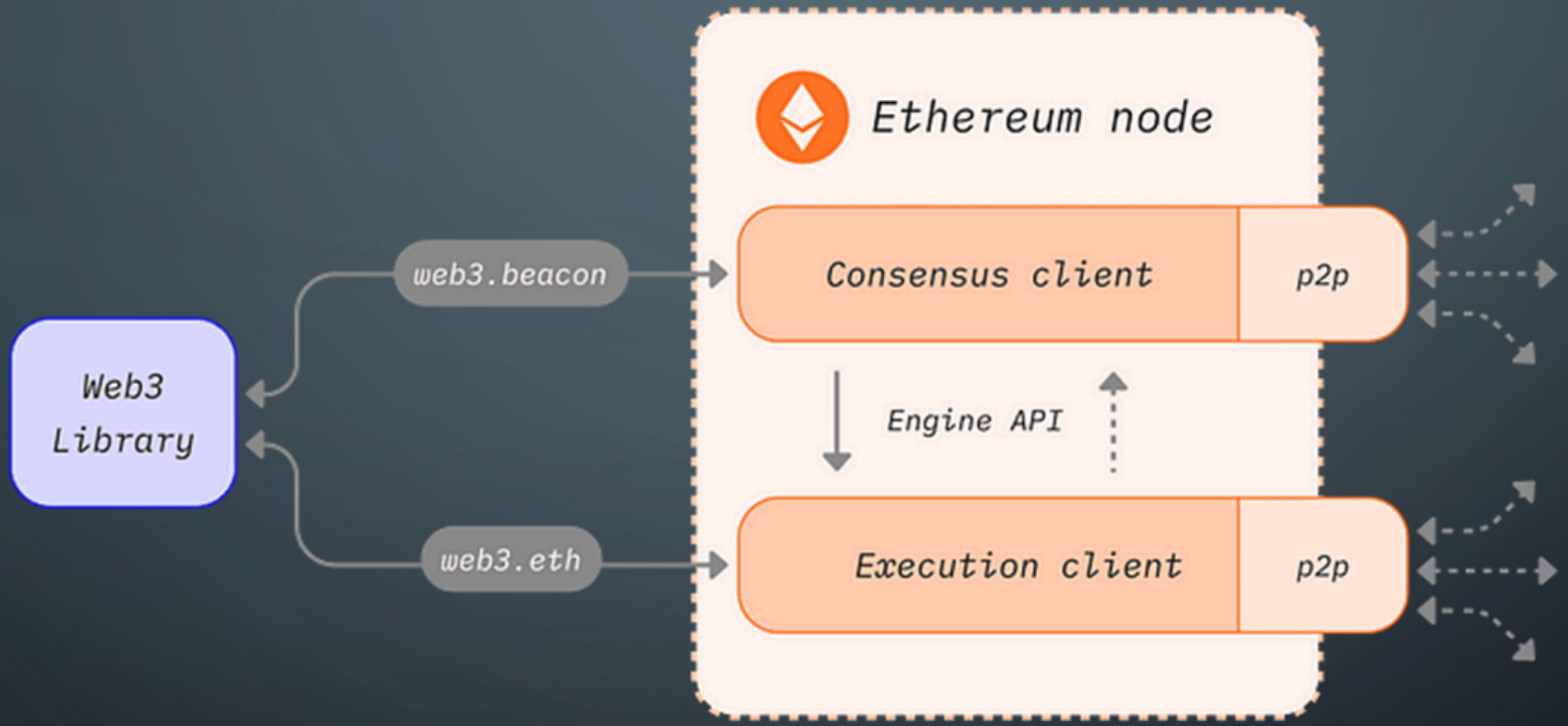


ETHEREUM NODES

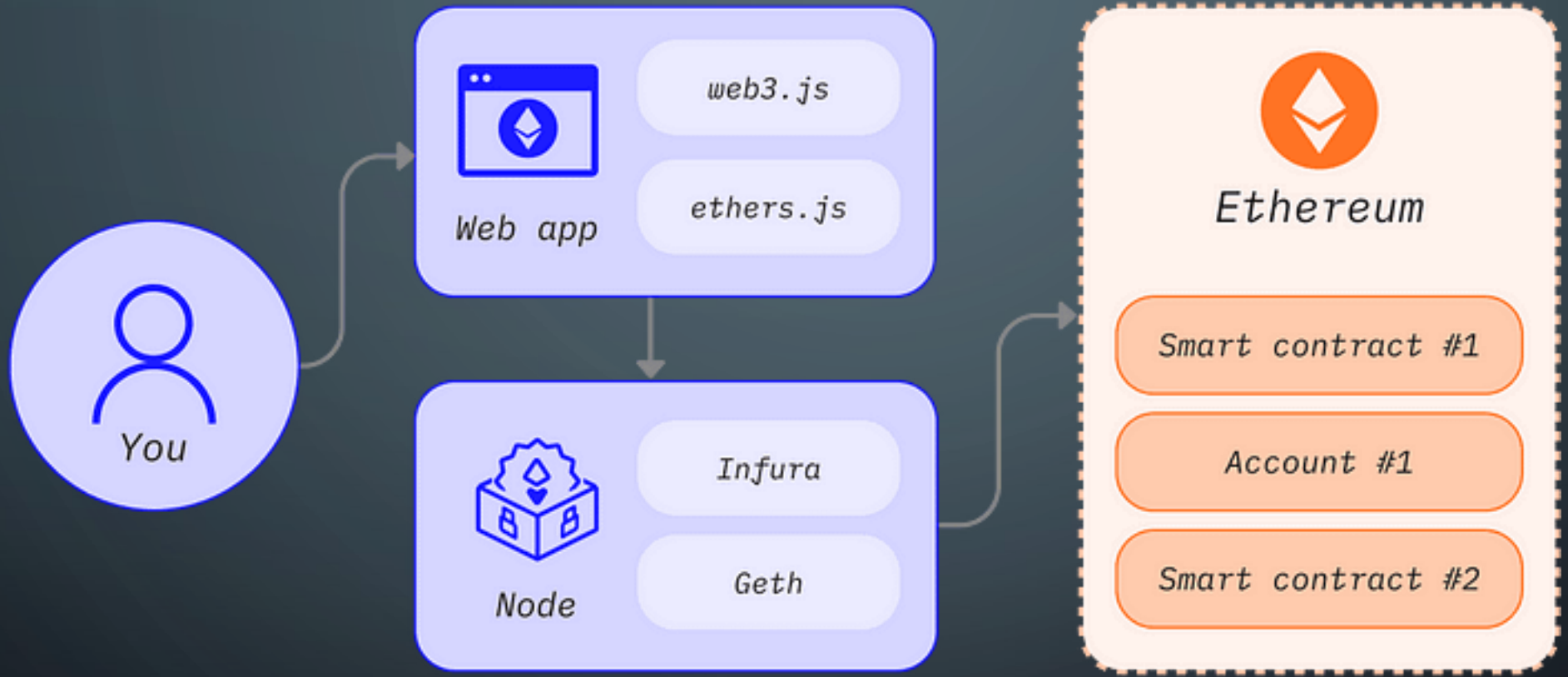
COMPONENTS OF A NODE COMPARISON

Execution Client	Consensus Client	Validator
Gossips transactions over its p2p network	Gossips blocks and attestations over its p2p network	Proposes blocks
Executes/re-executes transactions	Runs the fork choice algorithm	Accrues rewards/penalties
Verifies incoming state changes	Keeps track of the head of the chain	Makes attestations
Manages state and receipts tries	Manages the Beacon state (contains consensus and execution info)	Requires 32 ETH to be staked
Creates execution payload	Keeps track of accumulated randomness in RANDAO	Can be slashed
Exposes JSON-RPC API for interacting with Ethereum	Keeps track of justification and finalization	

