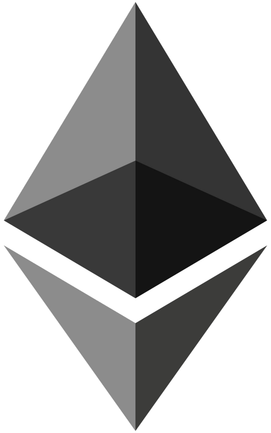
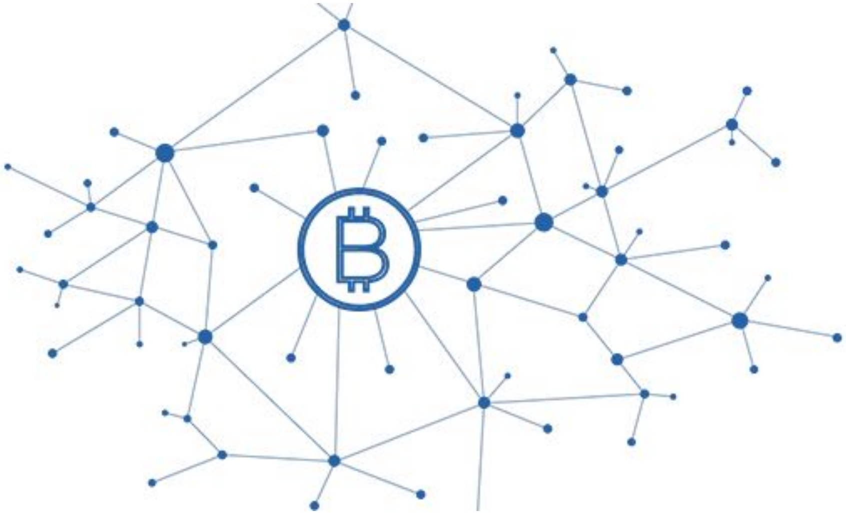


Ethereum

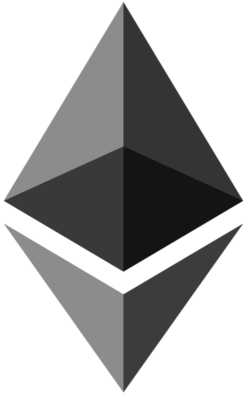
Beyond Bitcoin

Bitcoin - The decentralized financial platform

Bitcoin’s **Backbone** - **Blockchain** Technology

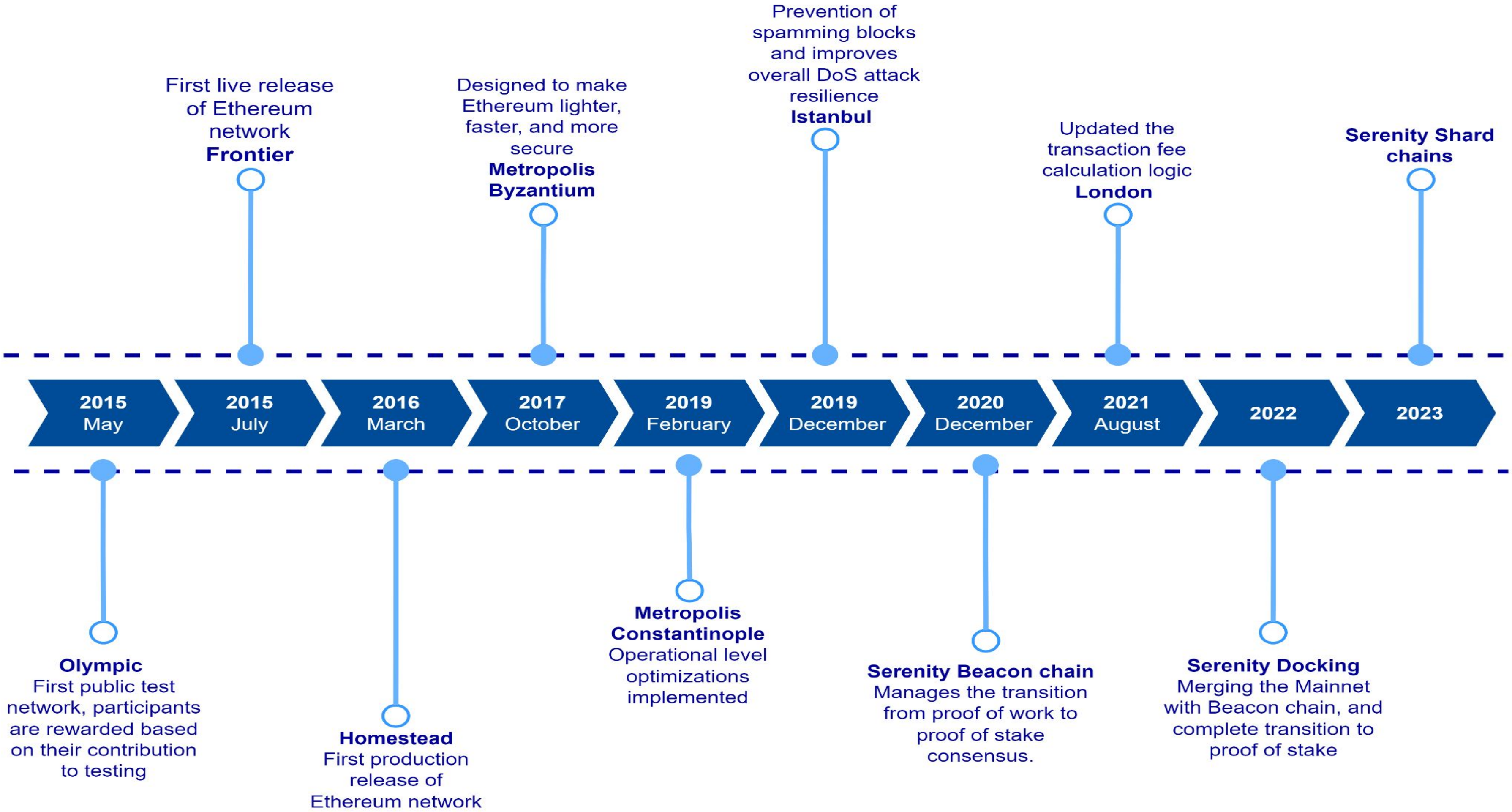


What is Ethereum Blockchain?



Ethereum was first of it kind, general purpose programmable blockchain technology

