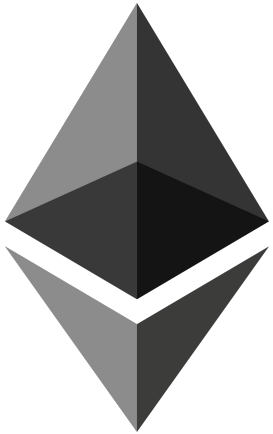
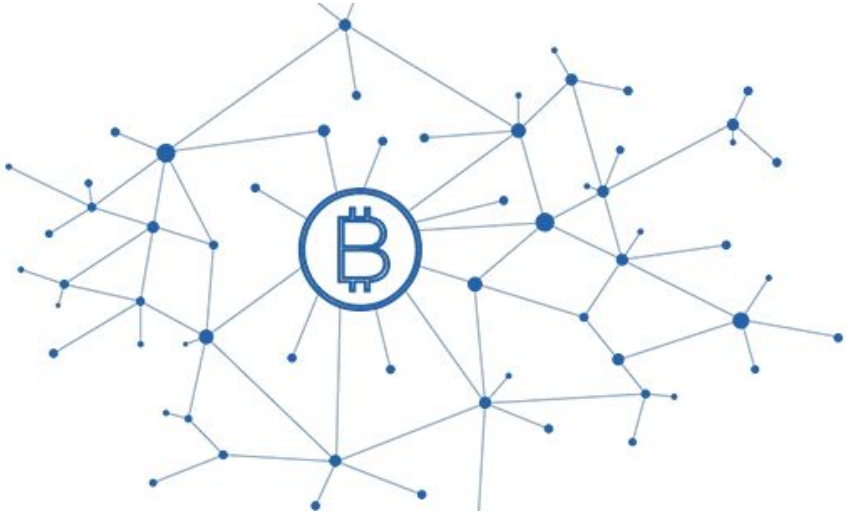


Ethereum

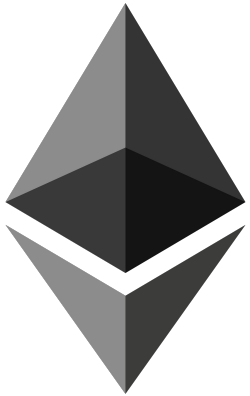
Beyond Bitcoin

Bitcoin - The decentralized financial platform

Bitcoin's **Backbone** - **Blockchain** Technology

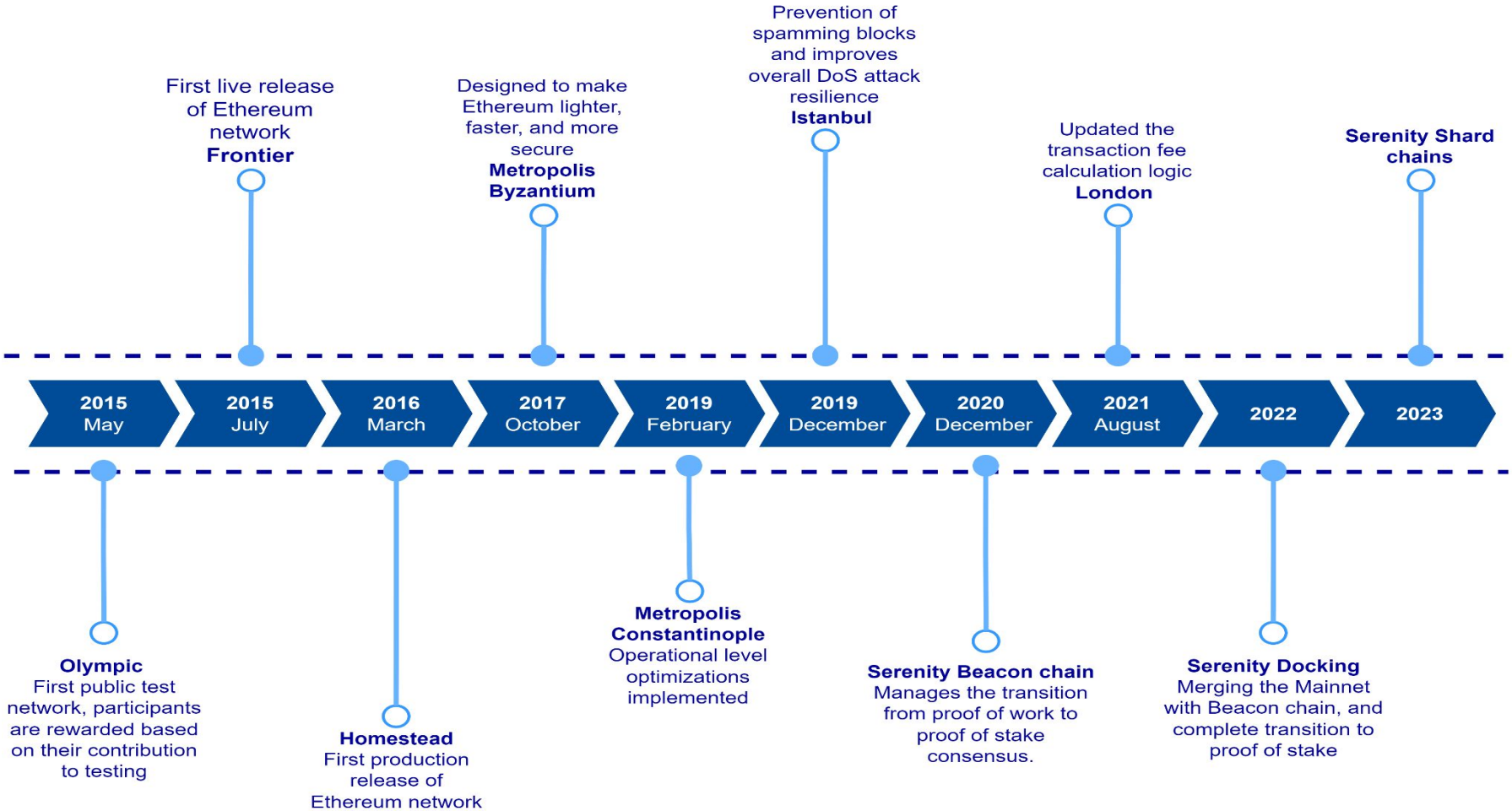


What is Ethereum Blockchain?