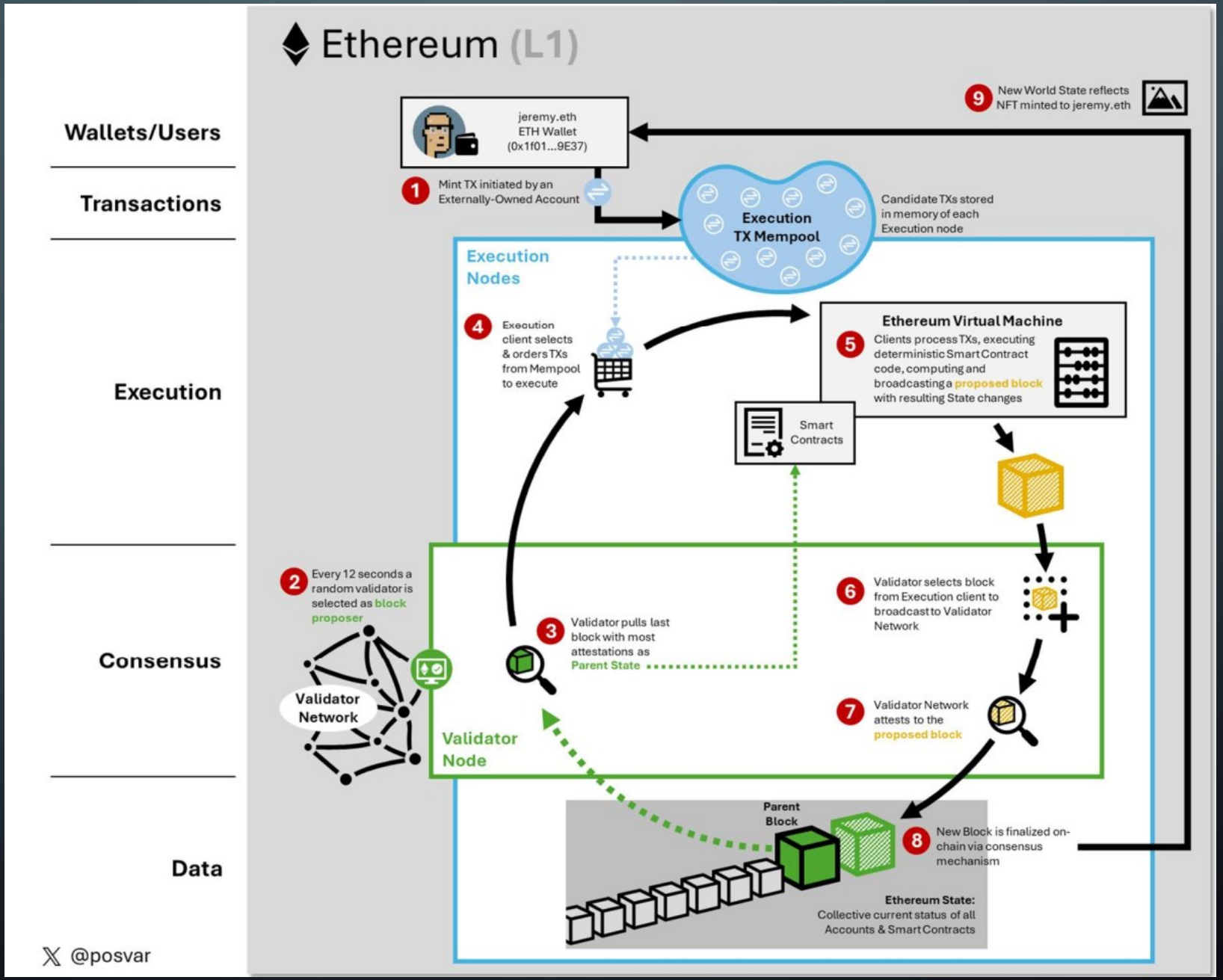
AN ETHEREUM NODE



INTERACTION WITH A NODE



AN ETHEREUM TRANSACTION



ETHEREUM VIRTUAL MACHINE AND SMART CONTRACTS

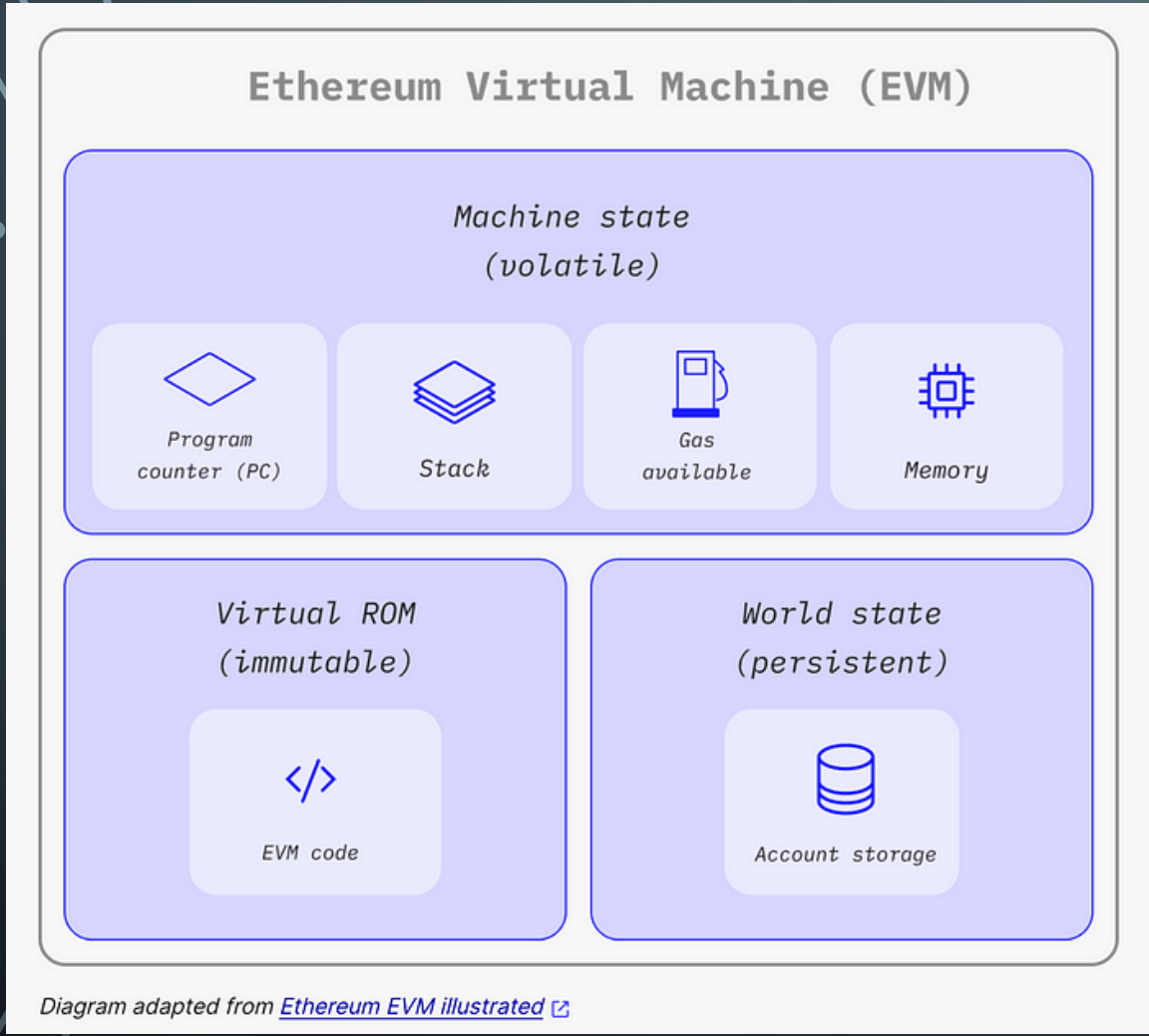
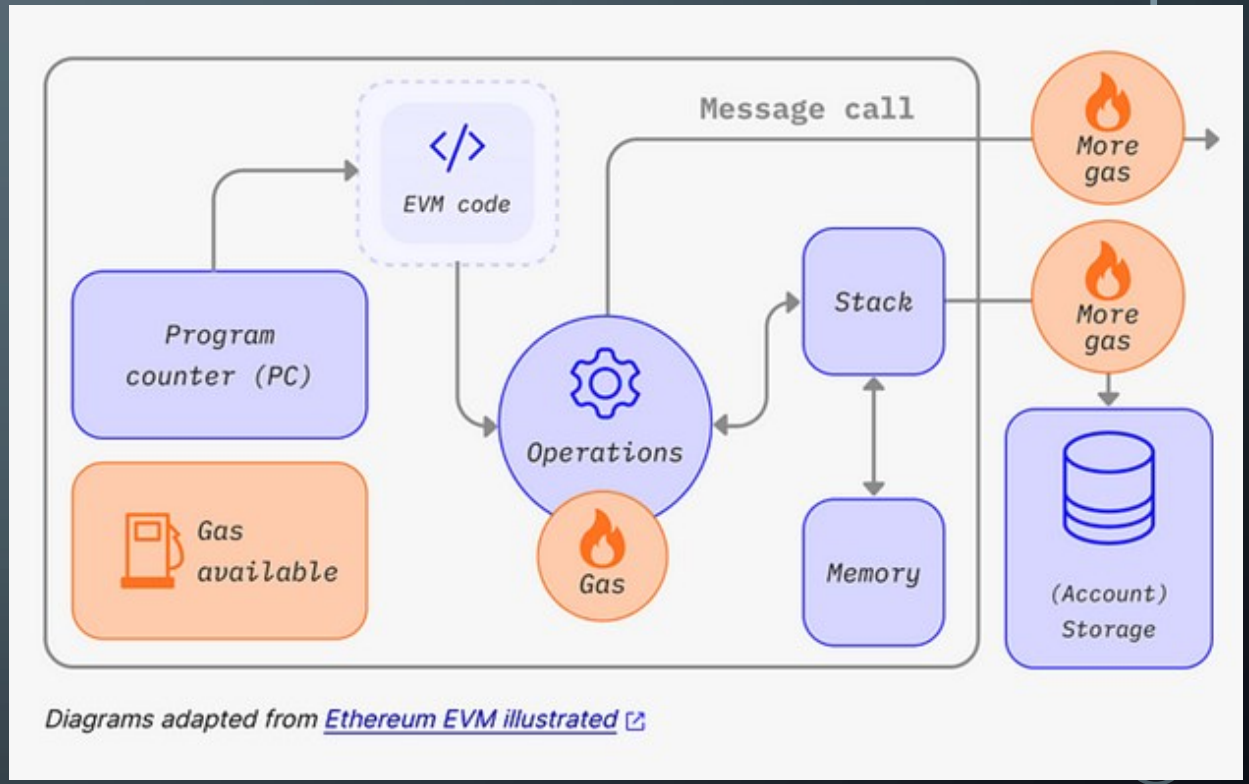
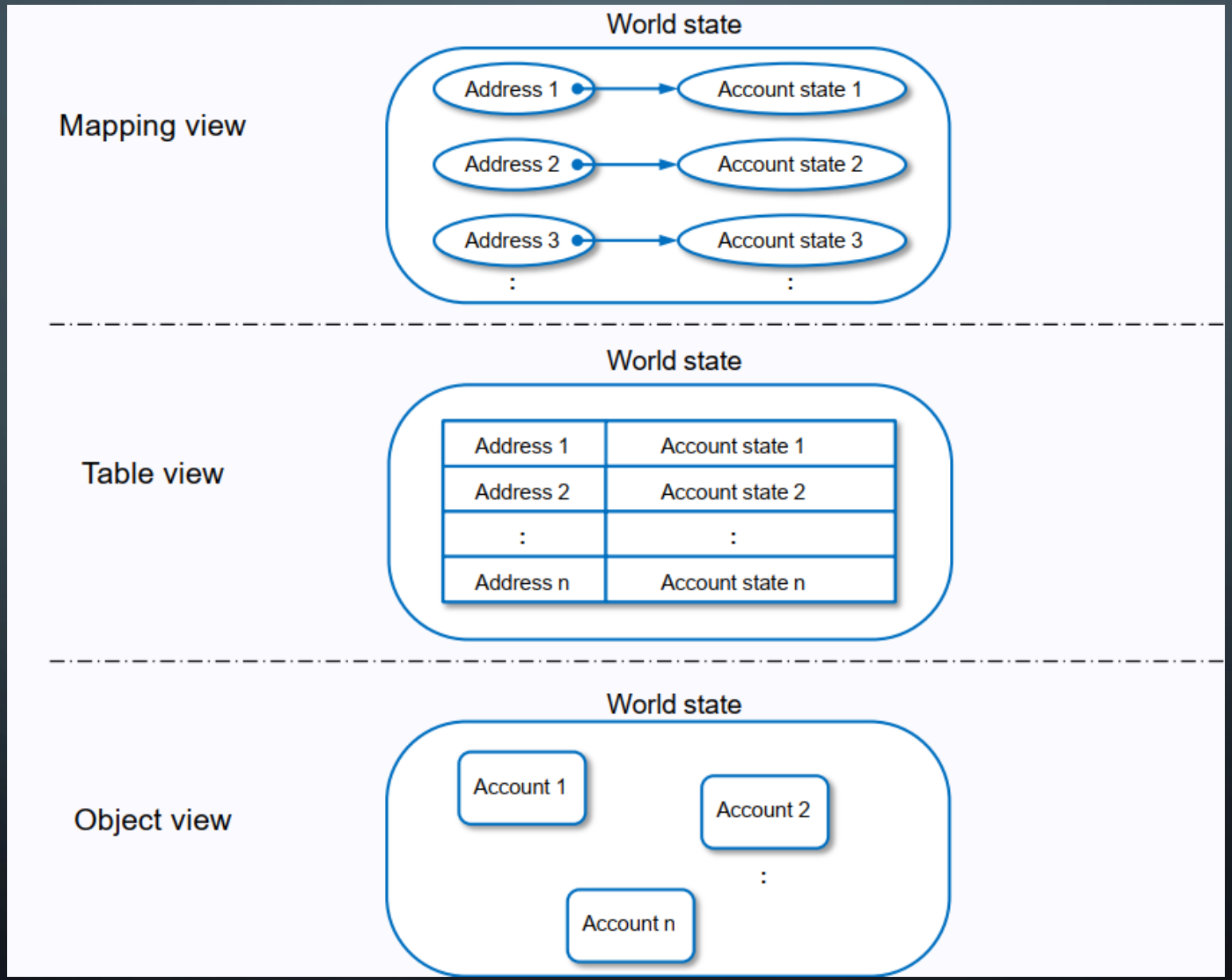


