What is Ethereum

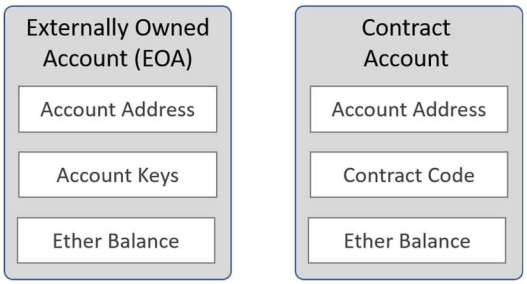
Ethereum is an open and programmable blockchain platform. Ethereum allows development of decentralized blockchain application through the use of smart contracts that perform arbitrary complex computations. Users can create and deploy smart contracts to the Ethereum platform and build decentralized applications. The platform is not owned or controlled by any entity and is powered by the peers who run the Ethereum nodes.

Ethereum Virtual Machine (EVM)

EVM is the runtime environment for smart contracts in Ethereum. The node in the Ethereum network run the EVM. All the nodes in the blockchain network perform the same computations, thus providing redundancy in the execution of smart contracts. While this massive amount of redundancy in not efficient approach for execution, but this is required to maintain consensus in the network where there is no centralized authority or a trusted third-party

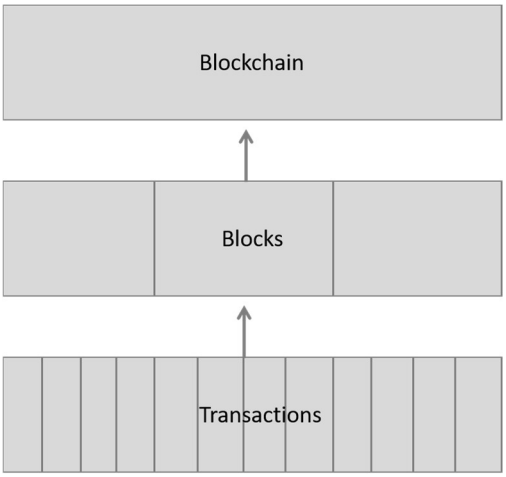
Accounts

Ethereum has two types of accounts – Externally Owned Accounts (EOAs) and Contract Accounts. EOAs are the accounts which are owned and controlled by the users. The contract accounts are controlled by the associated contract code which is store with the account. The contract code execution is triggered by transactions sent by EOAs or messages sent by other contracts.



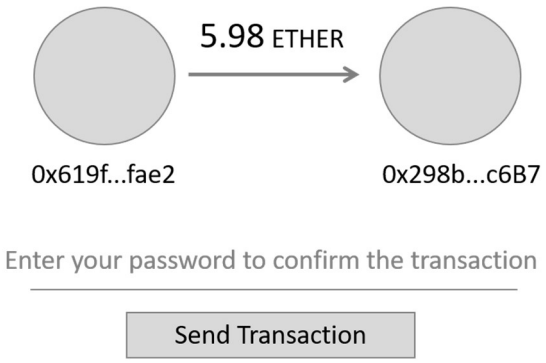
Blocks

The transactions in a blockchain network are bundled into blocks and executed on all the participating nodes. A block contains a transaction list, the most recent state, a block number and a difficulty value. The blocks are added to the blockchain at regular intervals.



Transactions & Messages

Transactions are the message which are send by EOAs to other EOAs or contract accounts. Each transaction includes the address of the recipient, transaction data payload, and a transaction value. When the transaction is sent to an EOA, the transaction value is transferred to the recipient. When the transaction is sent to a contract account, the transaction data payload is used to provide input to the contract function to be executed. Contracts deployed on a blockchain network can send messages to other contracts. The difference between a transaction and a message is that a message is produced by a contract while a transaction is produced by and EOA.



Mining

The transaction on a blockchain network are verified in a process called mining. The participating nodes in the network are given incentives in the form of Ethers for performing the mining operations. Miners compete to do complex mathematical computations and the node that wins earns a reward in Ethers. Miners produce blocks which are verified by other miners for validity. Once a winning block is selected, all other nodes update to that new block.