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

Evolution of Ethereum



Ethereum World Computer

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

Ethereum blockchain is a horizontal technology comprised of 4 basic components

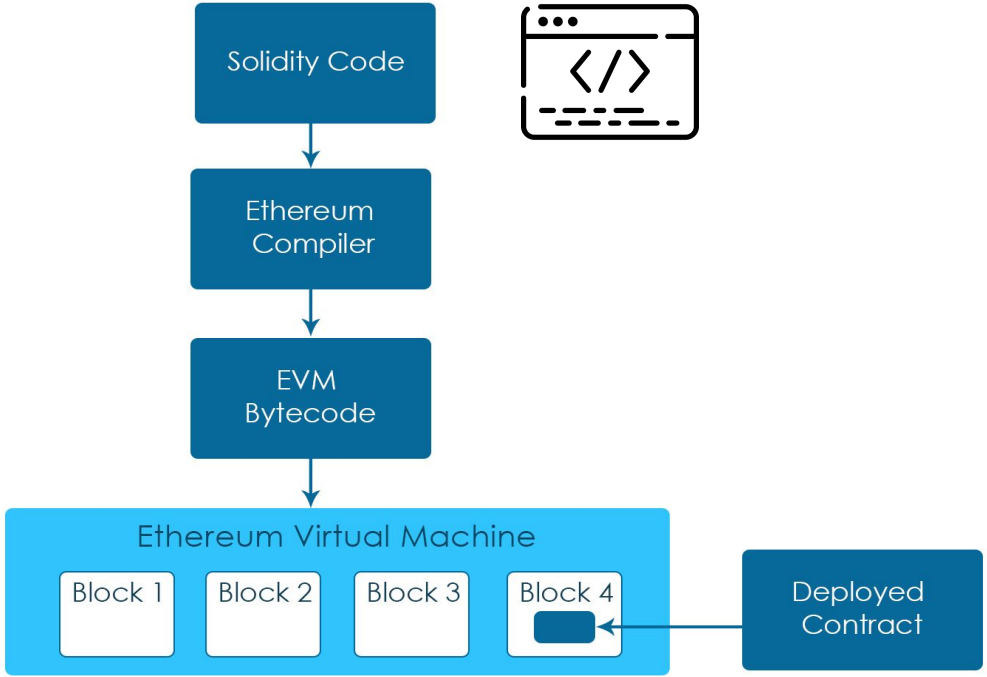
Digital Ledger: A continually updated, network hosted database of all transactions

Consensus Mechanism : Responsible for verifying and Updating transactions

Digital Asset: The good transacted on a Blockchain

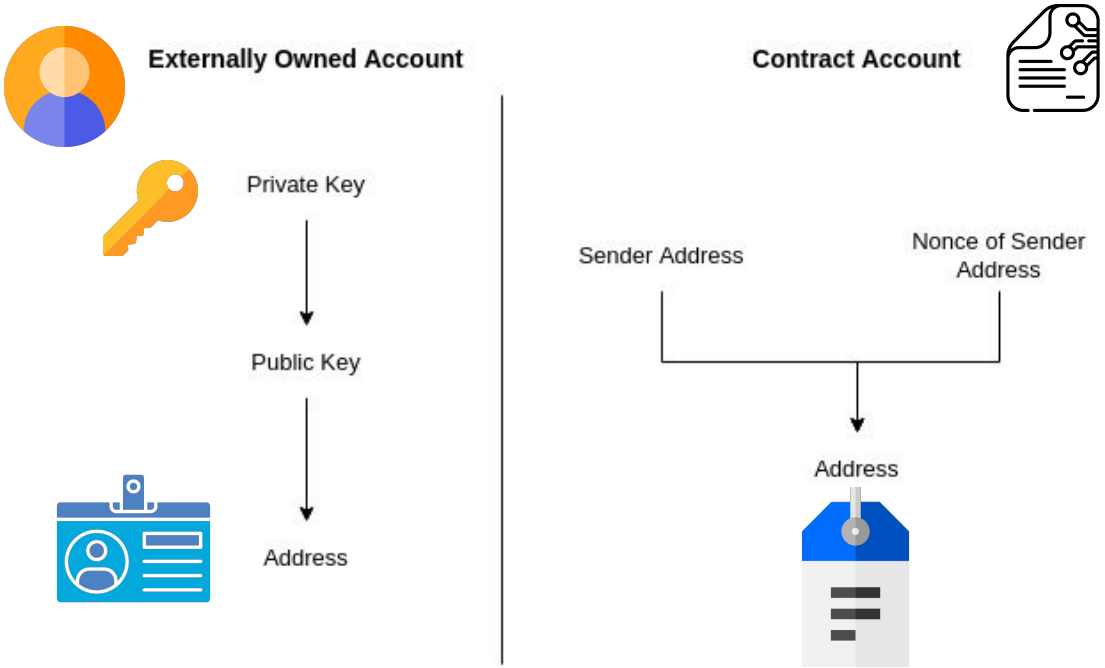
Network Participants: Able to manipulate the Ledger and view past transactions