Diagram adapted from Ethereum EVM illustrated

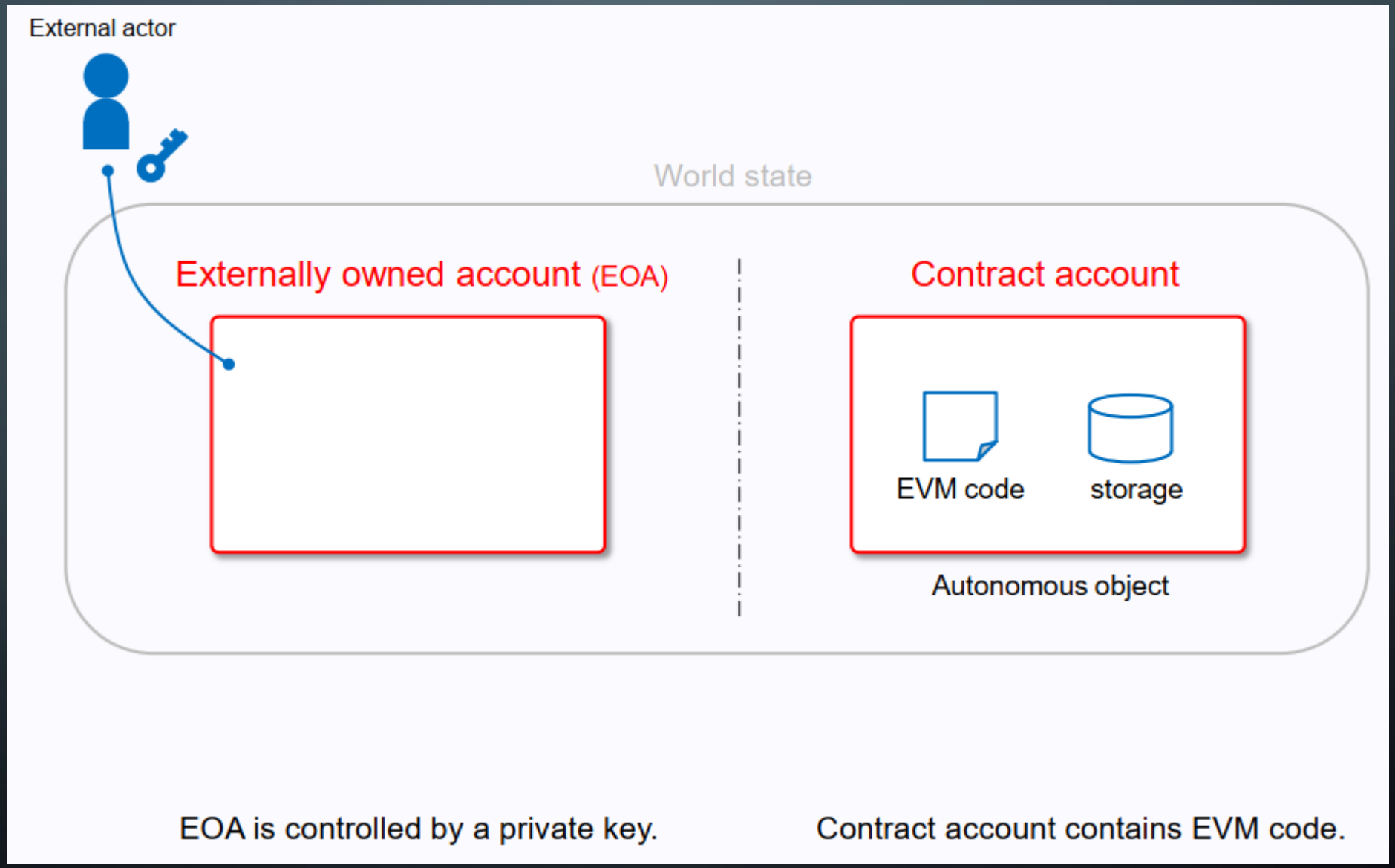


Diagrams adapted from Ethereum EVM illustrated

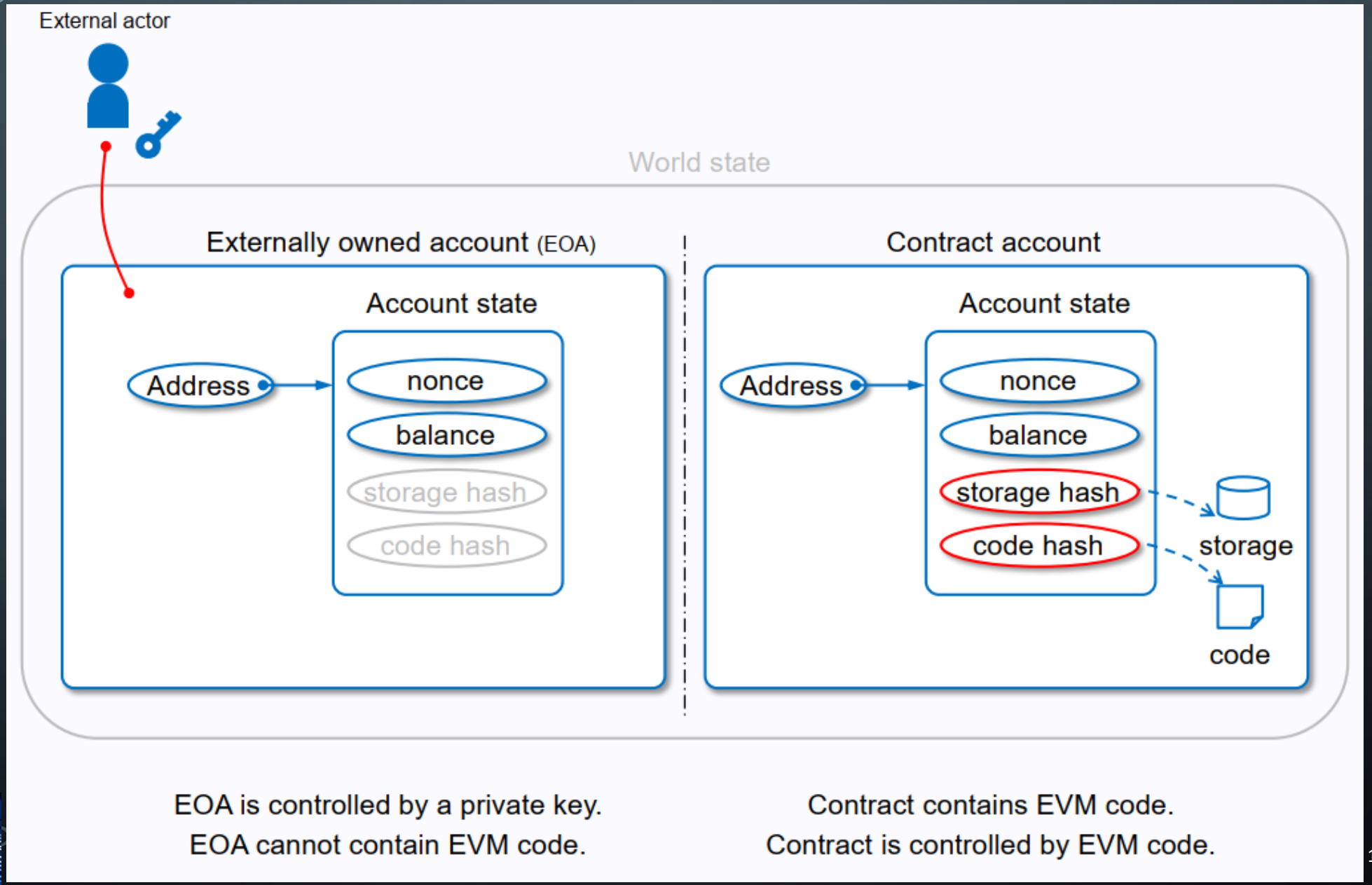
SEVERAL VIEWS OF WORLD STATE