Ether

Ether is the currency which is used in the Ethereum blockchain network. The miners in the Ethereum network receive mining rewards in the form of Ethers. The base unit of Ether is called Wei (where 1 Ether = 10^{18} Wei)

Gas

Gas is the name of the crypto-fuel which is consumed for performing the operations on a blockchain network. All transactions on the network are charged a certain amount of gas. While sending a transaction, the sender sets a gas price which represents the fee the sender is willing to pay for gas. The senders of the transactions are charged a gas fee, which is paid to the miners and the balance is refunded to the sender. The gas fee paid is proportional to the amount of work that is needed to execute the transaction, in terms of the number of atomic instructions.

Decentralized Storage Platform – Swarm

Swarm is a decentralized storage platform and content distribution service for Ethereum. Swarm has been designed to serve as a decentralized and redundant store of Ethereum's public record, and also to store and distribute Dapp code. Swarm is a peer-to-peer storage platform which is maintained by the peers who contribute their storage and bandwidth resources.

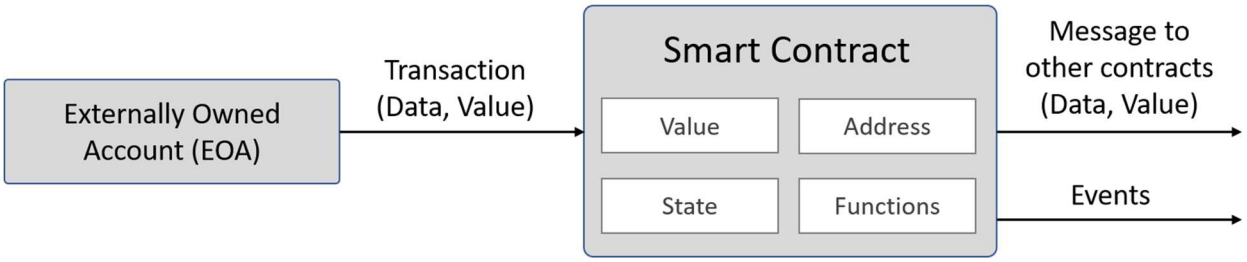
Decentralized Messaging Platform – Whisper

Whisper is a communication protocol that allow decentralized application (Dapps) to communicate with each other. With Whisper, Dapps can publish messages to each other. Whisper message are transient in nature and have a time-to-live (TTL) set.

Smart Contracts

Smart contract is a piece of code that resides on a blockchain and is identified by a unique address. A smart contract includes a set of executable functions and state variables. The function code is executed when transactions are sent to the function. The transactions include input parameters which are required by the functions in the contract. Upon the execution of a function, the state variables in the contract change depending on the logic implemented in the function.

Smart Contract structure

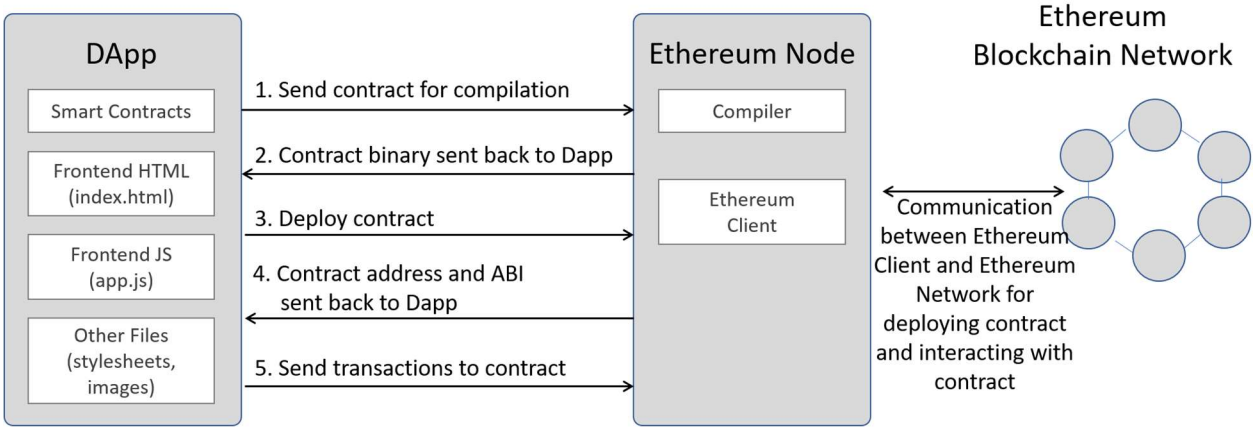


Decentralized Application (Dapps)

A Decentralized Application (or Dapp) is an application that use smart contracts. Dapps provide a user-friendly interface to smart contracts. A cryptocurrency application is an example of a Dapp the runs on a blockchain network. A decentralized application (Dapp) comprises smart contracts and files for web user interface front-end (HTML, JavaScript, stylesheets and images). Building a Dapp involves the following steps:

01. Implement smart contracts in a high-level language.
02. Compile the contracts with language-specific compilers to generate the contract binary
03. Deploy the contracts on Ethereum Blockchain network using Ethereum clients.
04. Build web application that interact with the smart contracts.

