BCDV 1010
Smart Contract Development Essentials

2023 January

week 03 - class 15

Lets refresh….

What is Ethereum?

Ethereum is a distributed network of computers (known as nodes) running software that can verify blocks and transaction data. The software application, known as a client, must be run on your computer to turn it into an Ethereum node.

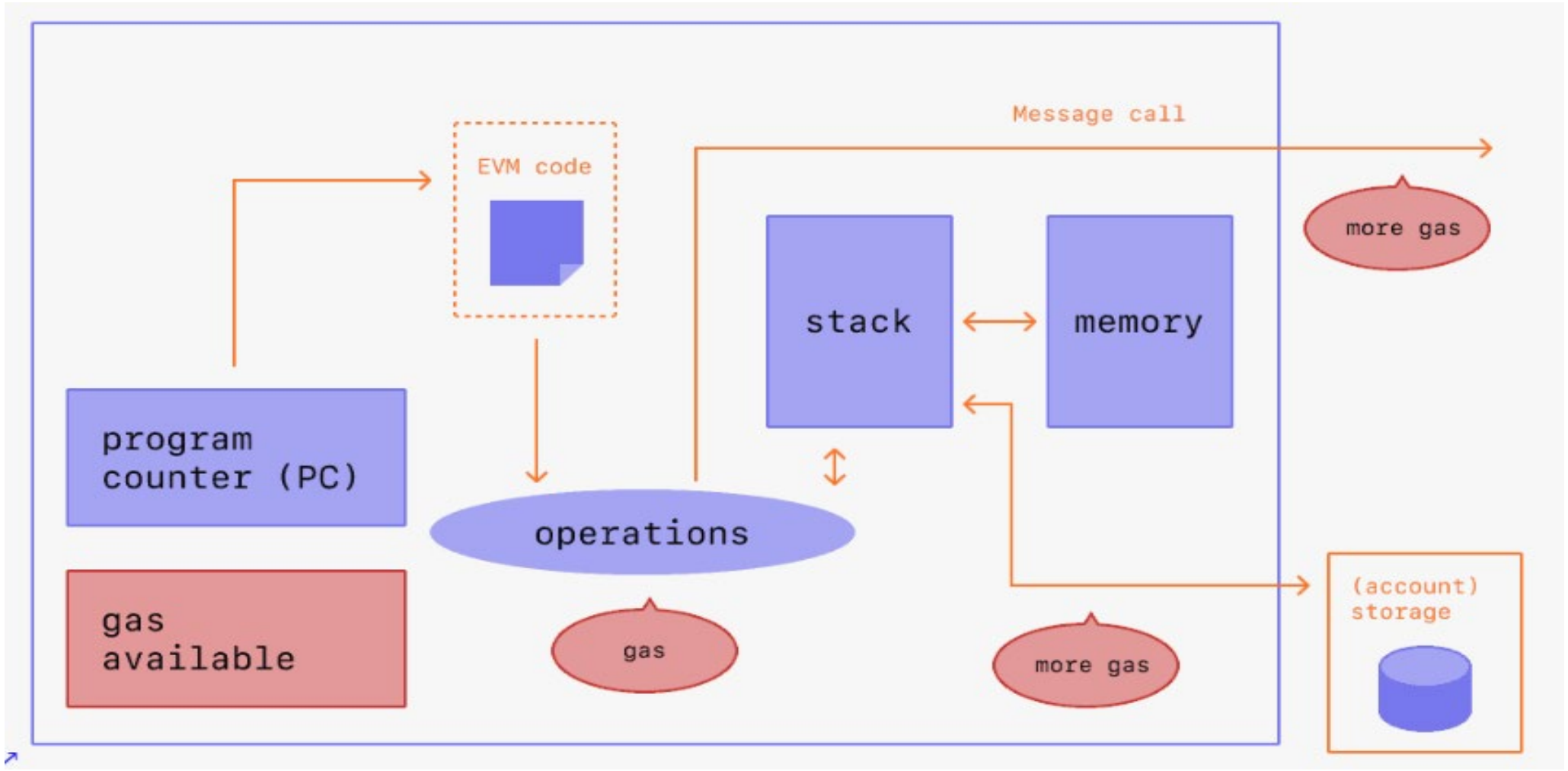
How Ethereum works?

Instead of a distributed ledger, Ethereum is a distributed state machine. Ethereum's state is a large data structure which holds not only all accounts and balances, but a *machine state*, which can change from block to block according to a pre-defined set of rules, and which can execute arbitrary machine code. The specific rules of changing state from block to block are defined by the EVM.

During execution, the EVM maintains a transient *memory* (as a word-addressed byte array), which does not persist between transactions.

Contracts, however, do contain a Merkle Patricia *storage* trie (as a word-addressable word array), associated with the account in question and part of the global state.

Compiled smart contract bytecode executes as a number of EVM opcodes, which perform standard stack operations like XOR, AND, ADD, SUB, etc. The EVM also implements a number of blockchain-specific stack operations, such as ADDRESS, BALANCE, BLOCKHASH, etc.


Message call
EVM code
more gas
stack
memory
program
counter (PC)
operations
(account)
storage
gas
available
gas
more gas

State

In the context of Ethereum, the state is an enormous data structure called a modified Merkle Patricia Trie, which keeps all accounts linked by hashes and reducible to a single root hash stored on the blockchain.

Transactions

Transactions are cryptographically signed instructions from accounts. There are two types of transactions: those which result in message calls and those which result in contract creation.

Contract creation results in the creation of a new contract account containing compiled smart contract bytecode. Whenever another account makes a message call to that contract, it executes its bytecode.