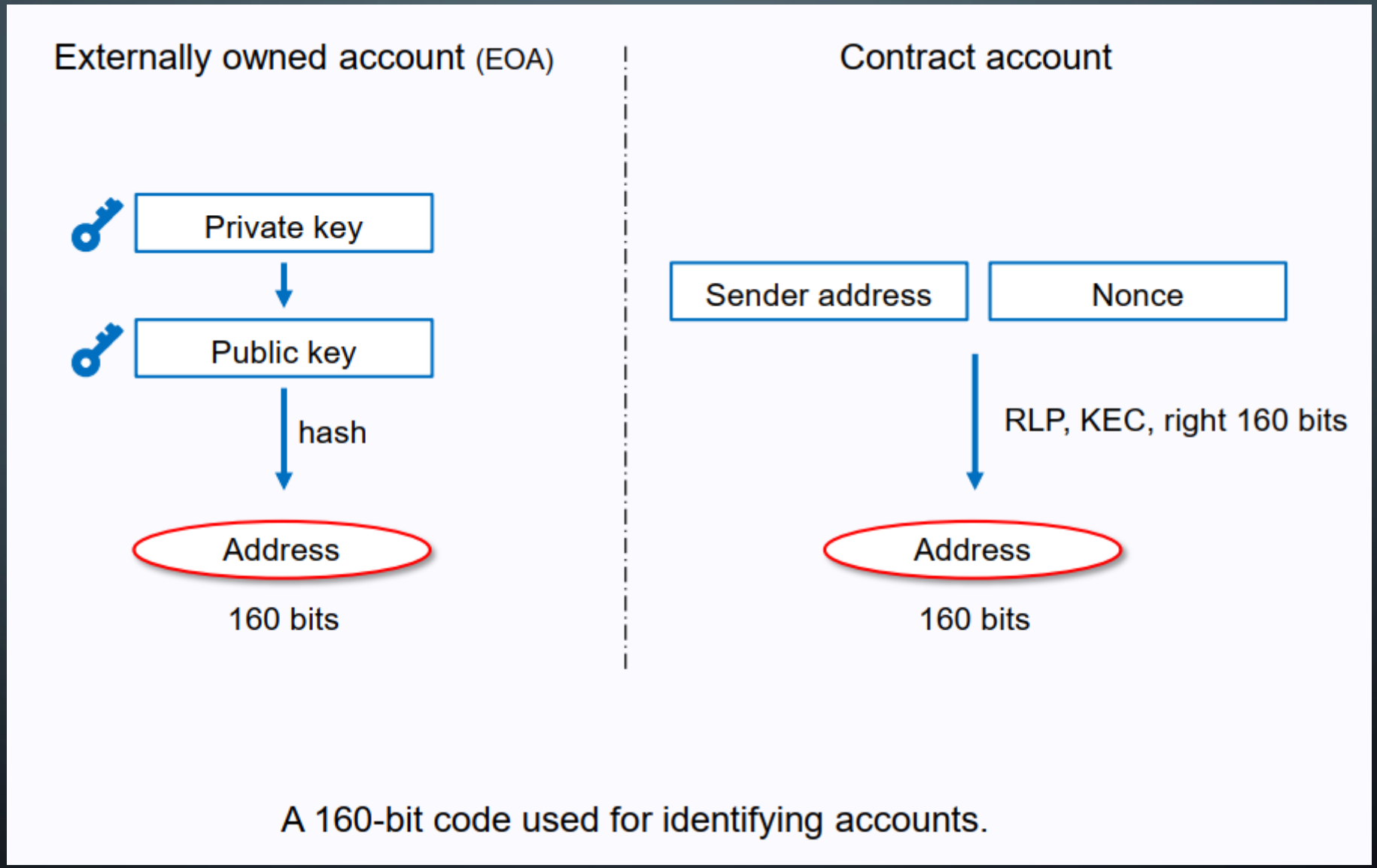
THE TWO TYPES OF ACCOUNTS



ACCOUNT STATE

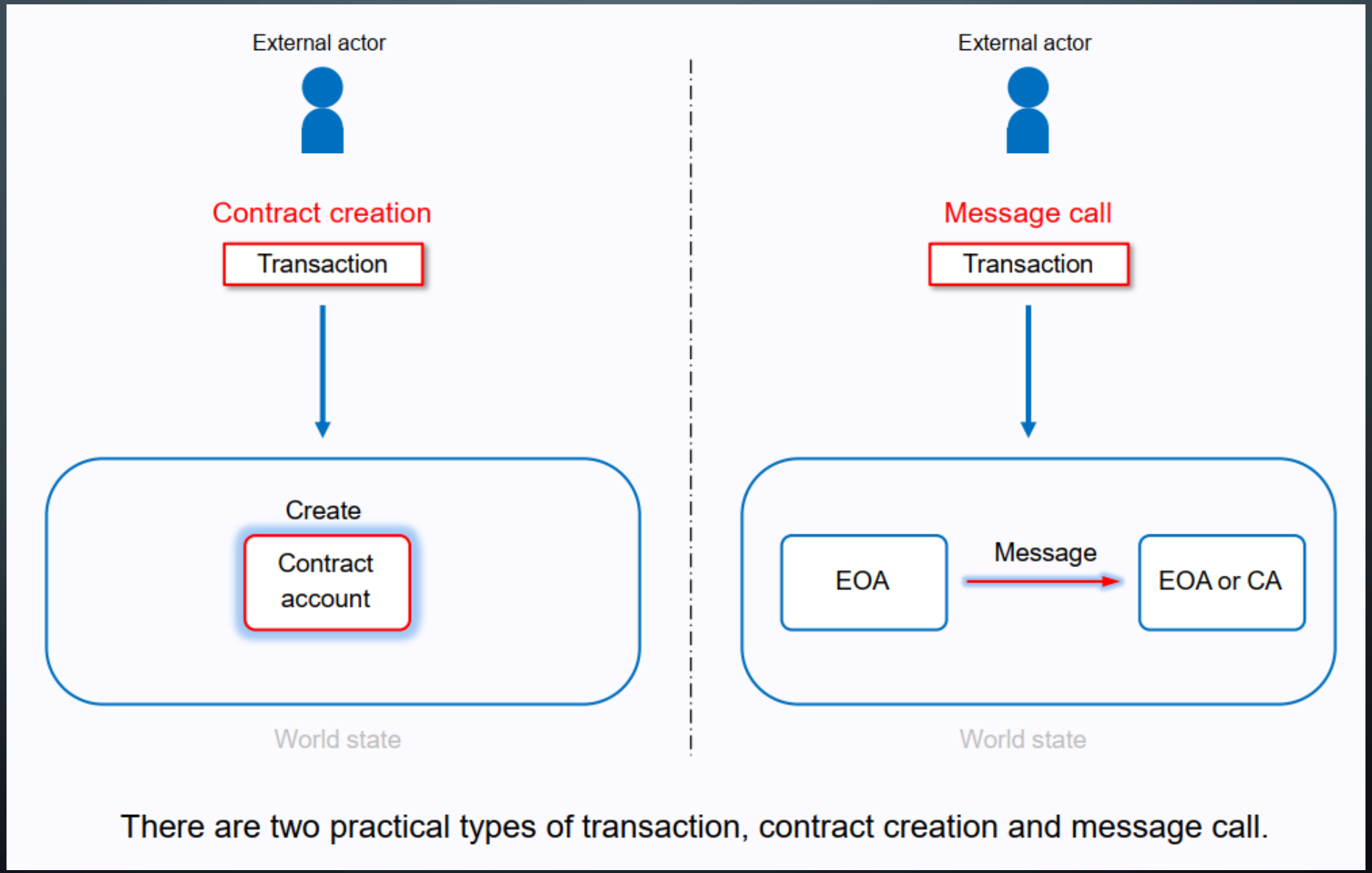


THE ACCOUNT ADDRESS



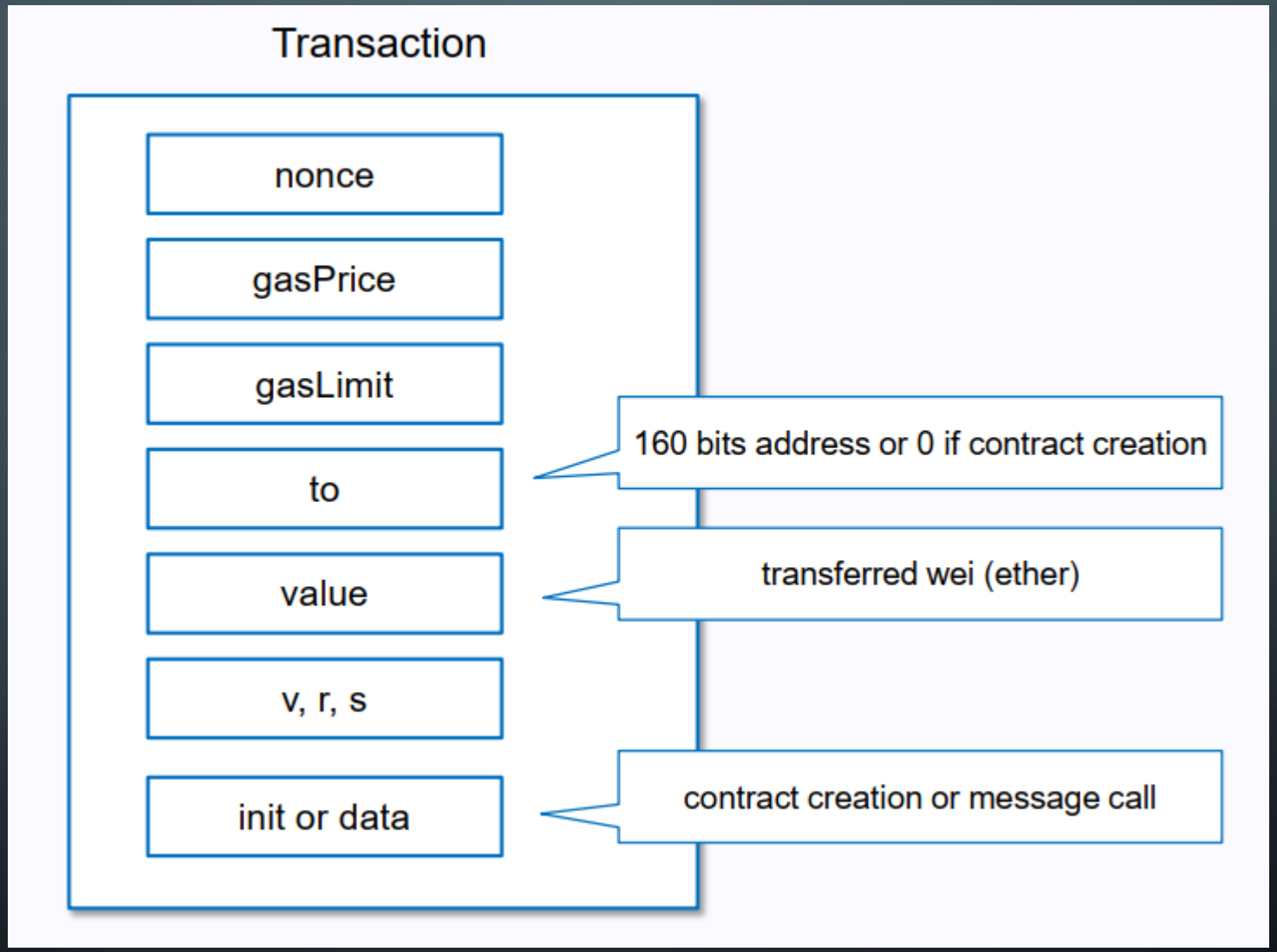
RLP – Recursive-Length Prefix serialization operation