Dapp creation workflow



Tools & Interface

These are the tools and interfaces required for developing application on the Ethereum blockchain platform.

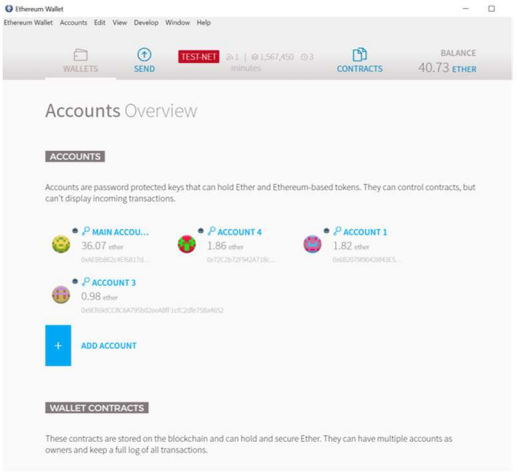
Ethereum Clients

Ethereum clients allow us to setup and Ethereum node on our coputer. An Ethereum client is like a Java Virtual Machine (JVM) and allows us to run Ethereum programs. With an Ethereum client, we can participate in the Ethereum network and perform tasks such as creating accounts and contracts, sending Ether to other accounts, sending transactions to contracts, mining on Ethereum network and other tasks related to the Ethereum Blockchain network. (Geth = Go-ethereum)

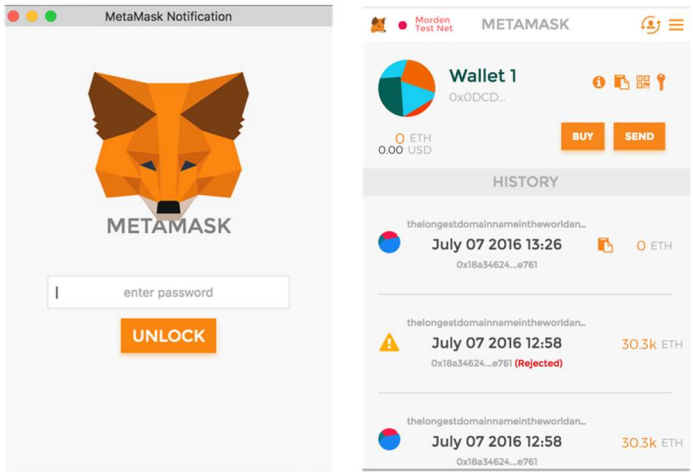
Graphical User Interfaces

The Mist Ethereum Wallet application provides a graphical user interface for performing tasks such as managing Ethereum accounts, sending Ether to other account, deploying contracts, send transaction to contracts and viewing account transactions. However, for users who do not want to install the Mist Browser and download the entire Blockchain, the MetaMask Chrome extension provides a user-friendly option to interact with the Dapps from Chrome browser.

Ethereum Wallet



MetaMask



Compilers

Ethereum provides various high-level languages for implementing contracts, including Solidity which is similar to JavaScript.

Dapp Frameworks

Dapp framework such as Truffle or Embark simplify the steps involved in the creation of Dapps.

Web3 JavaScript API

Web3 is a JavaScript API created by the Ethereum Foundation which provides methods for interacting with the Ethereum network.

JSON RPC

The Ethereum JSON-RPC is a stateless and lightweight remote procedure call (RPC) protocol that is used by Ethereum clients implemented in different programming languages to interact with an Ethereum node.

From Web 2.0 to the Next Generation Decentralized Web

The blockchain technology stack enable a transition from Web 2.0 to the next generation decentralized web. In the context of Ethereum, the term Web 3.0 is often used to refer to this next generation decentralized web. Here are the differences between a Web 2.0 application and a Dapp.