About Ethereum Virtual Machine



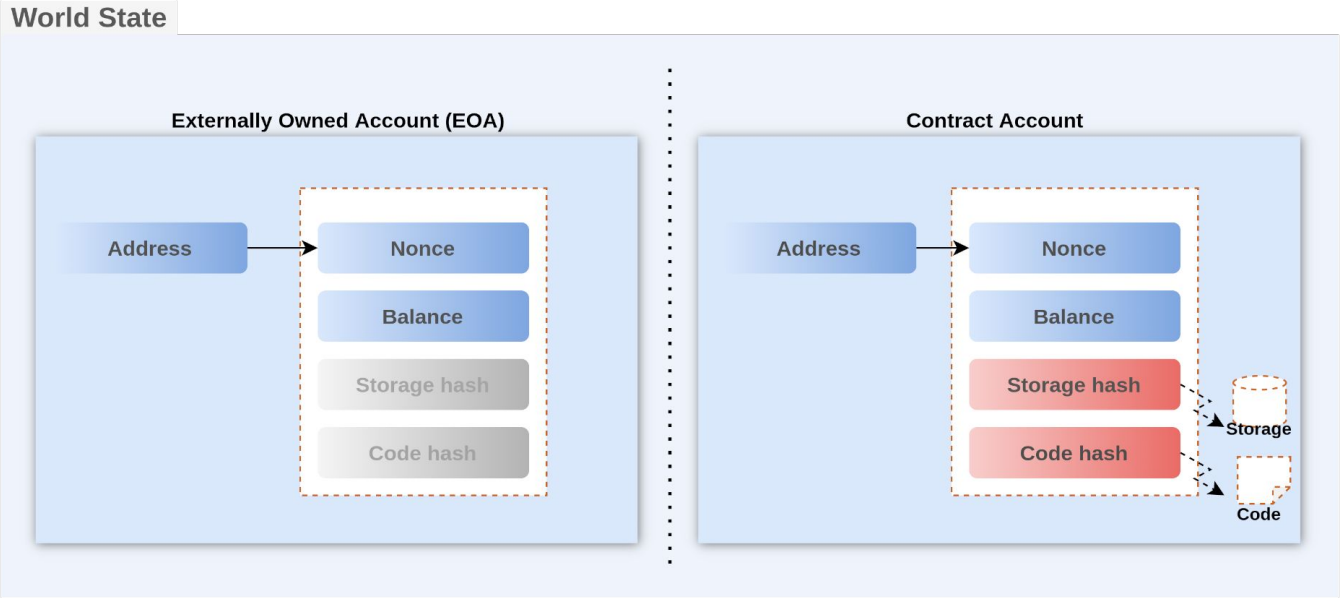
Accounts

An Identity in the pseudo anonymous Ethereum network.