Evolution of Ethereum



2015 May
Olympic
First public test network, participants are rewarded based on their contribution to testing

2015 July
First live release of Ethereum network
Frontier

2016 March
Homestead
First production release of Ethereum network

2017 October
Designed to make Ethereum lighter, faster, and more secure
Metropolis Byzantium

2019 February
Metropolis Constantinople
Operational level optimizations implemented

2019 December
Prevention of spamming blocks and improves overall DoS attack resilience
Istanbul

2020 December
Serenity Beacon chain
Manages the transition from proof of work to proof of stake consensus.

2021 August
Updated the transaction fee calculation logic
London

2022
Serenity Docking
Merging the Mainnet with Beacon chain, and complete transition to proof of stake

2023
Serenity Shard chains

Ethereum World Computer

Ethereum Vision: One Computer (blockchain) for the entire world

Ethereum blockchain is a horizontal technology comprised of 4 basic components

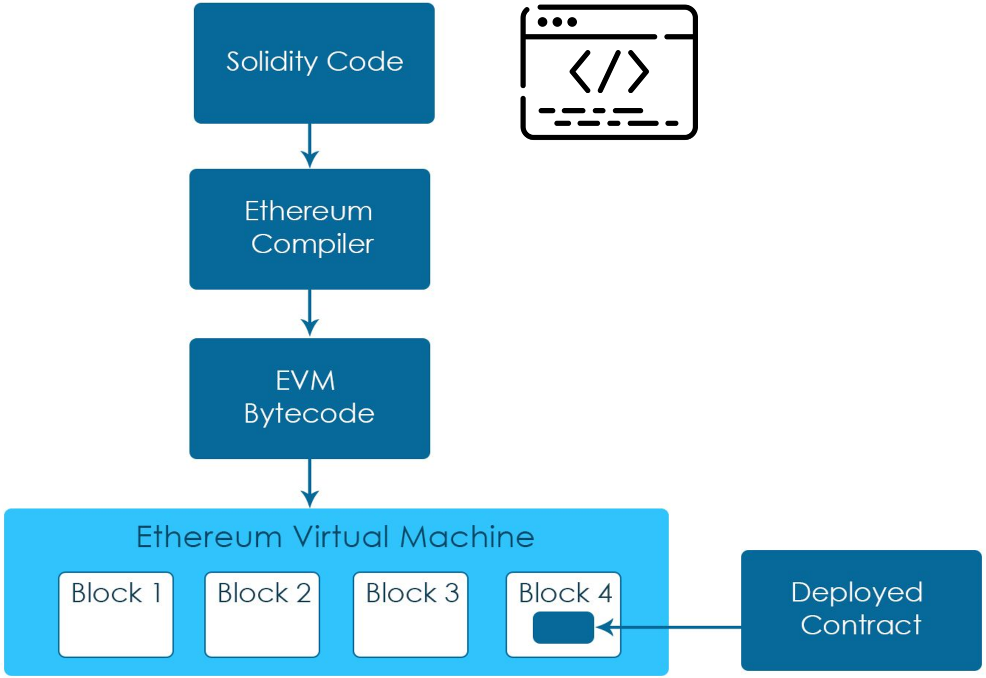
Digital Ledger: A continually updated, network hosted database of all transactions

Consensus Mechanism : Responsible for verifying and Updating transactions

Digital Asset: The good transacted on a Blockchain

Network Participants: Able to manipulate the Ledger and view past transactions

About Ethereum Virtual Machine


Solidity Code

Ethereum Compiler

EVM Bytecode

Ethereum Virtual Machine

Block 1

Block 2

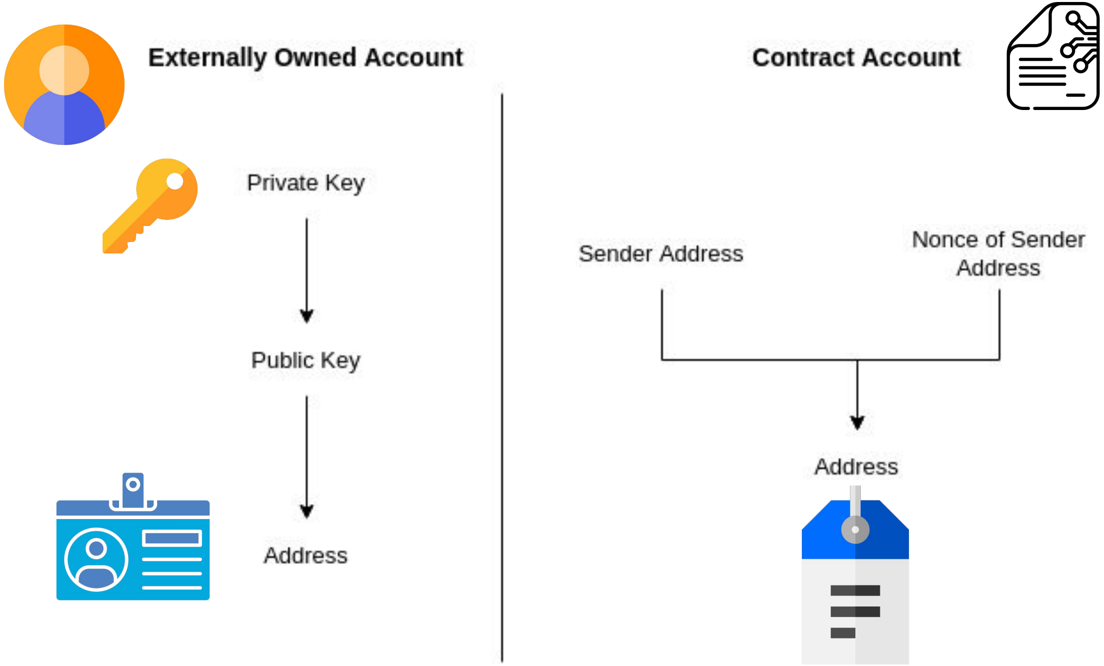
Block 3

Block 4

Deployed Contract

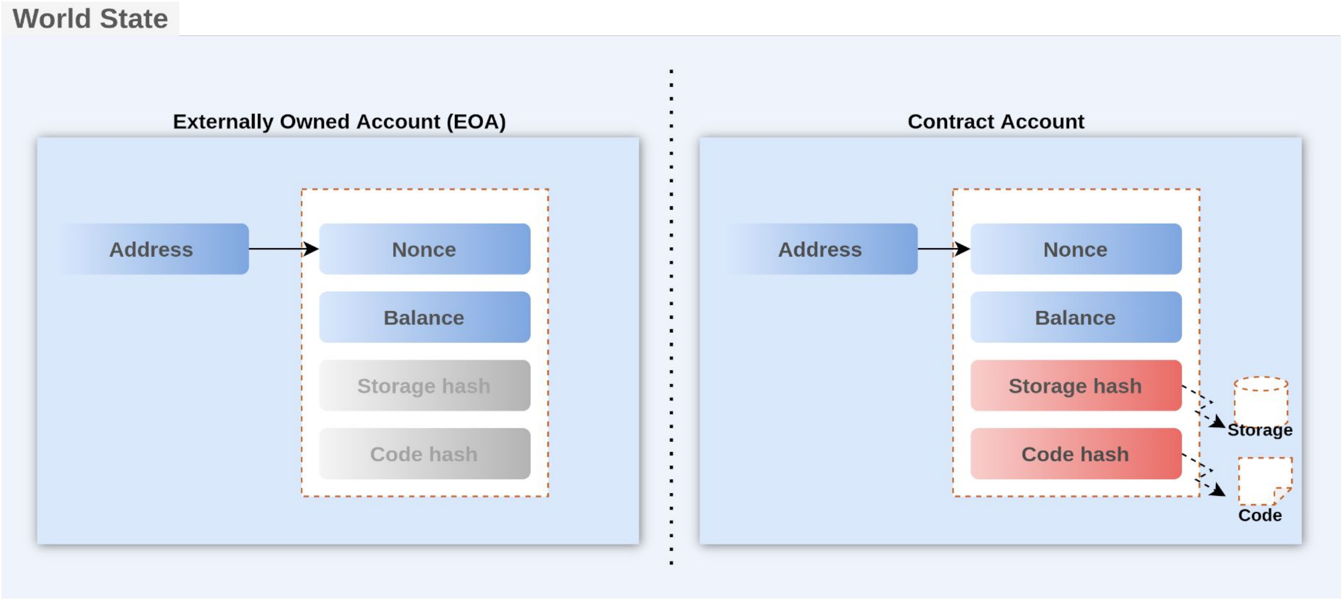
Accounts

An Identity in the pseudo anonymous Ethereum network.