TYPES OF TRANSACTIONS

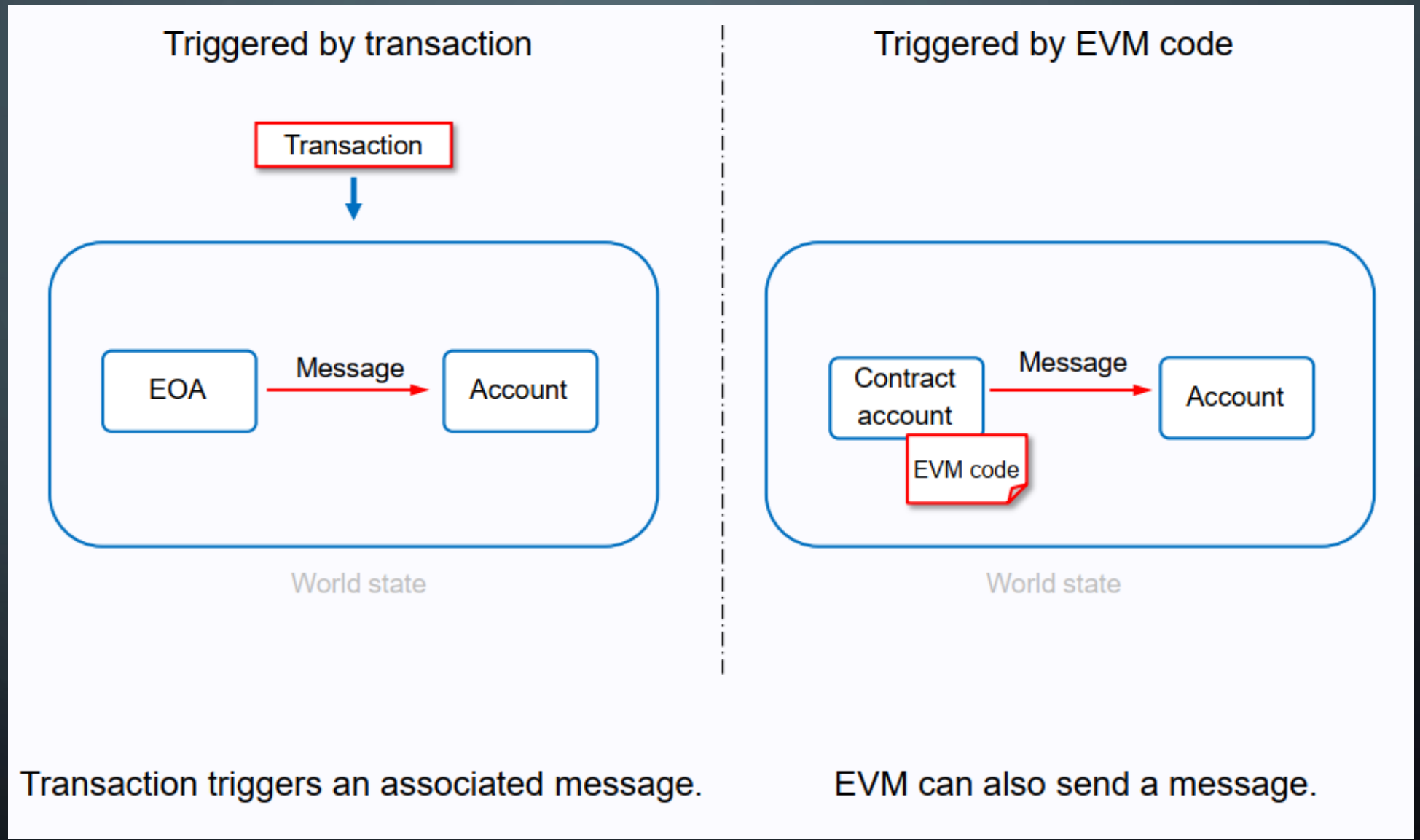


There are two practical types of transaction, contract creation and message call.

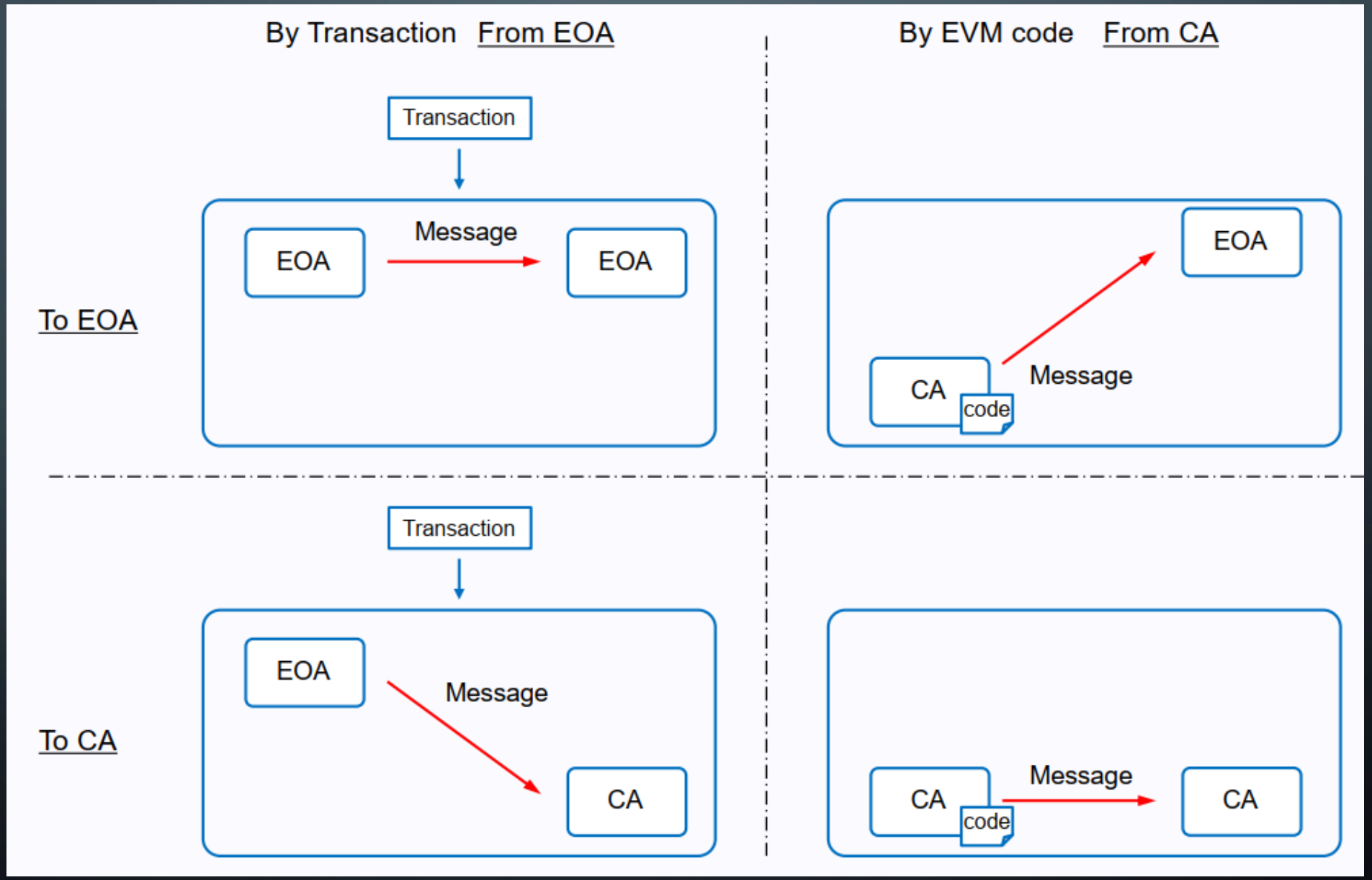
TRANSACTION INFO



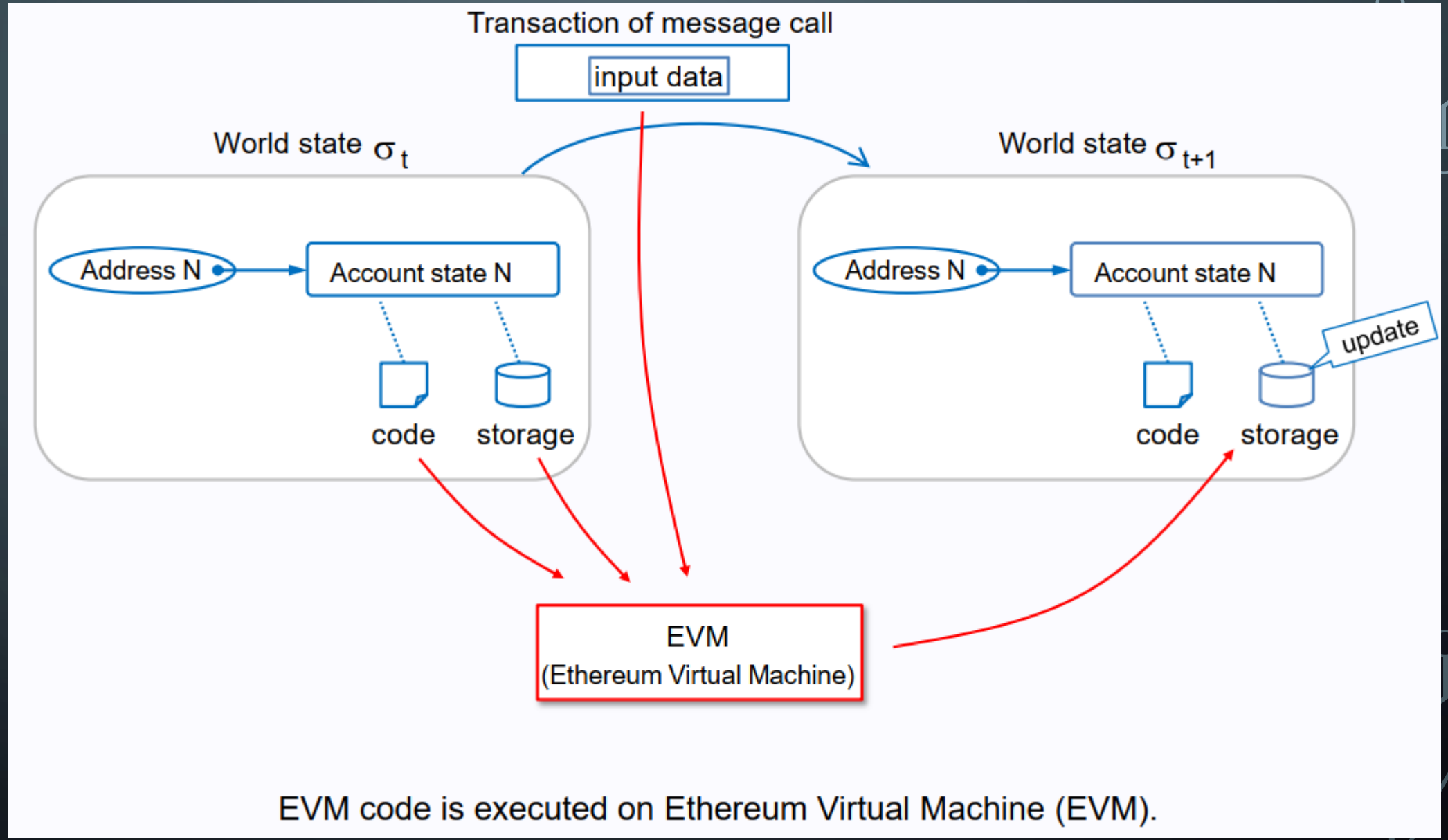
MESSAGES


Triggered by transaction
Transaction
EOA
Message
Account
World state
Triggered by EVM code
Contract account
Message
Account
EVM code
World state
Transaction triggers an associated message.
EVM can also send a message.