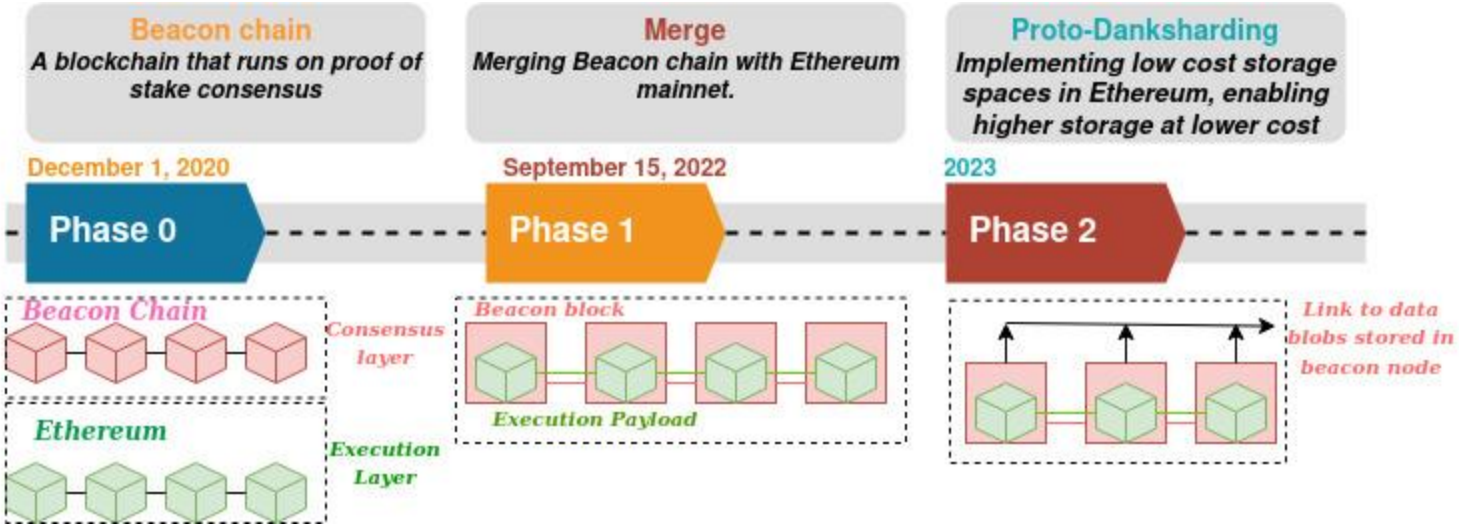
Accounts

Externally Owned Account (EOA) and Contract Account

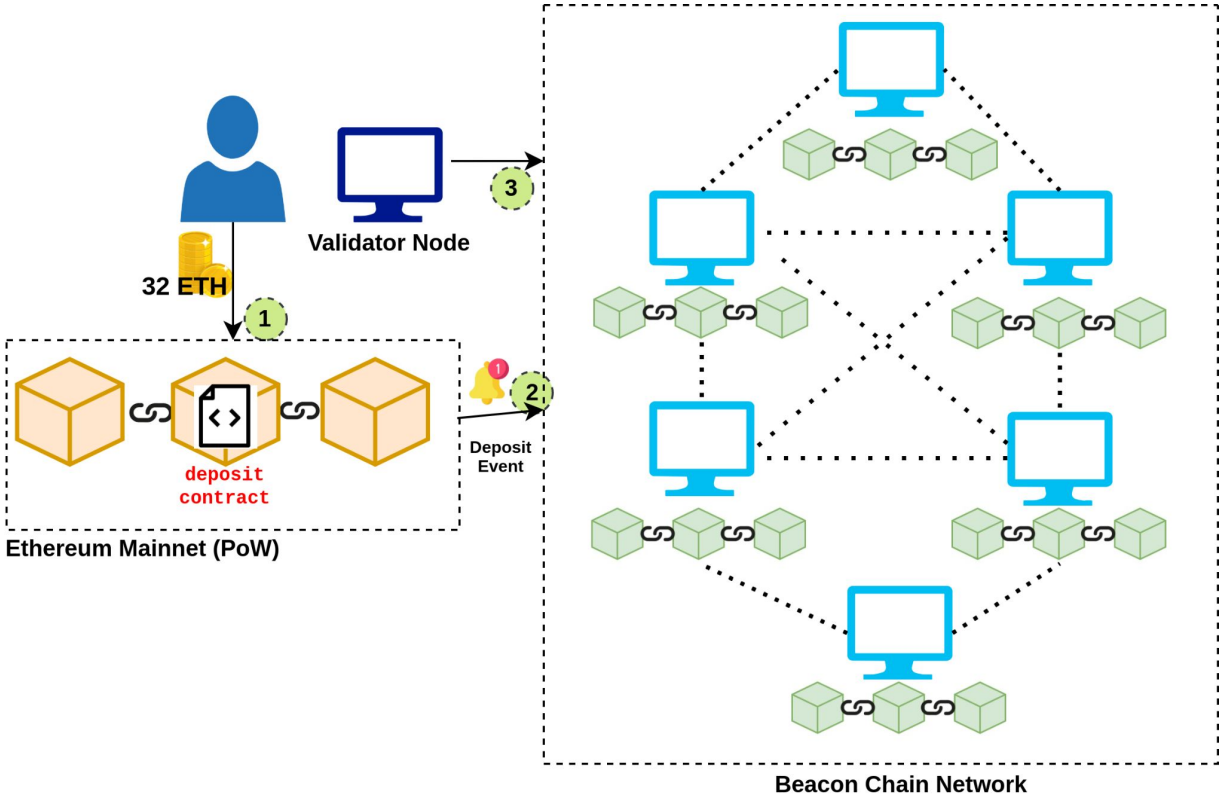


The Ethereum Upgrades

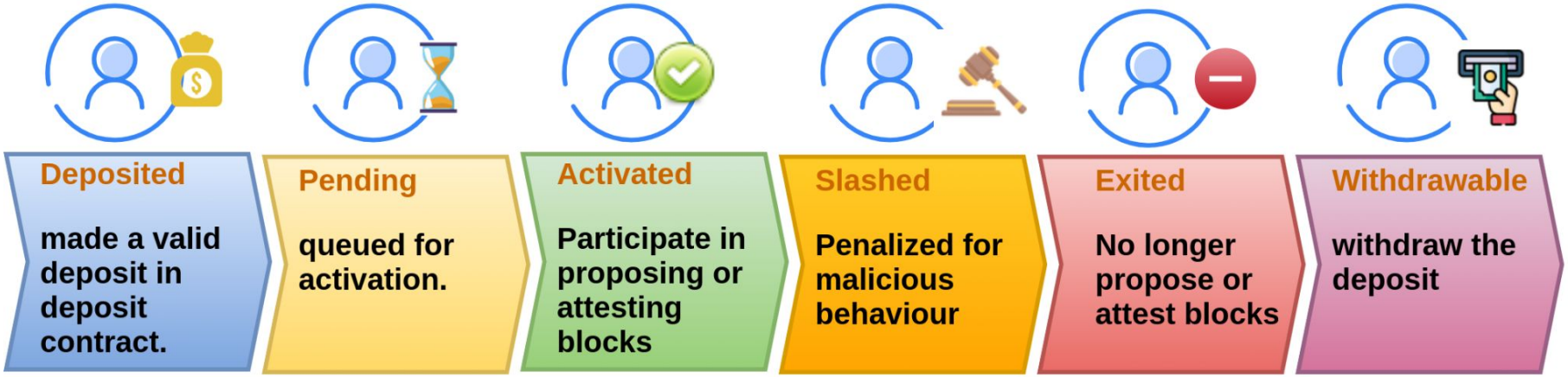
Ethereum Upgrade Roadmap



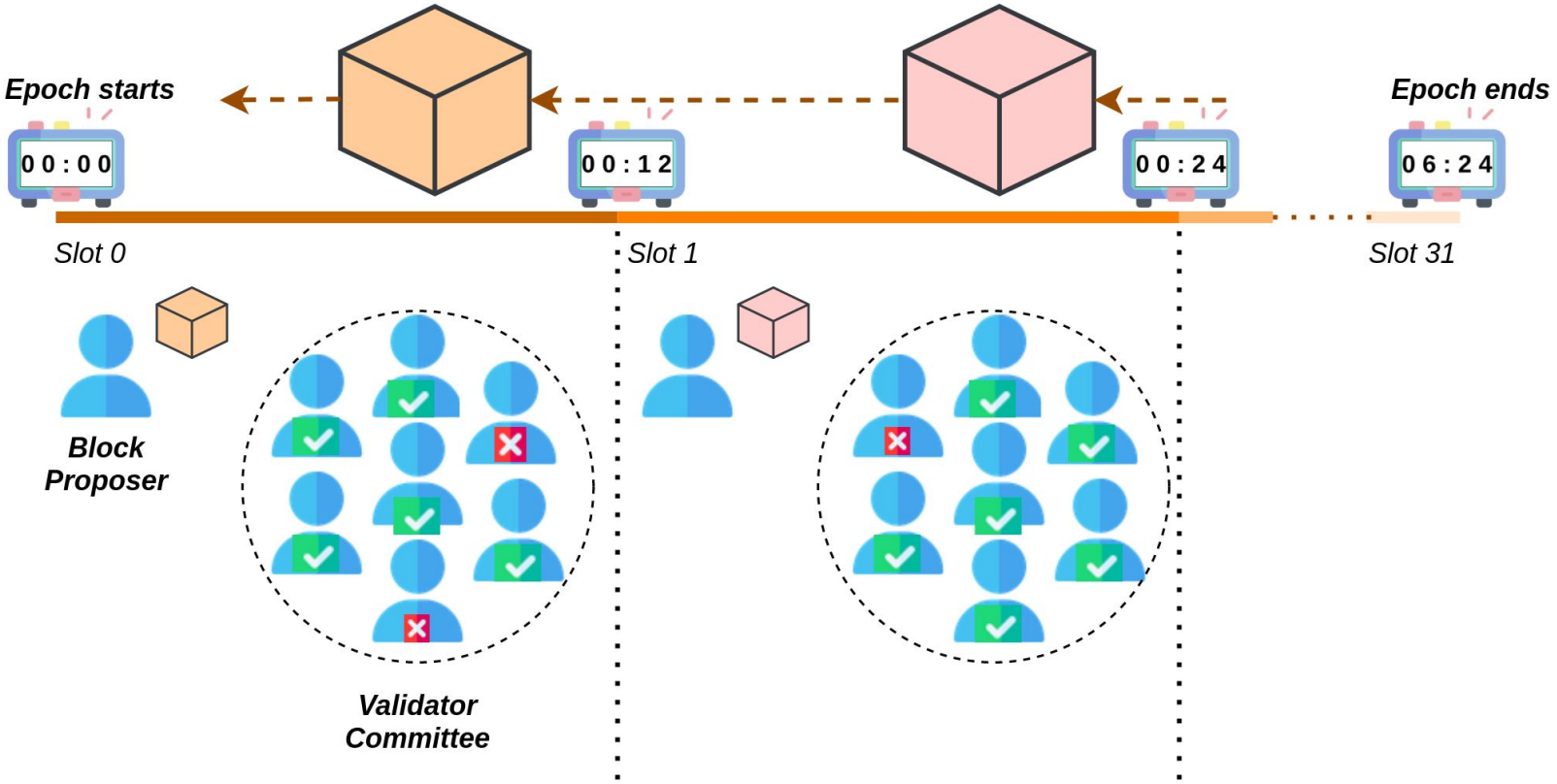
Phase 0: The Beacon Chain