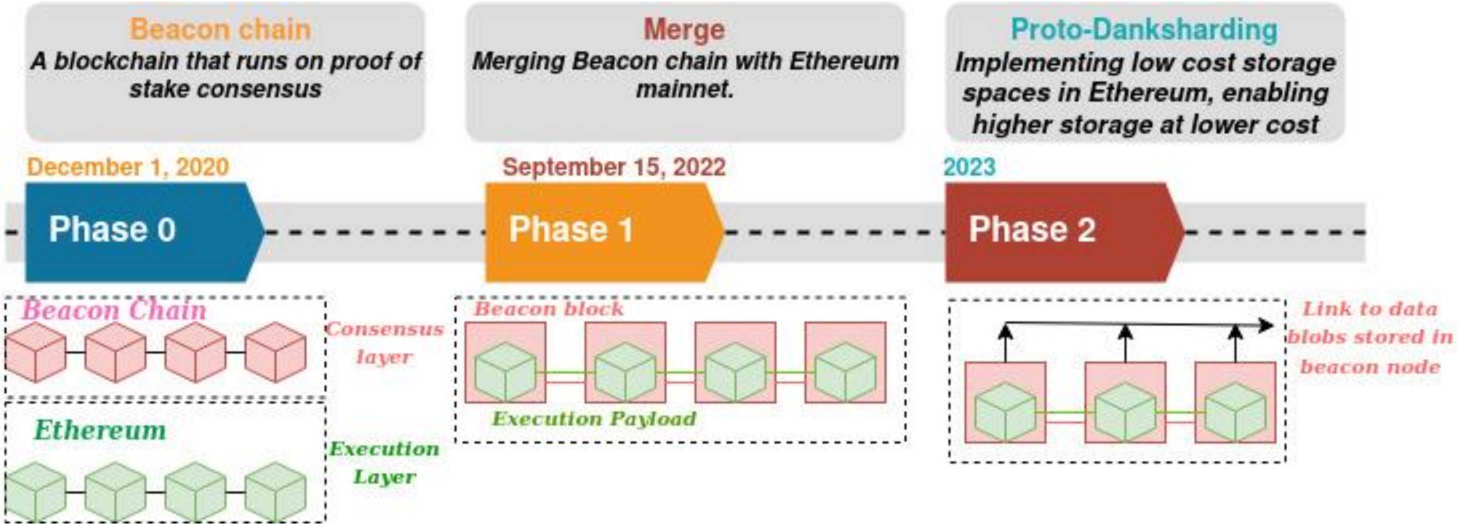
Accounts

Externally Owned Account (EOA) and Contract Account



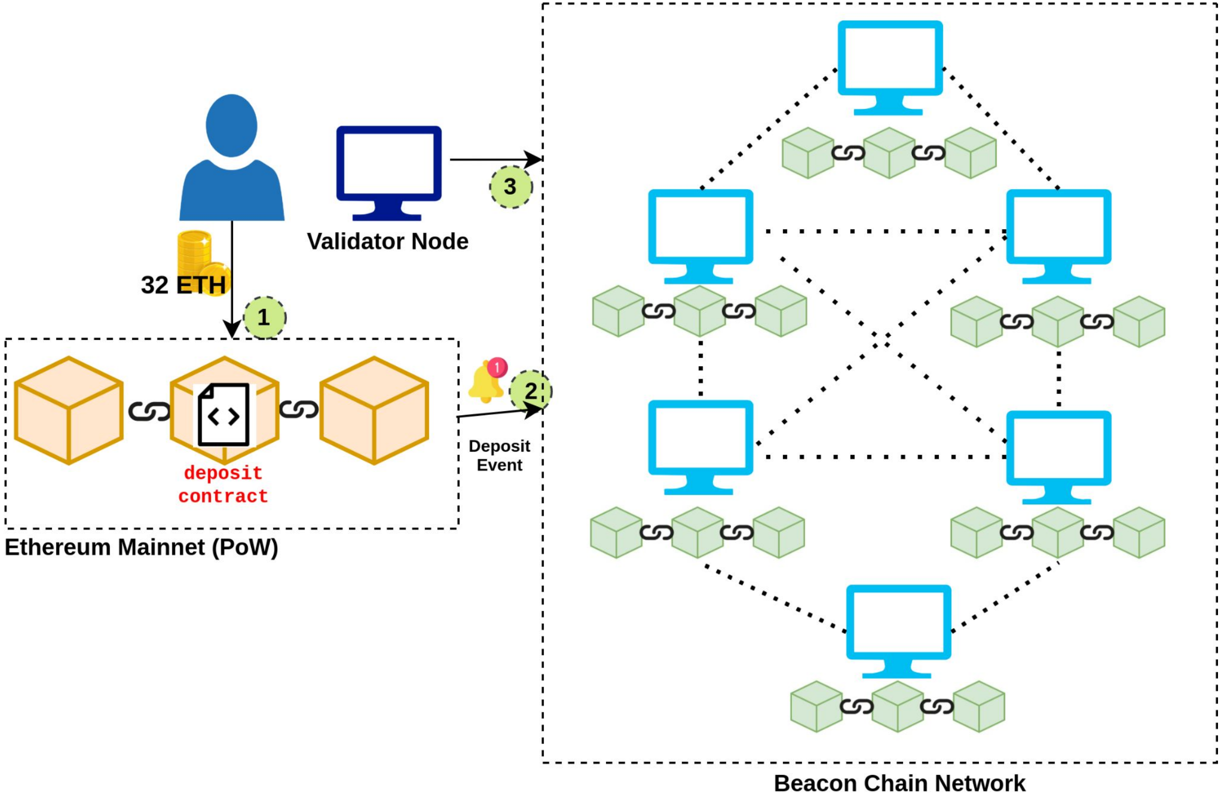
The Ethereum Upgrades

Ethereum Upgrade Roadmap

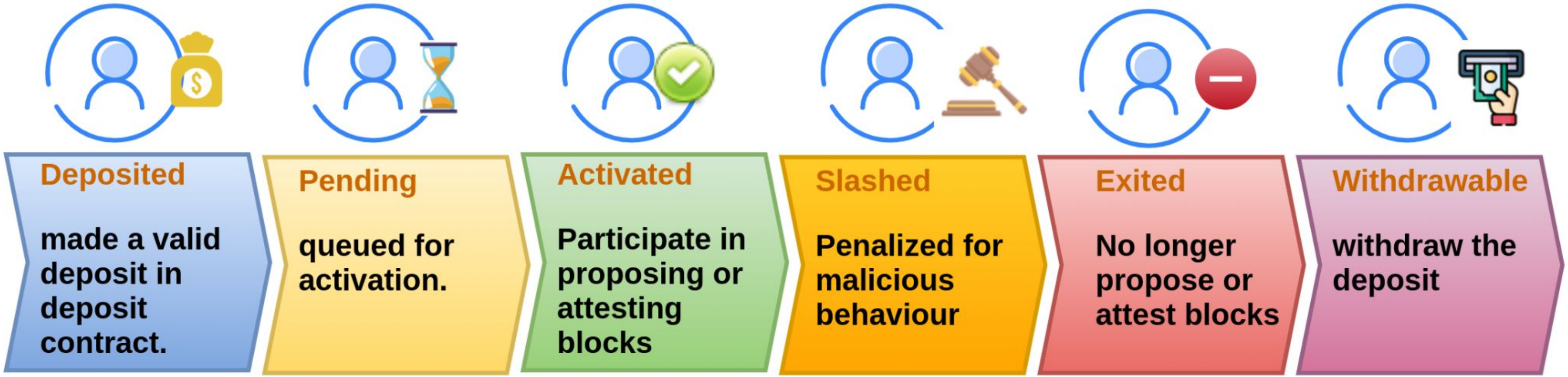


Beacon chain
A blockchain that runs on proof of stake consensus
Merge
Merging Beacon chain with Ethereum mainnet.
Proto-Danksharding
Implementing low cost storage spaces in Ethereum, enabling higher storage at lower cost
December 1, 2020
September 15, 2022
2023
Phase 0
Phase 1
Phase 2
Beacon Chain
Consensus layer
Ethereum
Execution Layer
Beacon block
Execution Payload
Link to data blobs stored in beacon node

Phase 0: The Beacon Chain



Validator Lifecycle



Deposited

made a valid deposit in deposit contract.

Pending

queued for activation.

