Ethereum Blockchain

Around 2013, a framework for code execution was introduced by Ethereum Founders. The centerpiece and thrust of this Ethereum blockchain is a smart contract.

Ethereum supports smart contracts and of virtual machine on which smart contracts execute. Smart contracts in turn enable decentralized application that accomplish more than a transfer of value.

What is a smart contract?

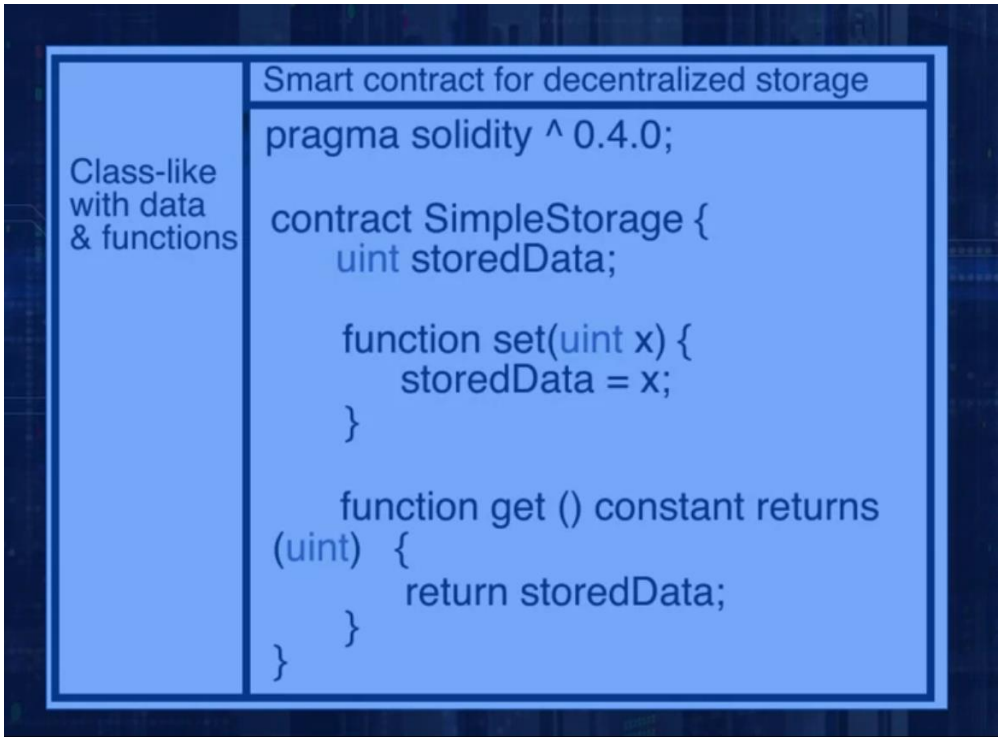
A smart contract is a piece of code deployed in the blockchain node. Execution of a smart contract is initiated by a message embedded in the transaction.

Specific programming languages have been designed for coding smart contracts. *Solidity* is one such language.

The code for the smart contracts is executed on a special structure known as *Ethereum Virtual Machine.*

Smart contract is designed, developed, compiled and deployed on the EVM that can be more than one smart contract in an EVM.

A simple Solidity smart contract to understand its structure: -



Ethereum Structure:

Accounts are basic unit of Ethereum Protocol.

Ethereum formally introduce the concept of an account as a part of the protocol.

The account is the originator and the target of a transaction.

A transaction directly updates the account balances as opposed to maintaining the state such as in the bitcoin UTXOs.

There are two types of accounts:

- Externally Owned Accounts
  Externally Owned Accounts or EOA are controlled by private keys.

- Contract Accounts.
  Contract Accounts or CA are controlled by the code and can be activated only by an EOA.

An externally owned account is needed to participate in the Ethereum network. It interacts with the blockchain using transactions.

A Contract Account represents a smart contract.

The participant node can send transaction for Ether transfer or it can send transaction to invoke a smart contract code or both. Both types of transaction require fees.

Fees are paid in Wei. Wei is a lower denomination of Ether.

A transaction in Ethereum includes:

- Recipient
- Signature of Sender authorizing transfer
- Amount of Wei
- Message to a contract
- STARTGAS (a value representing the maximum number of computational steps the transaction is allowed.)
- GASPRICE (Fee for Computations)

Ethereum Operations:

An Ethereum node is a computational system representing a business entity or an individual participant.

An Ethereum full node hosts the software needed for transaction initiation, validation, mining, block creation, smart contract execution and the Ethereum Virtual Machine, EVM.

When the target address in a transaction is a smart contract, the execution code corresponding to the smart contract is activated and executed on the EVM. The input needed for this execution is extracted from the payload field of the transaction. Current state of the smart contract is the values of the variables defined in it. The state of the smart contract may be updated by this execution. Results of this execution is told in the *receipts*.

A blockchain maintains both the state hash and the receipt hash.

Transaction validation involves checking the time-stamp and the nonce combination to be valid and the availability of sufficient fees for execution.

Miner nodes in the network receive, verify, gather and execute transactions. The in-work smart contract code are executed by all miners. Validated transactions are broadcast and gathered for block creation.

Incentive Model:

Every action in Ethereum requires crypto fuel, or gas. Gas points are used to specify the fees inside of Ether, for ease of computation using standard values.

Gas points allow for cryptocurrency independent valuation of the transaction fee and computation fees.

Ether, as a cryptocurrency, varies in value with market swings, but gas points do not vary.

Ethereum has specified gas points for each type of operation. Mining process computes gas points required for execution of a transaction.

If the fee specified and the gas point in the transaction are not sufficient, it is rejected. This is similar to mailing a letter with insufficient postage. The letter will not be delivered if it had insufficient postage.