CASES OF MESSAGES

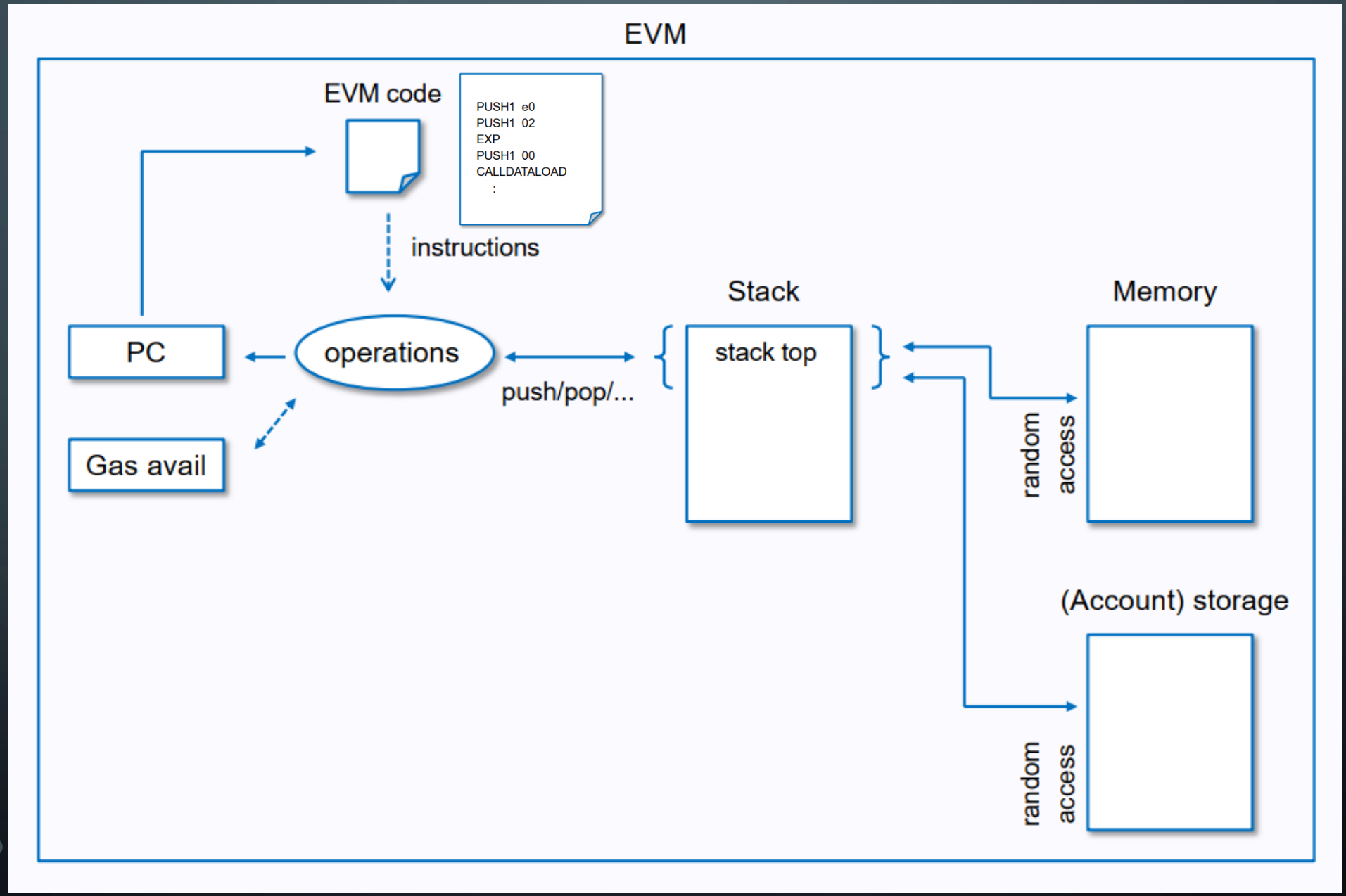


OPERATION OF EVM

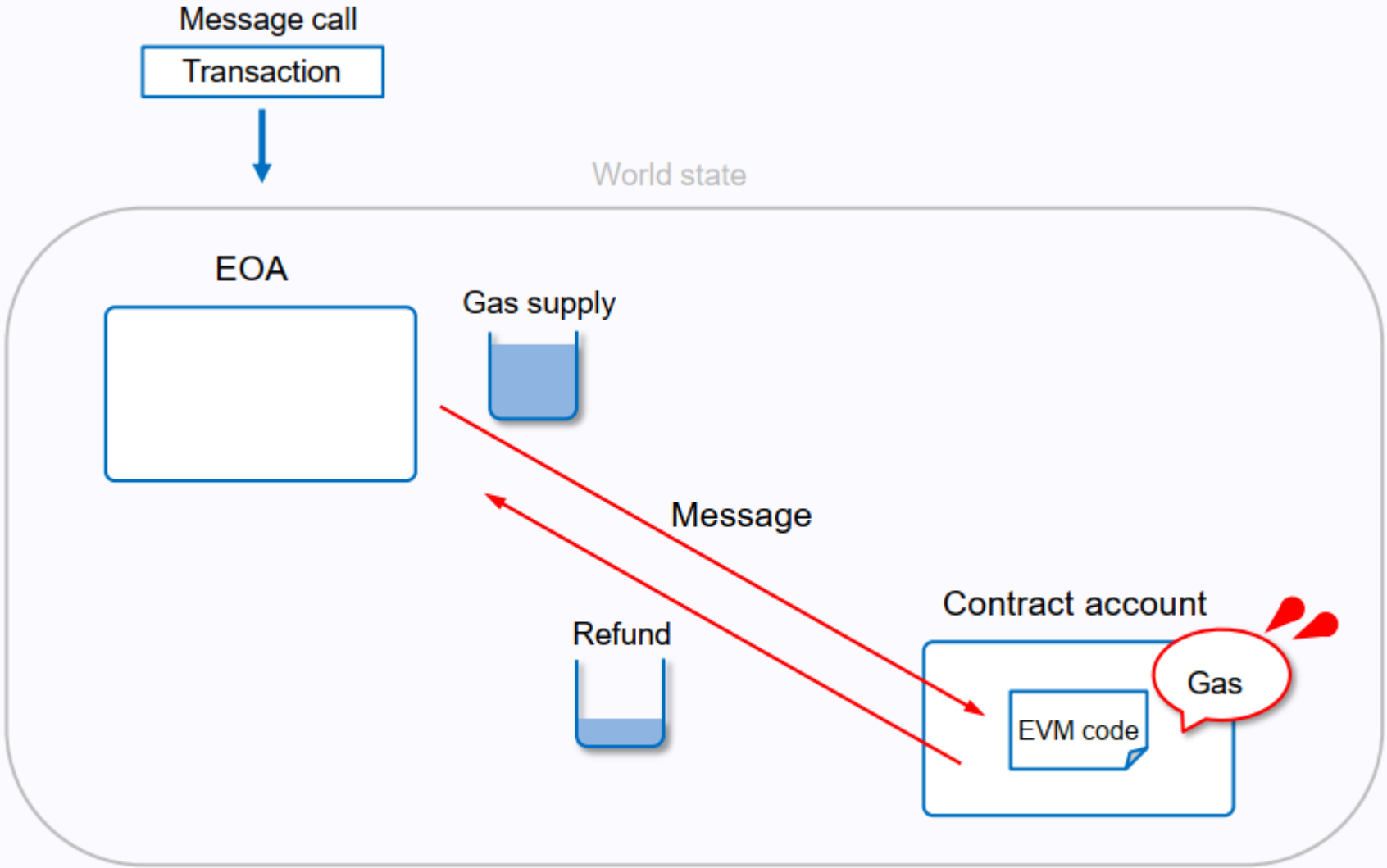


EVM code is executed on Ethereum Virtual Machine (EVM).