Activated

Participate in proposing or attesting blocks

Slashed

Penalized for malicious behaviour

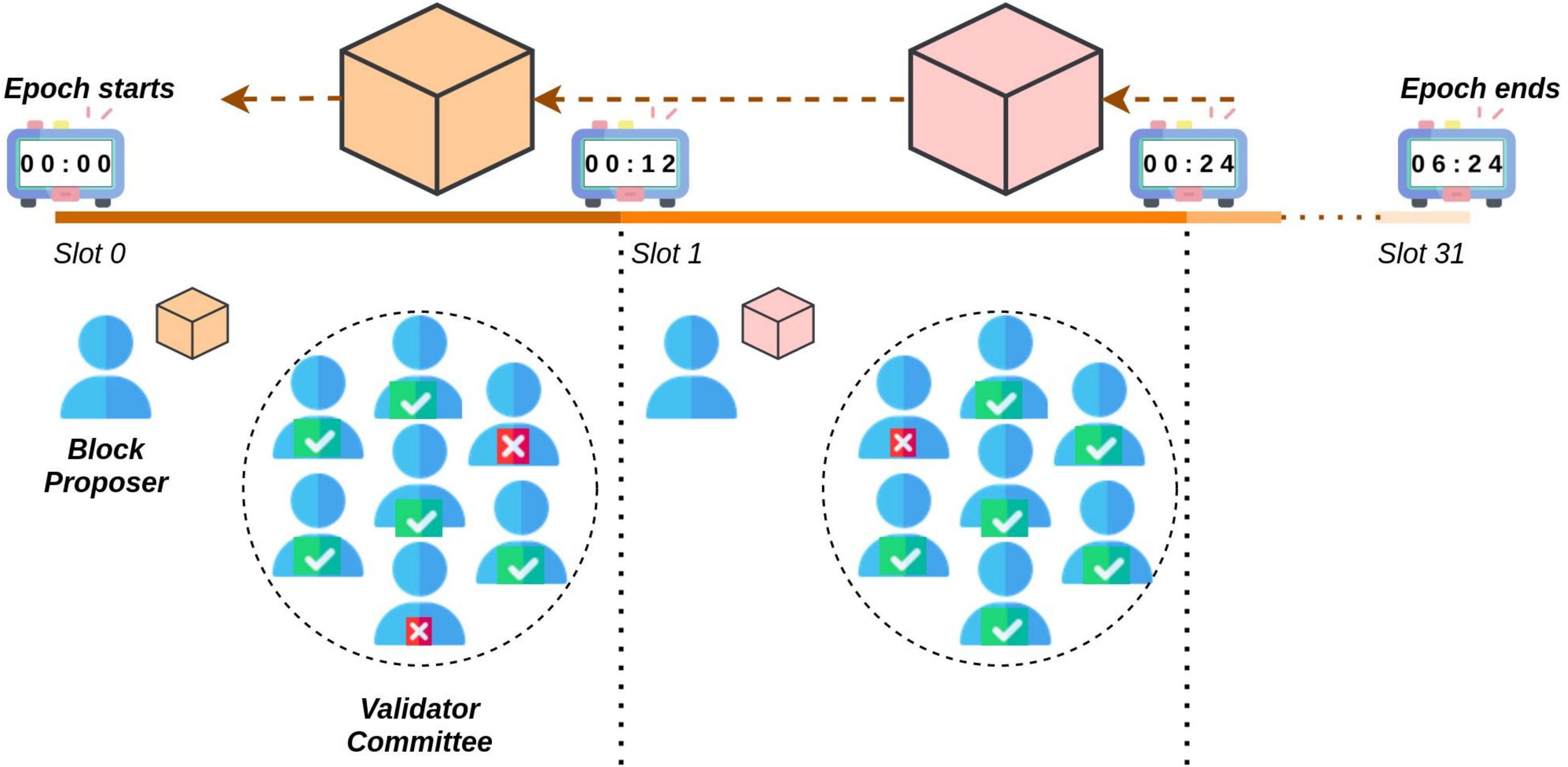
Exited

No longer propose or attest blocks

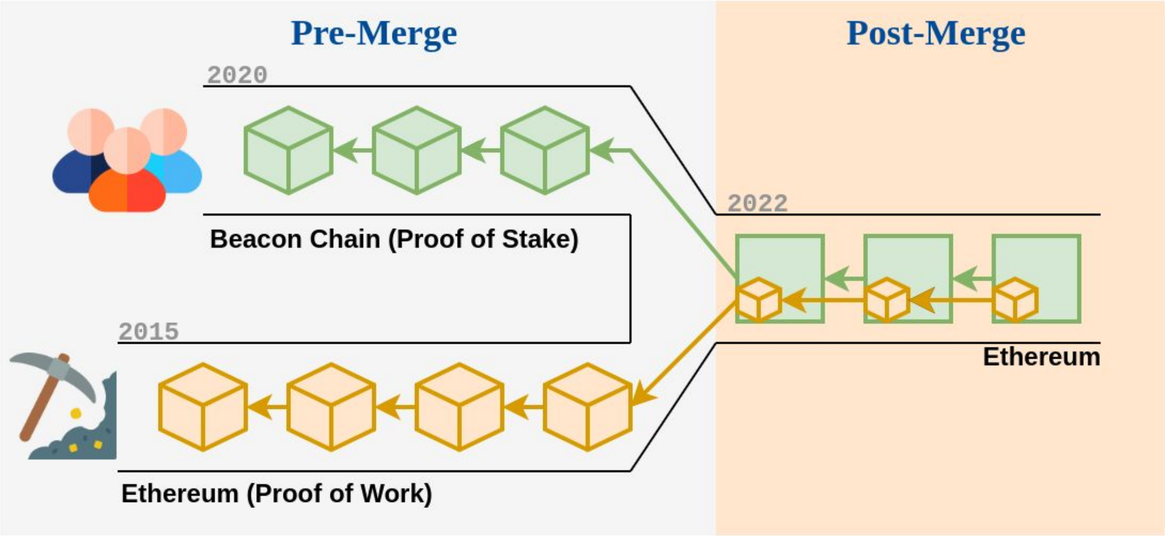
Withdrawable

withdraw the deposit

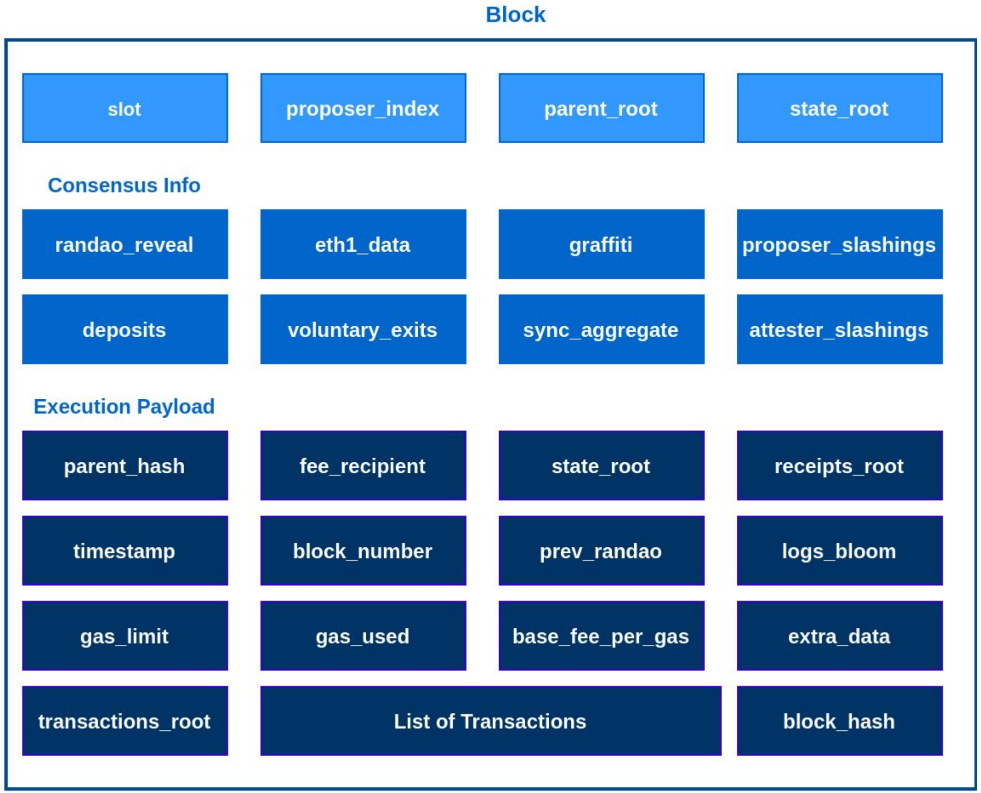
Proof-of-Stake



Structure of a Block



Ethereum Block Components



Block

slot | proposer_index | parent_root | state_root

Consensus Info

randao_reveal | eth1_data | graffiti | proposer_slashings

deposits | voluntary_exits | sync_aggregate | attester_slashings

Execution Payload

parent_hash | fee_recipient | state_root | receipts_root

timestamp | block_number | prev_randao | logs_bloom

gas_limit | gas_used | base_fee_per_gas | extra_data

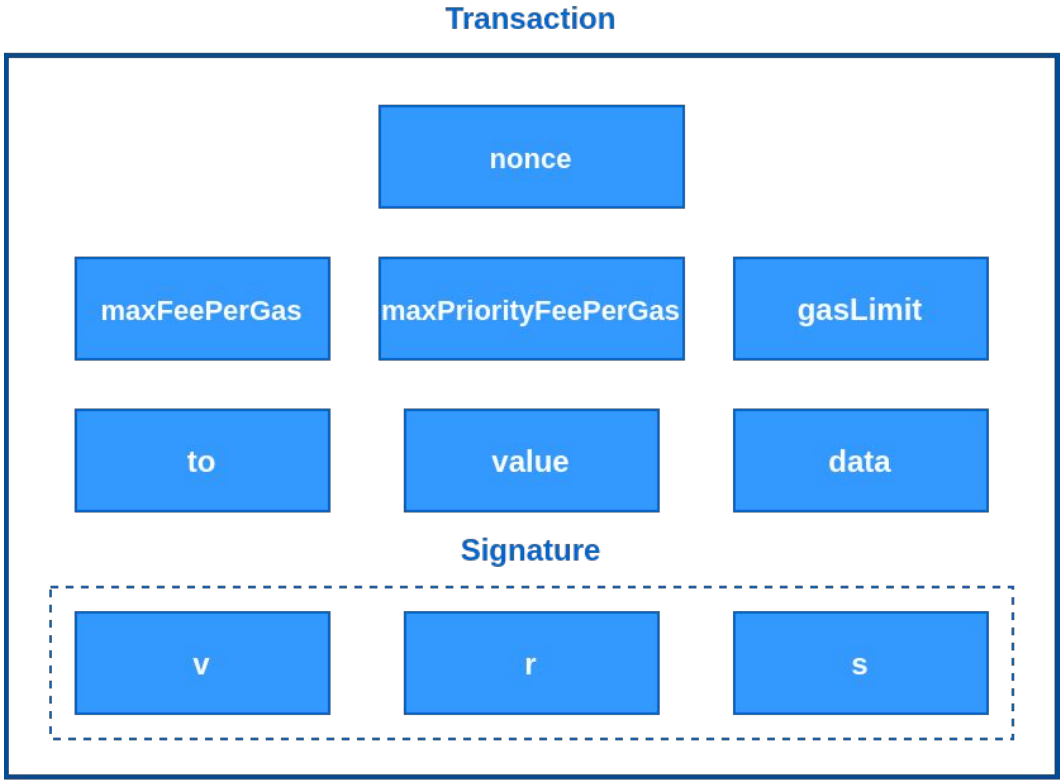
transactions_root | List of Transactions | block_hash

Ethereum Transaction

- Every transaction in an Ethereum Blockchain consists of following fields :
  - The recipient of the transaction (either user or smart contract).
  - Signature of the sender for identifying and validating the message being sent.
  - VALUE field that specifies the amount of wei to be transferred from the sender to the receiver.
  - NONCE- a sequentially incrementing counter which indicate the transaction number from the account
  - DATA field (Optional) that holds the message being sent to a contract.
  - TRANSACTION GAS LIMIT – maximum number of gas sender willing to spend on a particular transaction.
  - maxPriorityFeePerGas - the maximum amount of gas to be included as a tip to the validator
