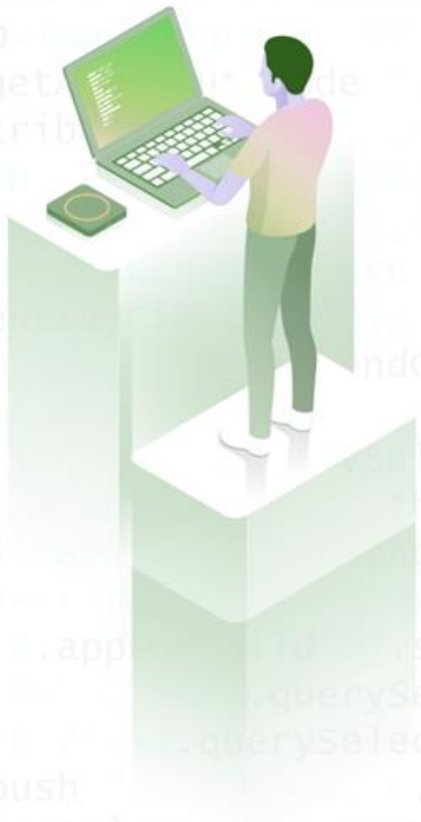
TECHNOLOGY

IIT KANPUR
Indian Institute of Technology, Kanpur

Professional Certification Program in Blockchain

TECHNOLOGY



Ethereum Blockchain

Learning Objectives

By the end of this lesson, you will be able to:

- Discuss the features of Ethereum and the differences between Ether and Bitcoin
- Analyze the various components of Ethereum such as smart contracts, EVM, and decentralized applications
- Classify the various Ethereum wallets
- Discuss the various Ethereum clients available

TECHNOLOGY

Introduction to Ethereum

Introduction to Ethereum

Ethereum is a decentralized platform that runs smart contracts and has its own cryptocurrency known as Ether.

Features of Ethereum

Smart Contracts

Automated programs that execute upon satisfying certain conditions

Currency

They have Ethers based on ERC-20 tokens

Fast Transactions

Mining speeds are very high and transactions are completed in 10-12 seconds

Community

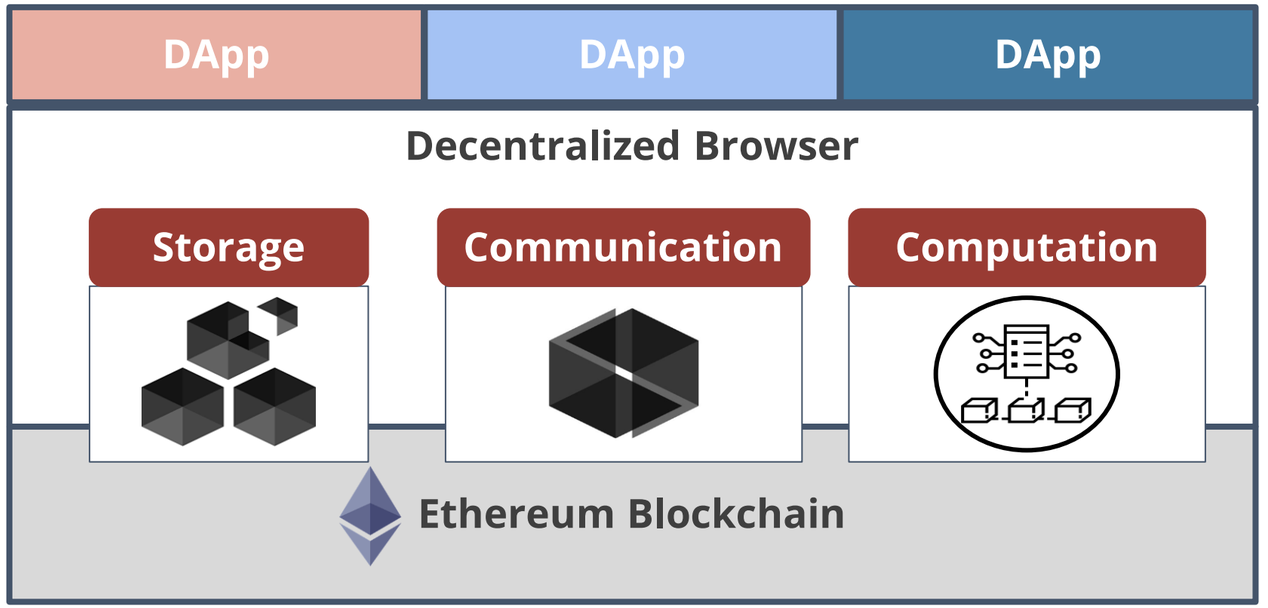
Ethereum has extensive developer community support

Security

Ethash and smart contracts are used to enhance security

Ethereum Ecosystem

The Ethereum ecosystem consists of technologies that help enable decentralized browser and applications such as storage, dynamic communication, and distributed computation.