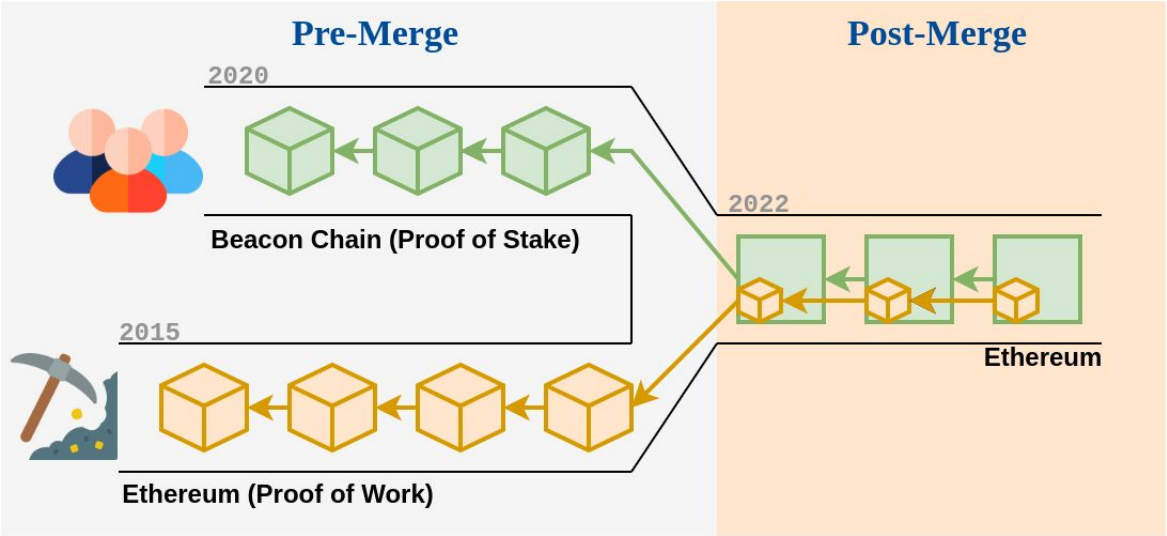
Validator Lifecycle



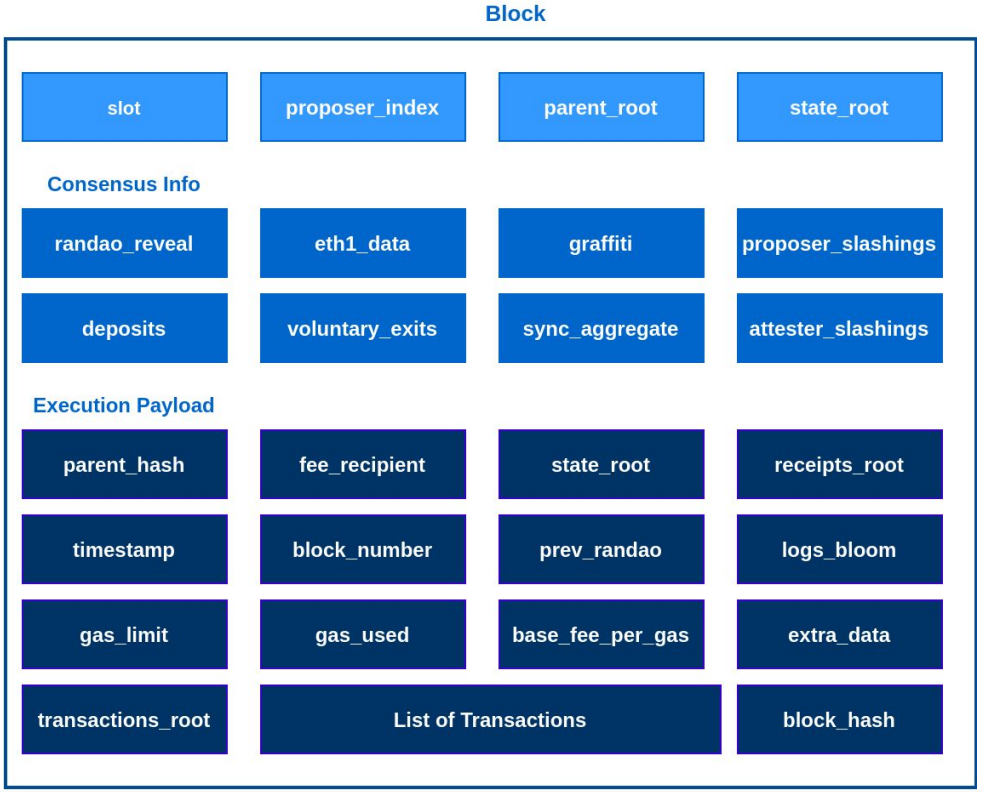
Proof-of-Stake



Structure of a Block



Ethereum Block Components

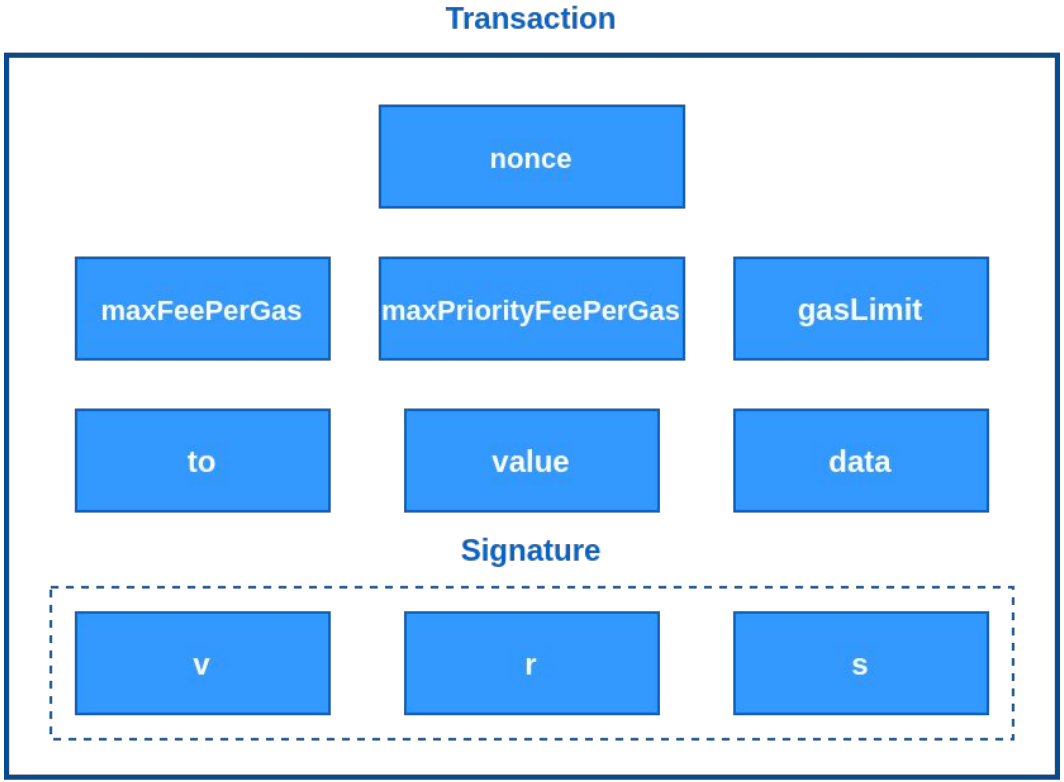


Ethereum Transaction

- 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



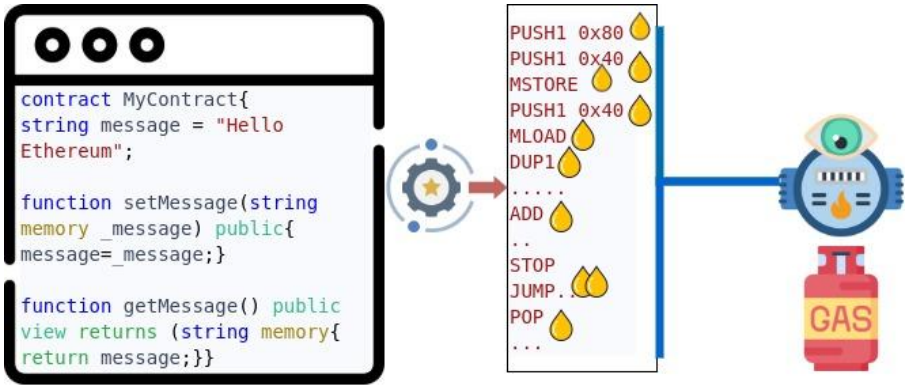