  - maxFeePerGas - the maximum amount of gas willing to be paid for the transaction (inclusive of baseFeePerGas and maxPriorityFeePerGas)

One unit of gas corresponds to the execution of one atomic instruction, i.e., a computational step

Transaction Structure



Transaction

nonce

maxFeePerGas

maxPriorityFeePerGas

gasLimit

to

value

data

Signature

v

r

s

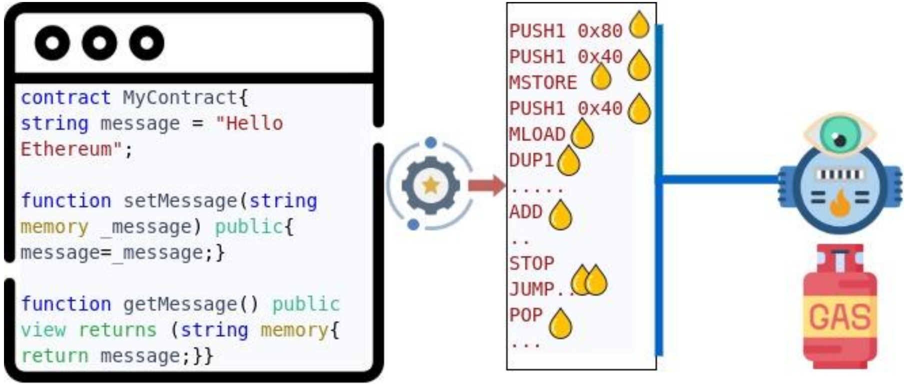
Transaction Cost: Ether

Ether is the name of the native crypto-currency of the Ethereum network.

Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

Gas

- Every operation (write or read) done to the blockchain network is known as a transaction, and each transaction has a fee. Which is paid in ether and is known as Gas Cost.
- Gas refers to a unit that estimates the amount of computational work required for executing specific operations under the Ethereum virtual machine.



```
contract MyContract{
string message = "Hello
Ethereum";

function setMessage(string
memory _message) public{
message=_message;}

function getMessage() public
view returns (string memory{
return message;}}
```

```
PUSH1 0x80
PUSH1 0x40
MSTORE
PUSH1 0x40
MLOAD
DUP1
.....
ADD
..
STOP
JUMP..
POP
...
```

o

Transaction Fee

Gas Limit refers to the maximum measure of gas you are happy to spend on a specific transaction.

Transaction Fee = Gas Limit *(Base fee + Tip)

GAS
Base Fee
Priority Fee

ERC 1559 or the ‘London’ Fork

This comes with some new terms:

Base Fee (Burnt):

- Set by Ethereum based on network traffic (tx), the minimum fee to get included in a block.

Priority Fee (Tip):

- Set by user, given to validators. (Default 2 Gwei), higher tip faster processing.