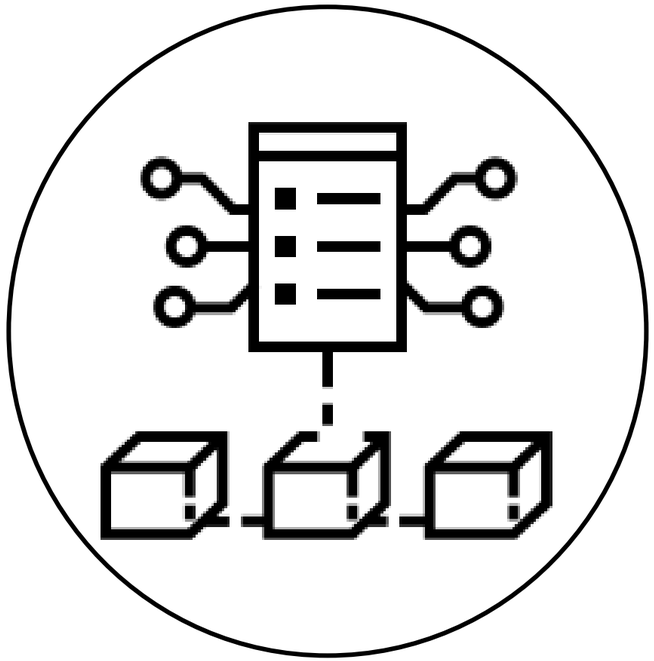
Swarm

- Swarm is a censorship resistant, permissionless, and decentralized file share and storage platform.
- It stores Ethereum records to distribute blockchain data as well as Dapp codes throughout the network.
- It runs on a peer-to-peer basis that allows to transfer resources/data among the nodes.

Whisper

- Whisper is an identity-based messaging system. It was designed for easy and efficient broadcasting and low-level asynchronous communication.
- It uses a TCP-based transport protocol called RLPx transport protocol for communication and encryption.
- It can theoretically provide 100% secrecy and also prevents DDoS attacks by using a consensus mechanism.
- The drawbacks of Whisper are:
  - It is a low-level API with limited bandwidth and uncertain latency.
  - It has unreliable packet tracing and performance is reduced if packet tracing is prioritized.

Smart Contract



- Smart contracts are computer programs that are stored on Ethereum's Blockchain.
- Contracts can be used to build currencies and store financial assets.
- They are used to design voting systems, decentralized organizations, data feeds, title registries, and thousands of other applications.

Smart Contract Languages

Contracts are compiled into bytecode on the Ethereum Virtual Machine and deployed to Ethereum Blockchain for execution.

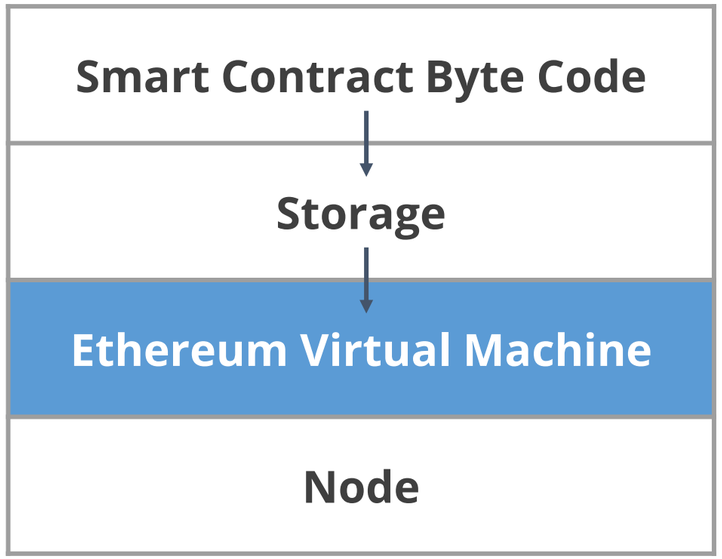
Various languages may be used to write these contracts, but the below mentioned ones are the most popular:

Solidity

Julia

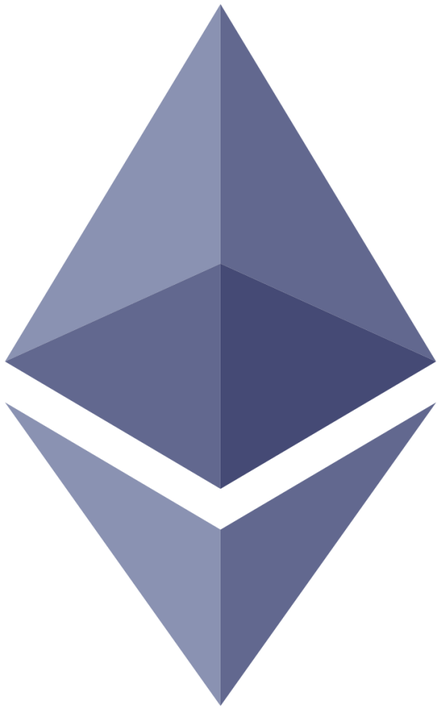
Vyper

Ethereum Virtual Machine (EVM)



- Ethereum Virtual Machine (EVM) is the runtime environment for the smart contracts in Ethereum.
- Developers can create applications that run on the EVM using user-friendly programming languages such as Solidity.
- The EVM is sandboxed and completely isolated to protect the host computers from the threat of viruses or malicious intrusion attempts.