EXECUTION MODEL

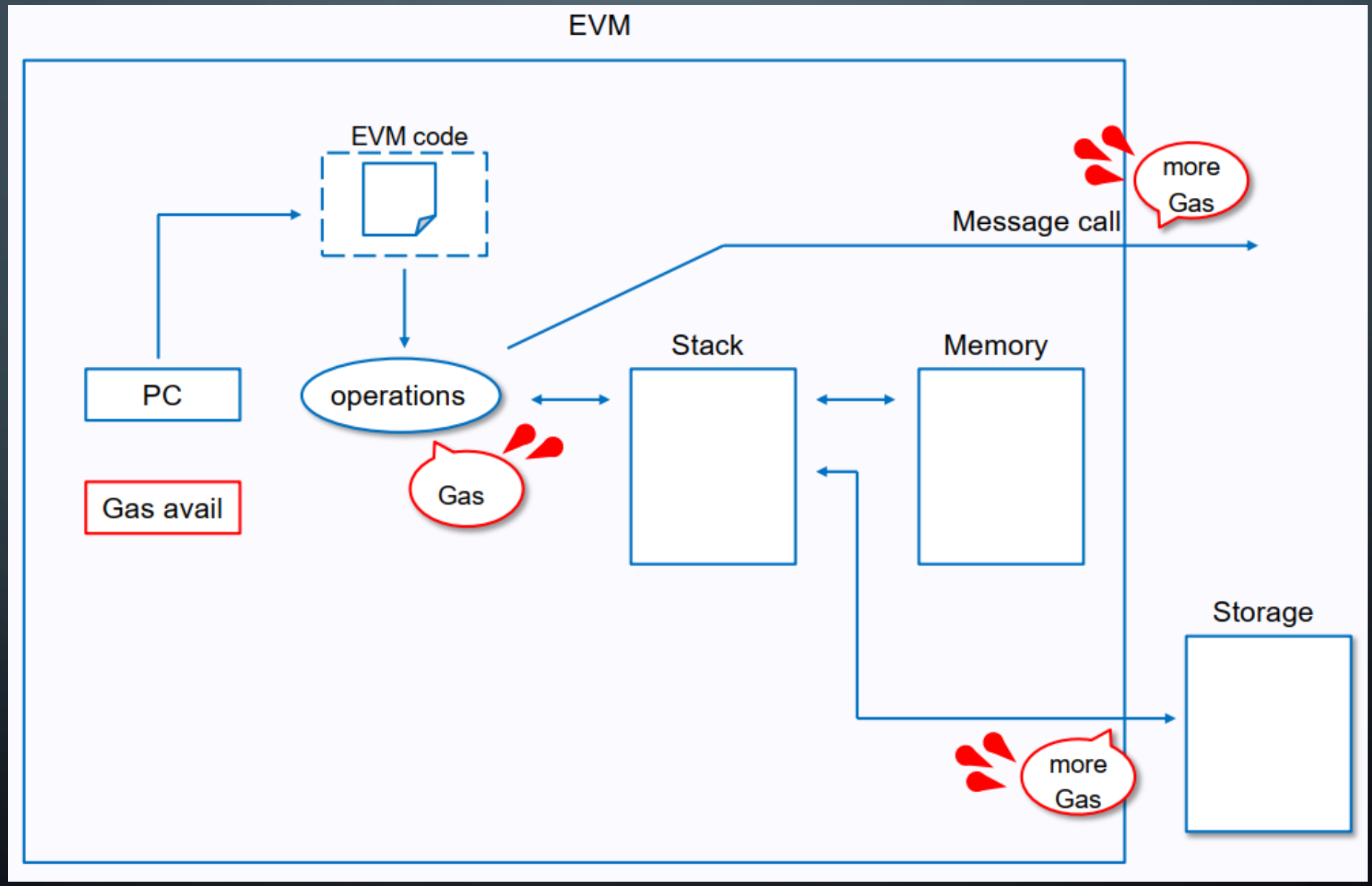


FEES AND GAS

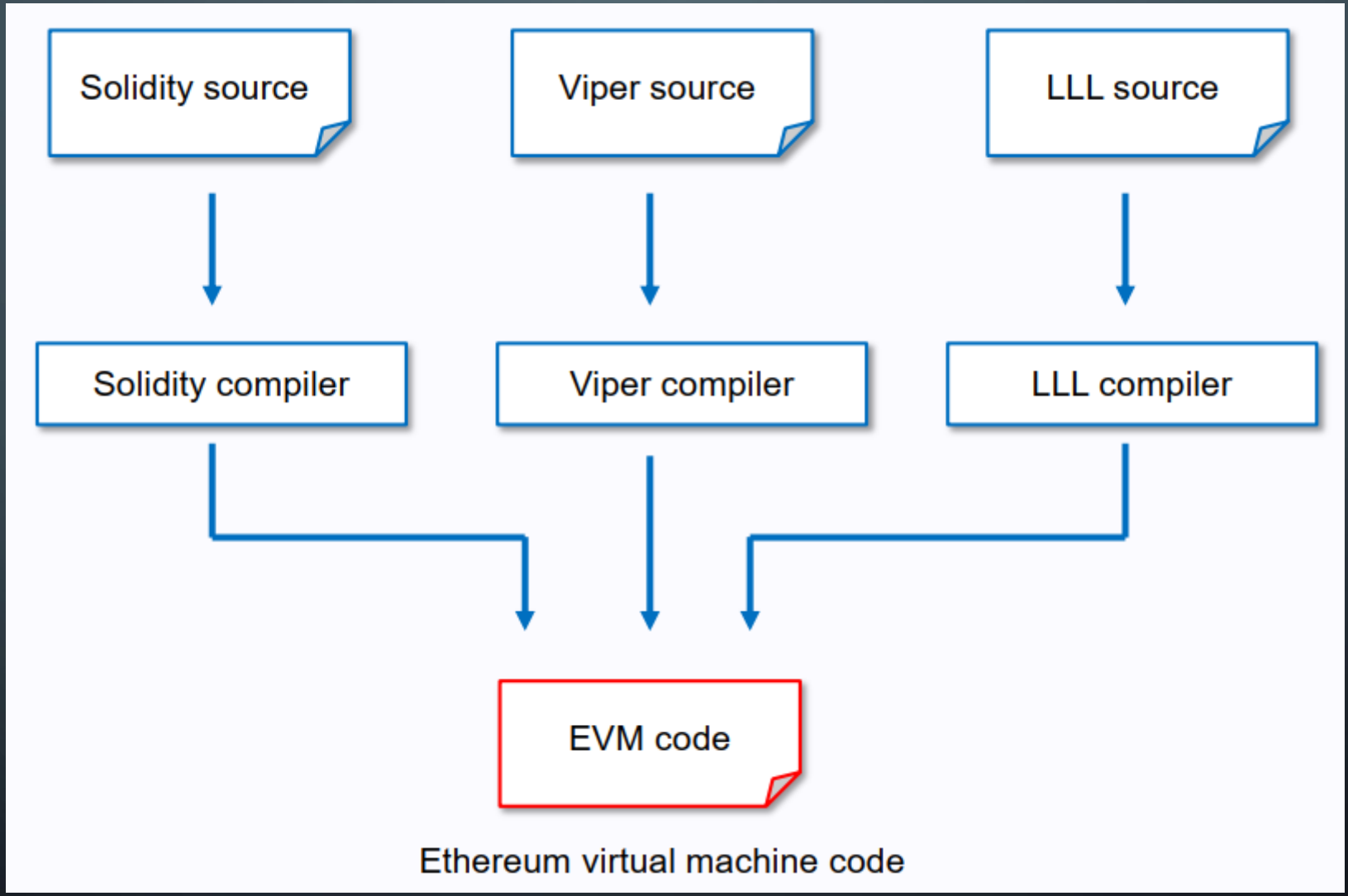


All programmable computation in Ethereum is subject to fees (denominated in gas).