Max Fee

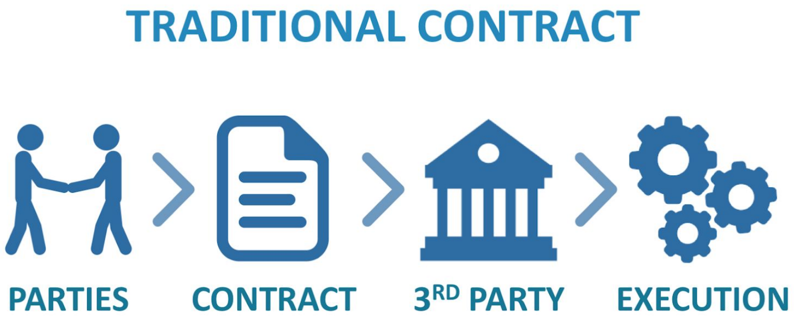
- Maximum fee the user willing to pay, so Max Fee - (Base Fee + Priority Fee) = Refunded to user

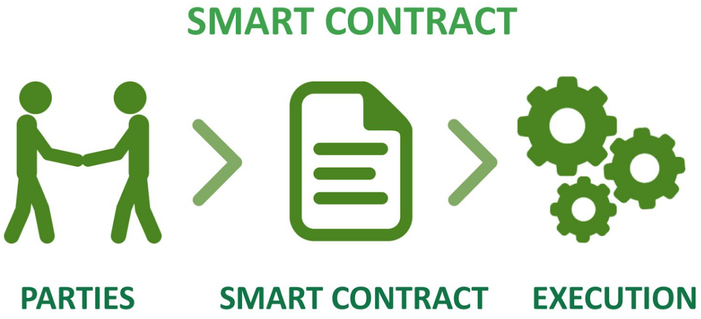
Ref: https://thedailygwei.substack.com/p/this-is-eip-1559-the-daily-gwei-300

Smart Contracts

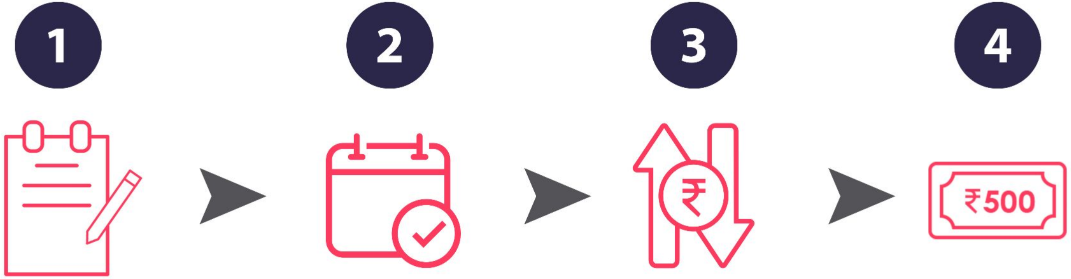
“A set of promises, specified in digital form, including protocols within which the parties perform on these promises”

-Nick Szabo





How do smart contracts work:



1 Pre-programmed Contracts

A line of code is established by all counterparties defining the rules, terms and conditions of the agreement.

2 Chain of Events

If the events specified by pre-defined conditions takes place, the code automatically gets executed.

3 Value Transfer

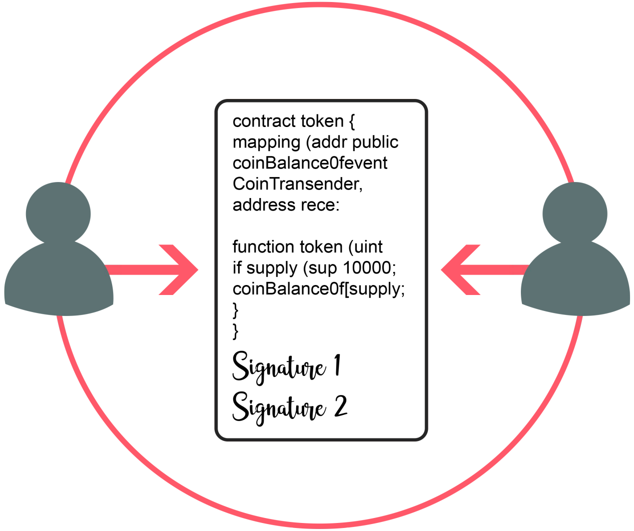
Once the code gets executed, the terms of contract makes sure that the transfer is made to the relevant parties.

4 Settlement

Once the transfer of value to the counterparties takes place, the transaction gets recorded on the blockchain.

Benefits

- Self-executing.
- Tamper-resistant.
- Reduces malicious or accidental events.
- Deterministic
- Provides transparency
- Reduced intermediaries
- Better trust among anonymous entities



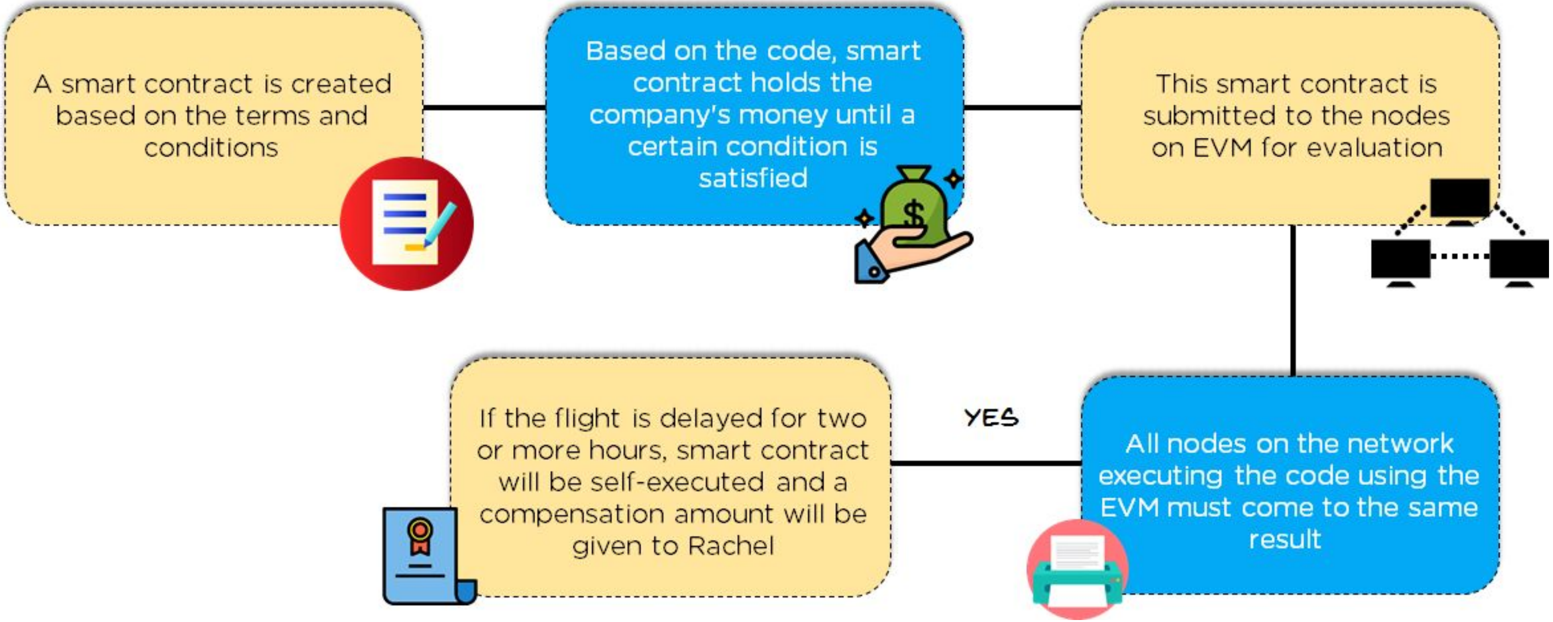
```
contract token {
mapping (addr public
coinBalance0fevent
CoinTransender,
address rece:

function token (uint
if supply (sup 10000;
coinBalance0f[supply;
}
}
```

Signature 1
Signature 2

A use case

Flight Delay Insurance



A smart contract is created based on the terms and conditions

Based on the code, smart contract holds the company's money until a certain condition is satisfied

This smart contract is submitted to the nodes on EVM for evaluation

All nodes on the network executing the code using the EVM must come to the same result

YES

If the flight is delayed for two or more hours, smart contract will be self-executed and a compensation amount will be given to Rachel