Transaction Cost: Ether

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.



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)

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

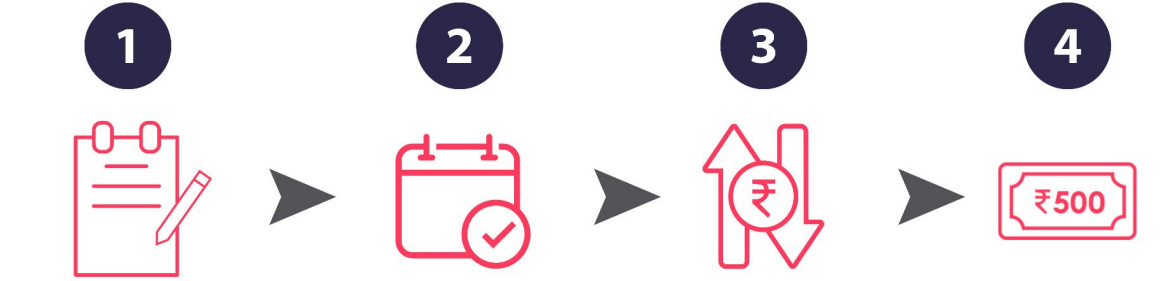
Ref: https://thedailygwei.substack.com/p/this-is-eip-1559-the-daily-gwei-300