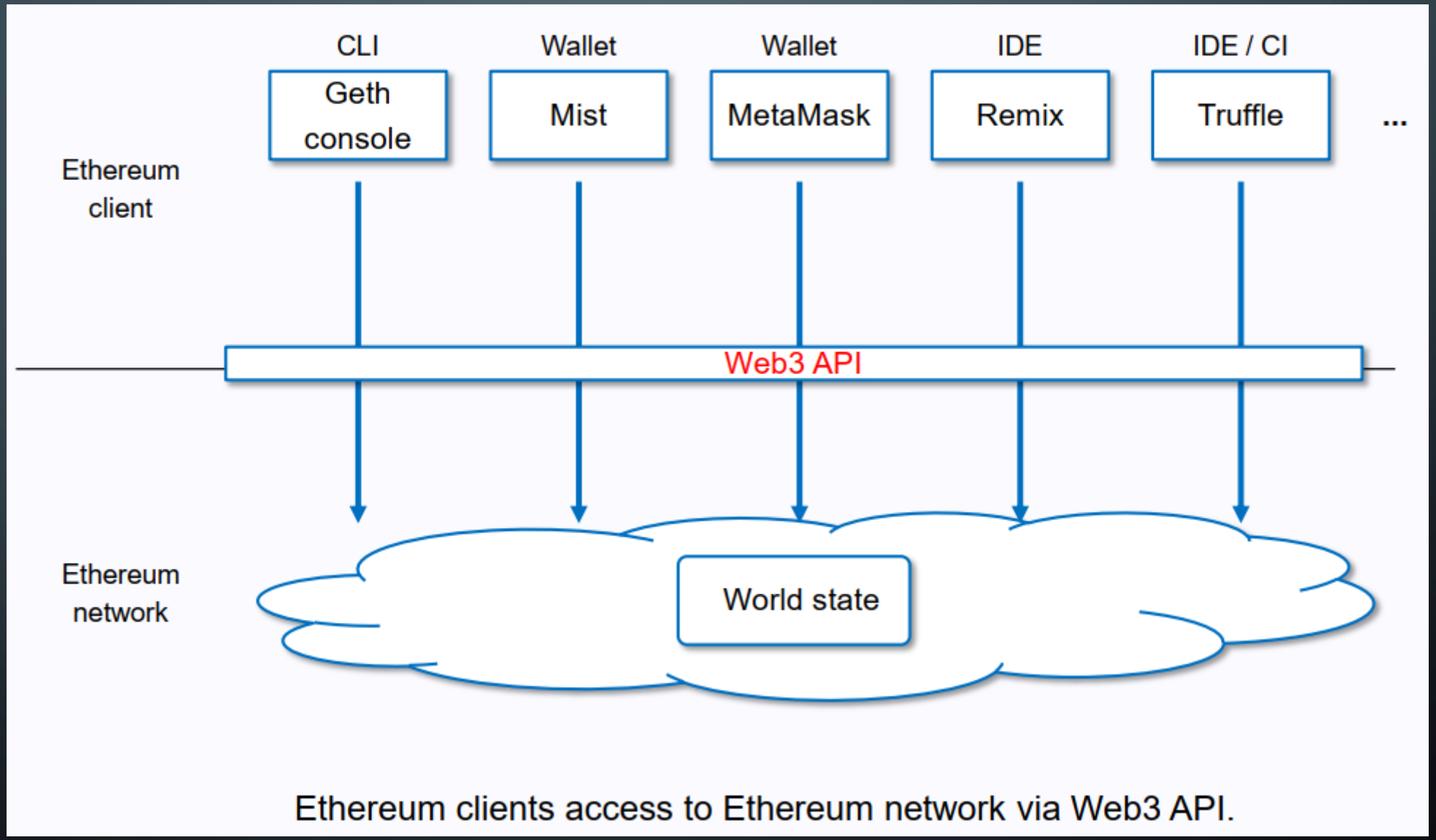
GAS CONSUMPTION



EVM CODE GENERATION

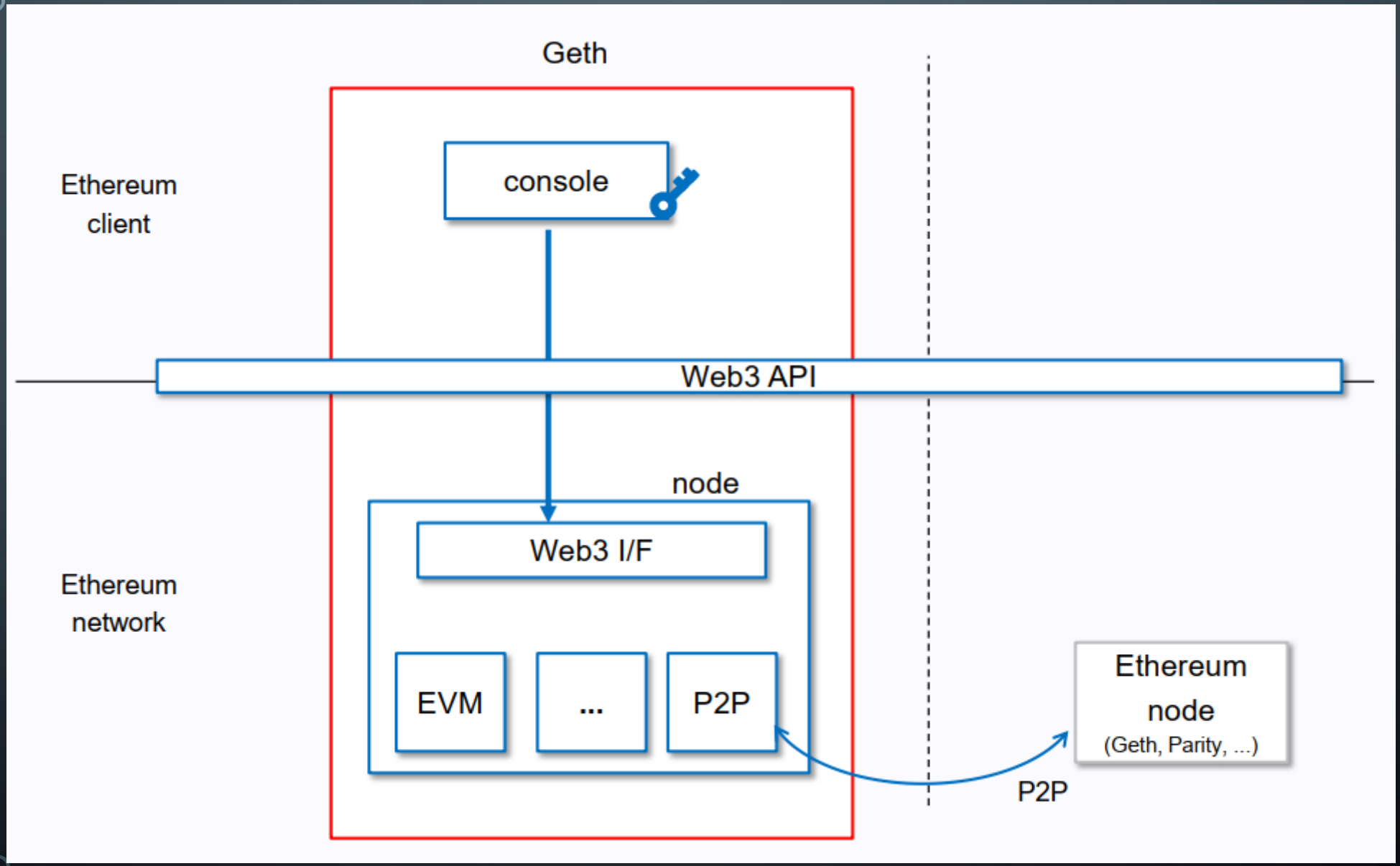


ETHEREUM CLIENT TOOLS

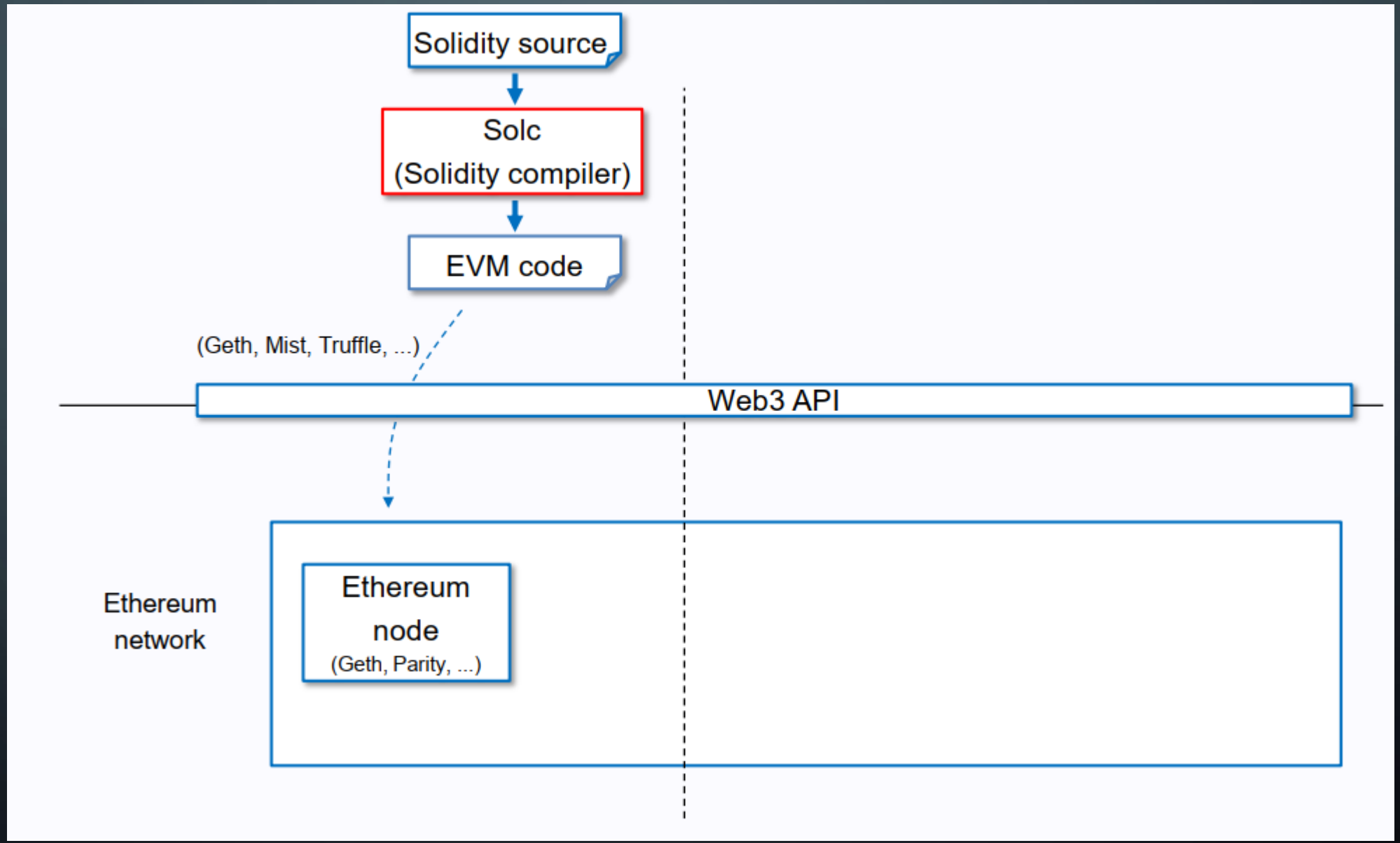


Ethereum clients access to Ethereum network via Web3 API.

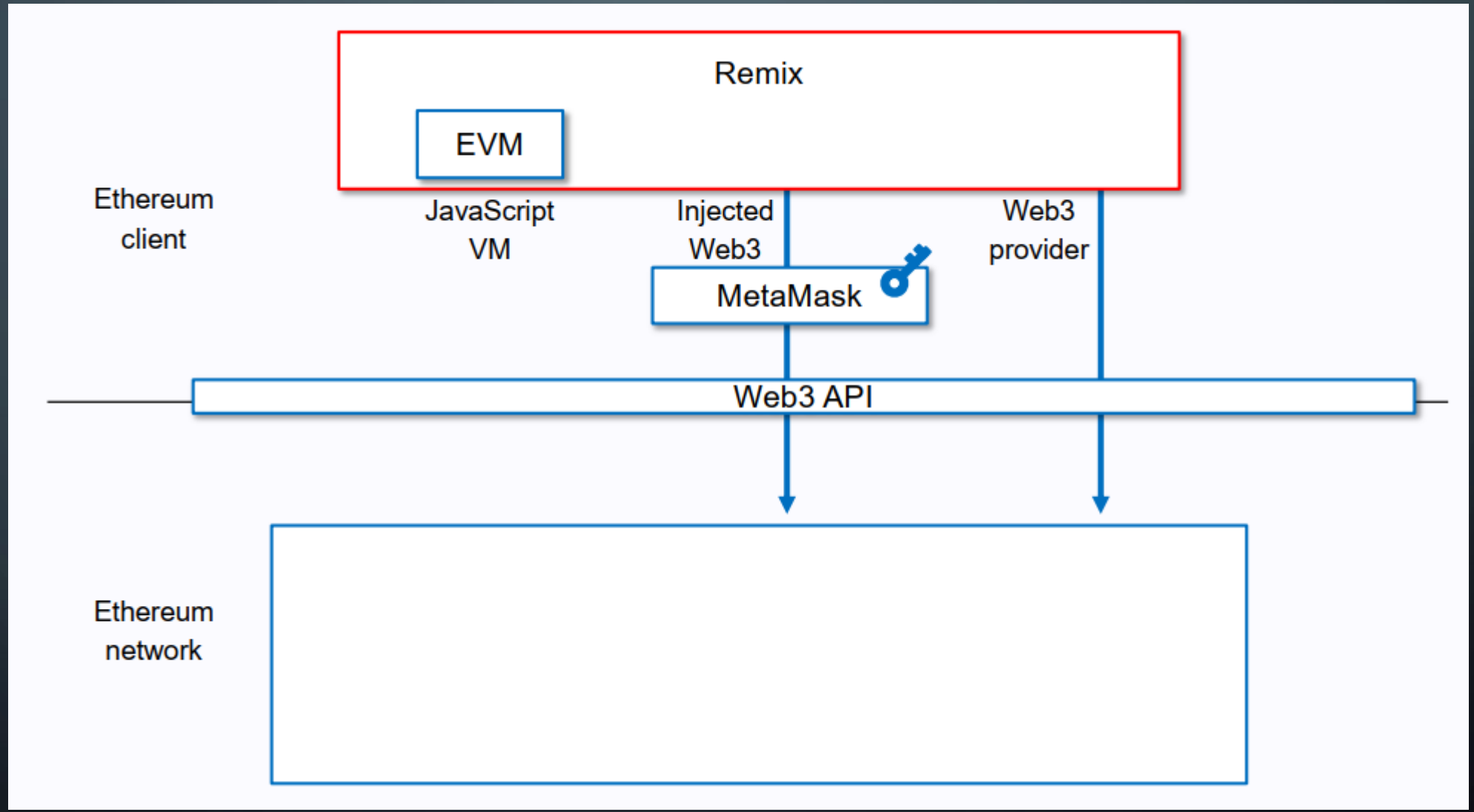
GETH ARCHITECTURE AND OPERATION



SOLIDITY COMPILER



REMIX IDE


Remix
EVM
Ethereum client
JavaScript VM
Injected Web3
Web3 provider
MetaMask
Web3 API
Ethereum network