Source:https://www.youtube.com/watch?v=_J6G5g-nKgo

SOLIDITY

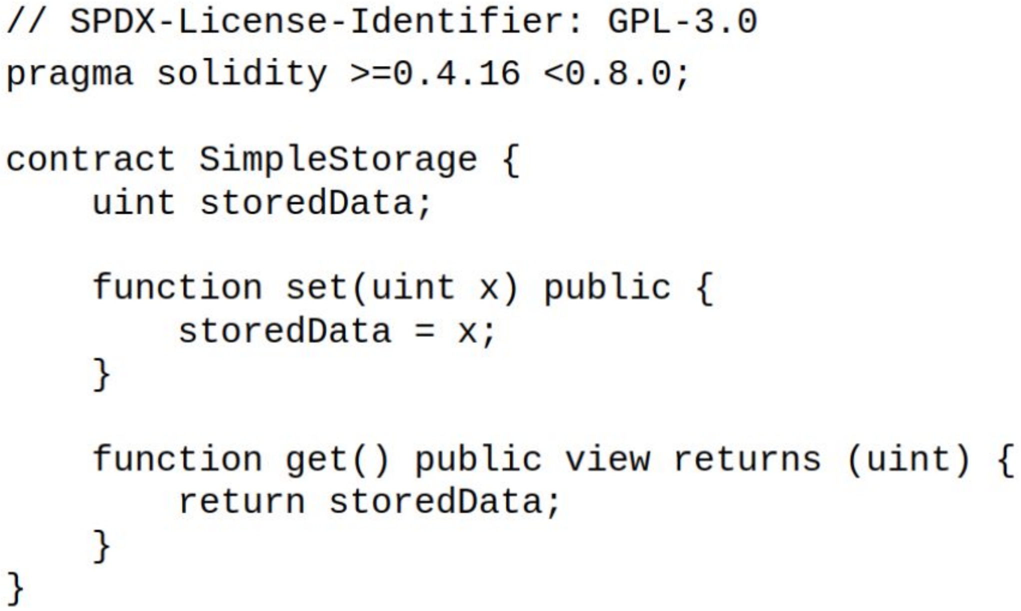
Created By : Gavin Wood

Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state.

Solidity Features

- Influenced by C++, Python and JavaScript.
- Designed to target the Ethereum Virtual Machine (EVM).
- Solidity is statically typed.
- Supports:

    1. Inheritance
    2. Libraries
    3. Complex User Defined Types



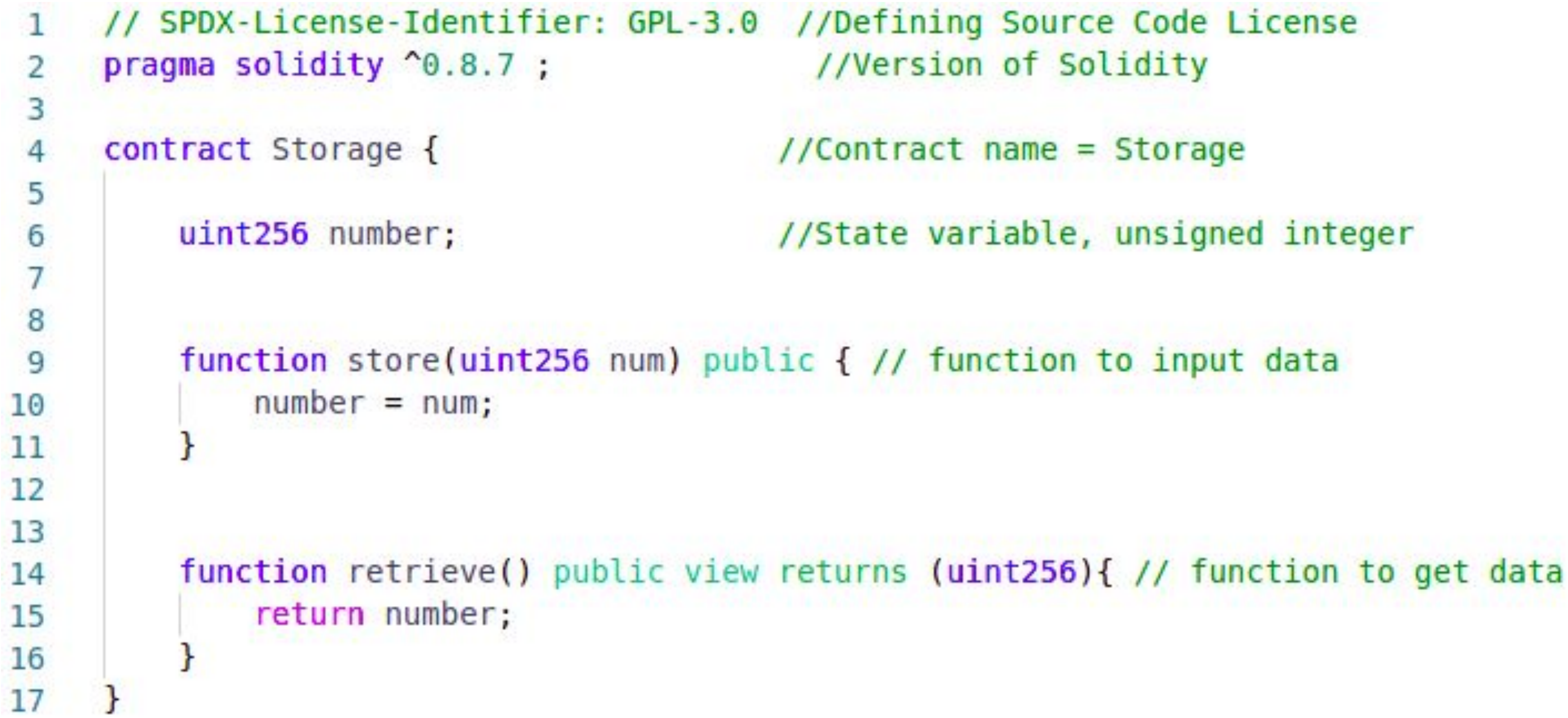
```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.4.16 <0.8.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Smart Contract



```solidity
// SPDX-License-Identifier: GPL-3.0  //Defining Source Code License
pragma solidity ^0.8.7 ;              //Version of Solidity

contract Storage {                  //Contract name = Storage

    uint256 number;                 //State variable, unsigned integer


    function store(uint256 num) public { // function to input data
        number = num;
    }