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:



Pre-programmed Contracts

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

Chain of Events

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

Value Transfer

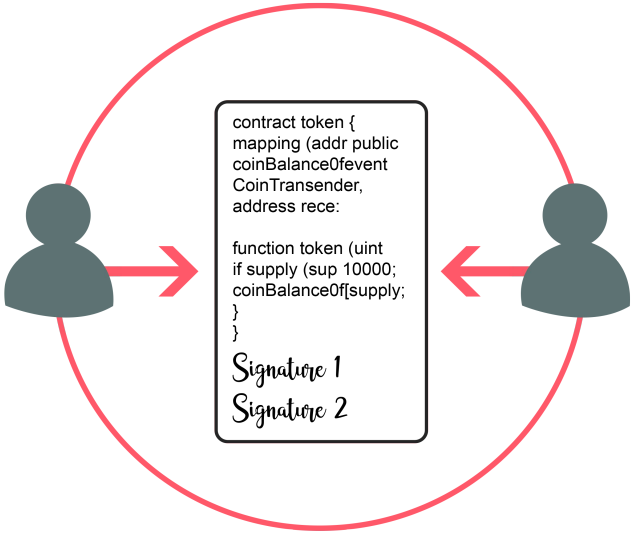
Once the code gets executed, the terms of contract makes sure that the transfer is made to the relevant parties.

Settlement

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

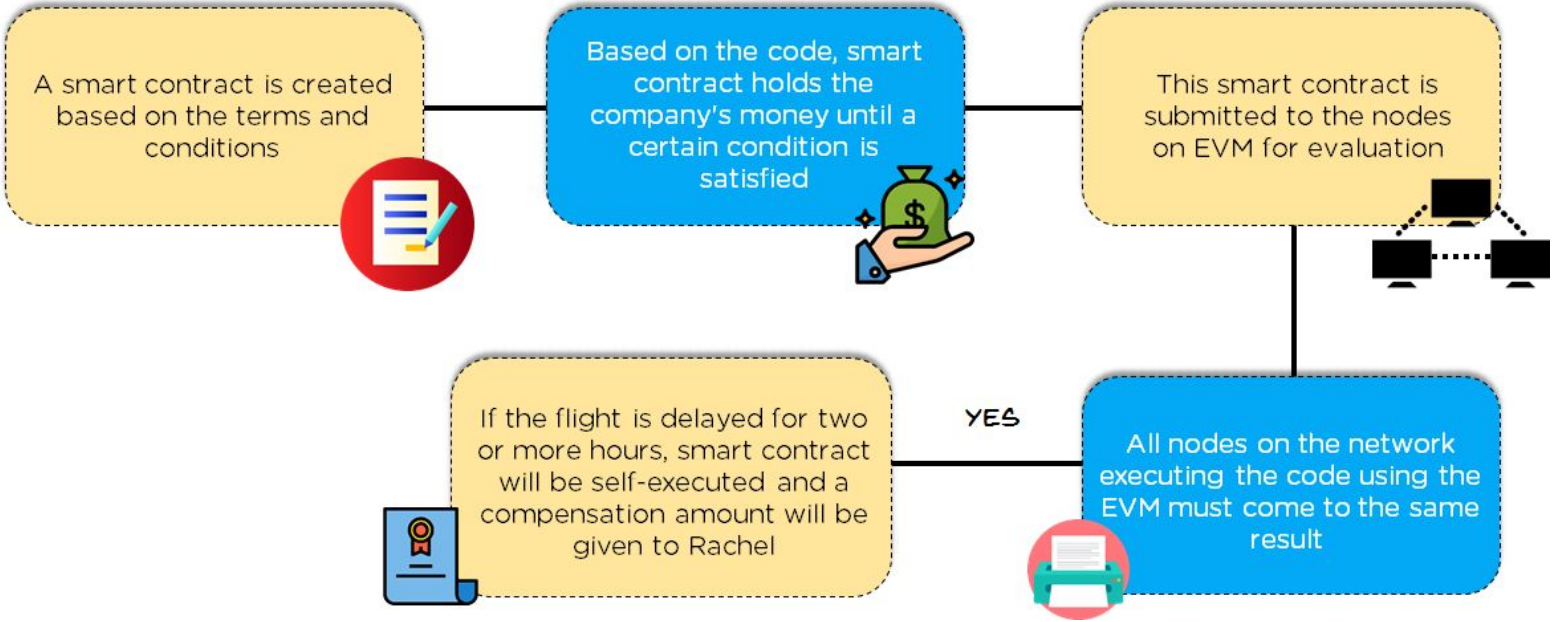
Benefits

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



A use case

Flight Delay Insurance



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

```
1  // SPDX-License-Identifier: GPL-3.0  //Defining Source Code License
2  pragma solidity ^0.8.7 ;              //Version of Solidity
3
4  contract Storage {                   //Contract name = Storage
5
6      uint256 number;                  //State variable, unsigned integer
7
8
9      function store(uint256 num) public { // function to input data
10         number = num;
11     }
12
13
14     function retrieve() public view returns (uint256){ // function to get data
15         return number;
16     }
17 }
```

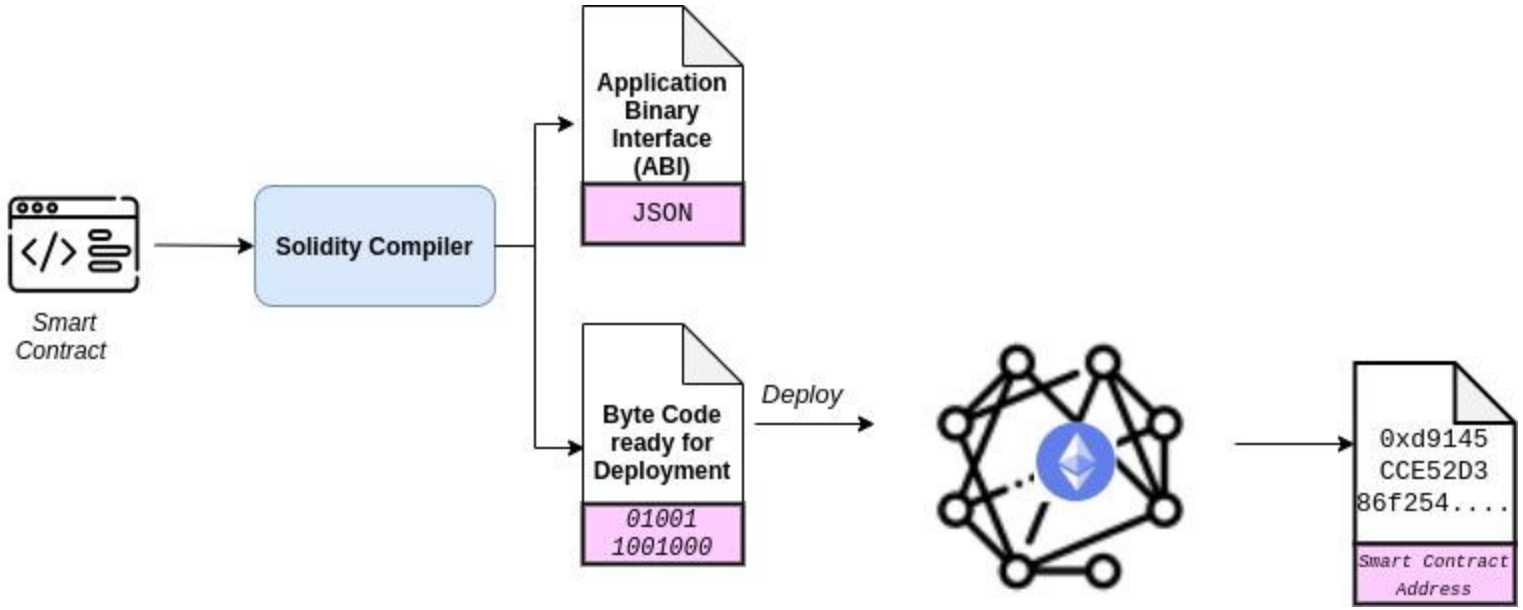
Ethereum Wallets

- 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/

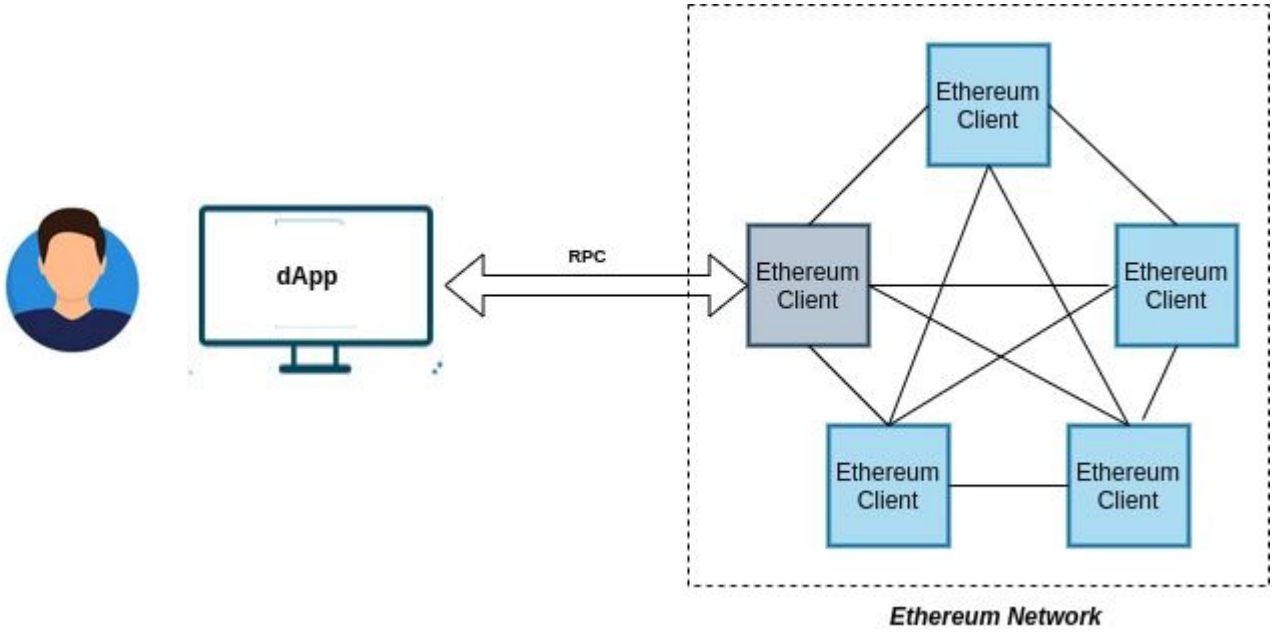
Remix IDE

- 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/

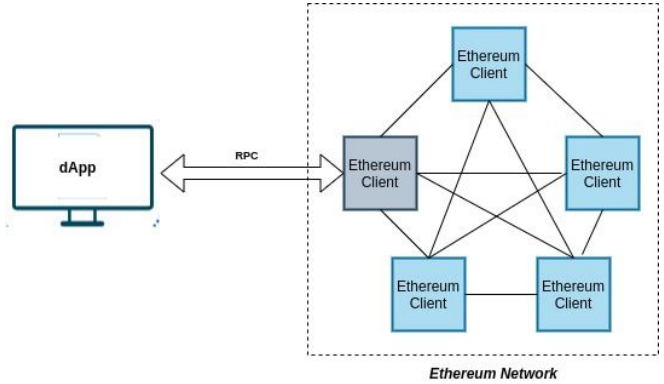
Smart Contract: Compilation & Deployment



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