    function retrieve() public view returns (uint256){ // function to get data
        return number;
    }
}
```

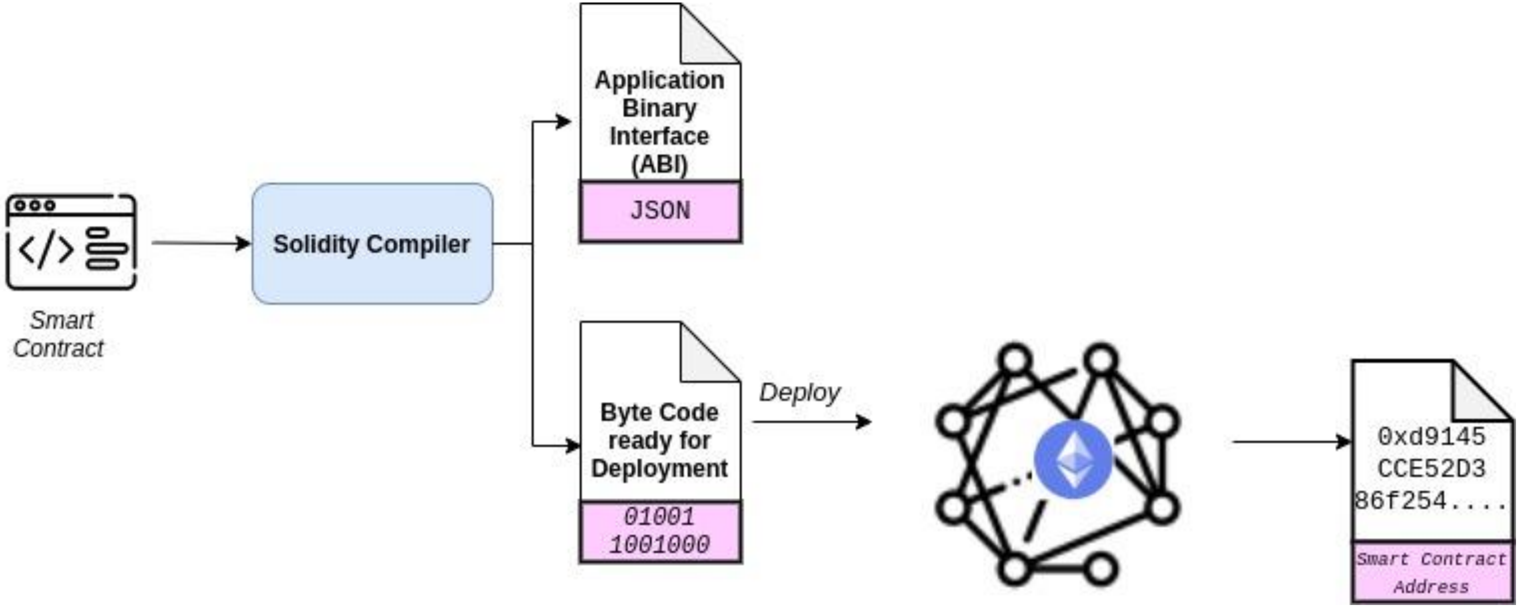
Ethereum Wallets

- Software application that helps you manage your Ethereum account.
- It holds your keys and can create and broadcast transactions on your behalf.
- **MetaMask** is a browser extension wallet that runs in your browser.
- https://metamask.io/

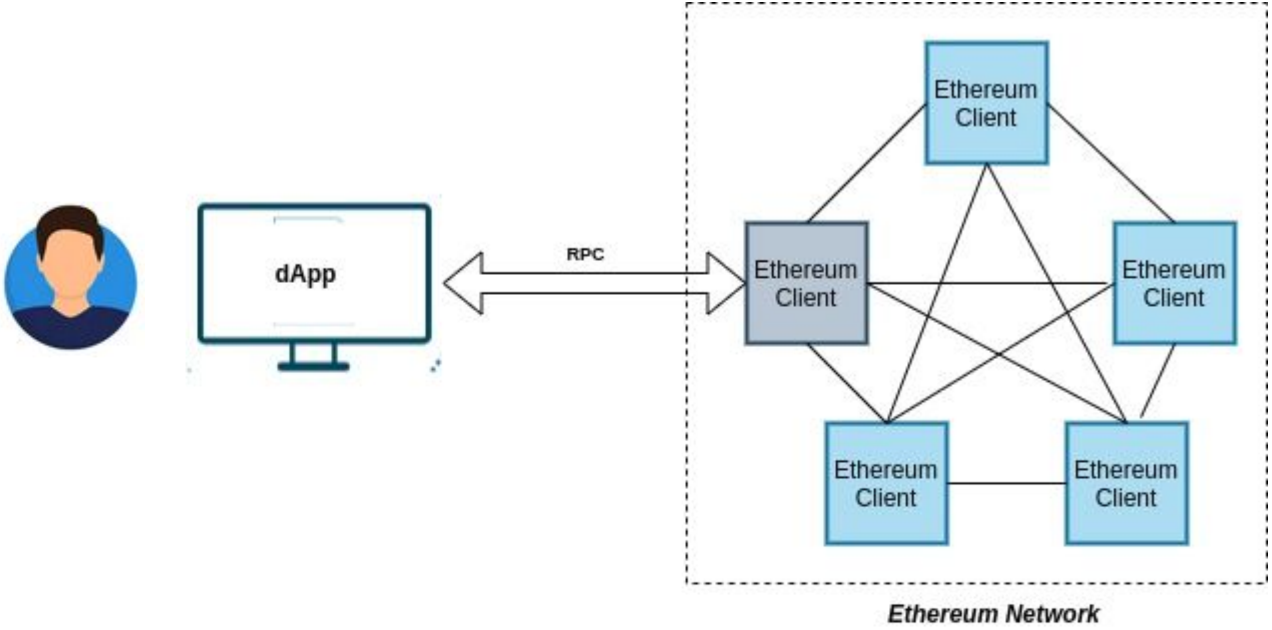
Remix IDE

- IDE for coding smart contracts in Solidity.
- Remix has an inbuilt ethereum node where you can deploy the contract and test it.
- https://remix.ethereum.org/
- By default files are stored in browser’s local storage.
- Refer https://remix-ide.readthedocs.io/

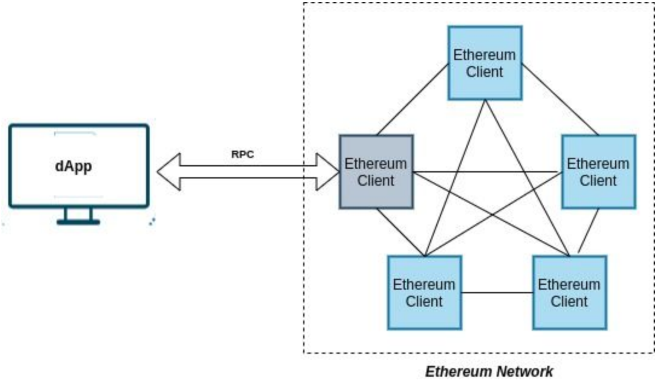
Smart Contract: Compilation & Deployment


Smart Contract
Solidity Compiler
Application Binary Interface (ABI)
JSON
Byte Code ready for Deployment
01001 1001000
Deploy
0xd9145 CCE52D3 86f254....
Smart Contract Address

Decentralized Application in Ethereum

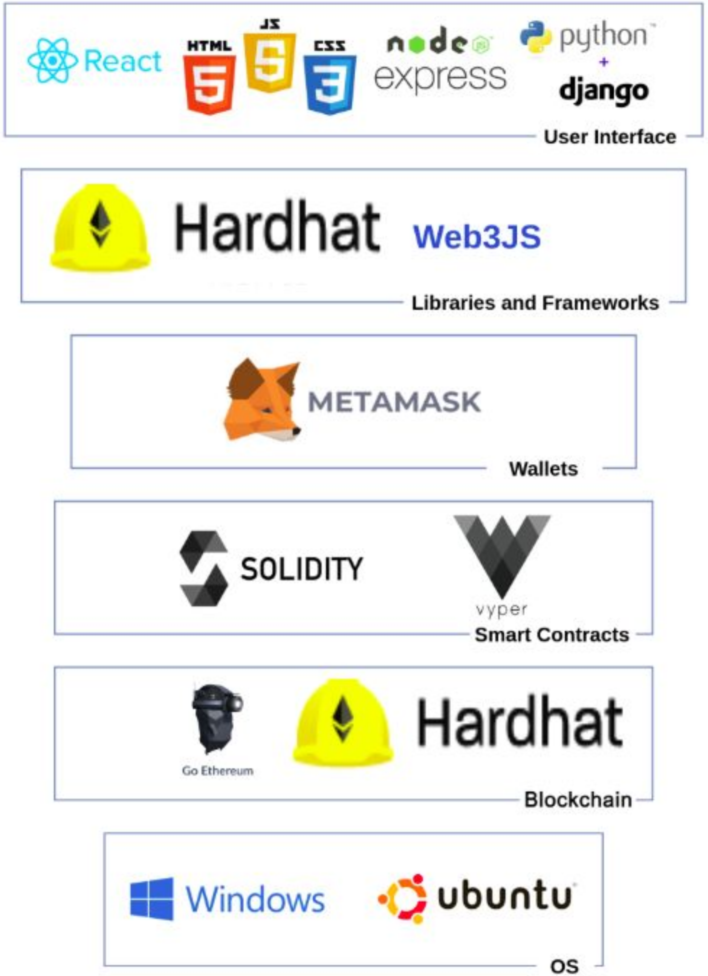


Creation of a DApp



- Design and implement smart contract
- Compile the contract
- Deploy the contract on Ethereum Blockchain network using Ethereum clients
- Build a Web application (Front-end) that interact with the smart contracts.

Decentralized Applications Tech Stack



- Upgrades
- Ethereum clients

Thank You