Ether



Ether is the primary digital asset or cryptocurrency of the Ethereum platform.

It is a transactional token that facilitates operation on Ethereum.

All Gas prices are paid in Ethers.

Bitcoin Vs Ether

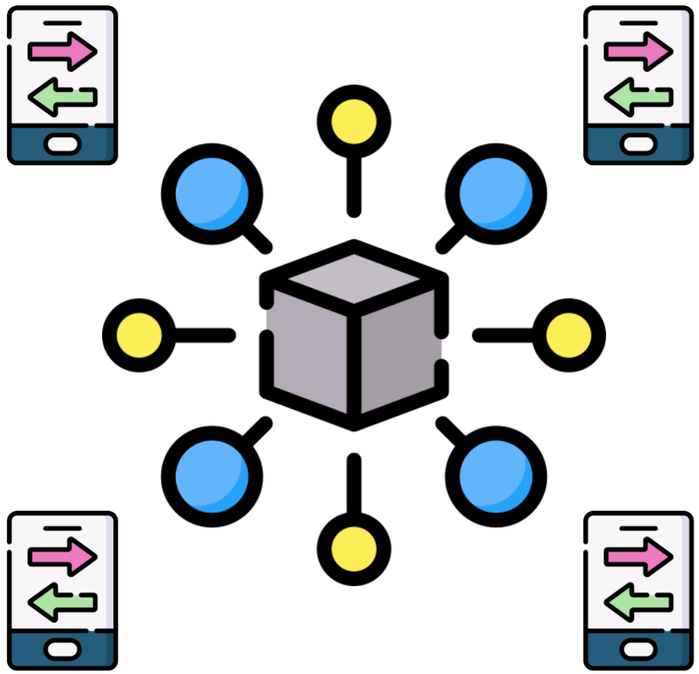
Bitcoin	Ether
Uses secure hash algorithm (SHA-256)	Uses Ethash algorithm
Used as currency for purchasing goods and services	Used as a currency and for making decentralized apps
Digital currency to compete against fiat currencies and gold	Mainly used for smart contracts
Transaction speed is slower	Transaction speed is much faster
Very high mining price	Lower Gas prices comparatively

Gas

Gas is a unit of measuring the amount of computational power required to run a smart contract or perform a transaction. It is similar to a transaction fee for every operation performed on Ethereum Blockchain.

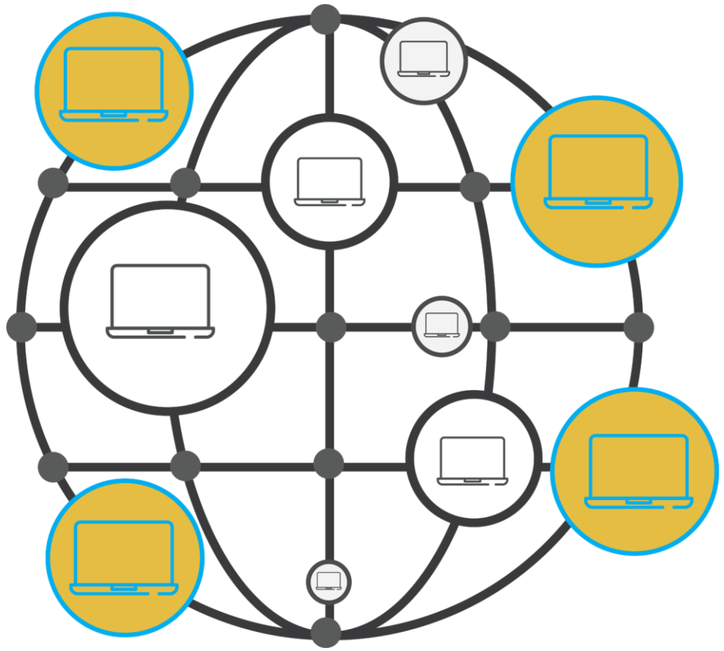
- The **Gas Limit** is the maximum amount of Gas that a user is willing to pay for performing an action or confirming a transaction (a minimum of 21,000).
- The **Gas Price** is the amount of Ether that the user is willing to spend on each unit of Gas.
- The transaction fee is calculated as **Gas Limit * Gas Price**

Decentralized Application (DApp)



- DApps are applications that run on a decentralized, distributed, peer-to-peer network, and do not have a central authority controlling the application platform.
- Their codes are open source and all users can access them irrespective of the region they reside in.
- All DApps run on the Blockchain network on top of smart contracts.

Decentralized Autonomous Organizations (DAO)



- DAOs are internet-based business organizations which are fully democratized and have no hierarchical management.
- DAOs are designed to hold the common assets and use a voting system to utilize these assets.
- DAOs exist entirely on Blockchain and are governed by the consensus protocols embedded into smart contracts.

Features of DAO

Improved stability

Negligible downtime

Higher reliability

No third-party involvement

Asset misutilization almost impossible

Enhanced privacy and security

Ethereum Networks

Ethereum Networks

Networks are different Ethereum environments that you can access for developing, testing, and releasing various decentralized applications. They are categorized into the following types:

Mainnet

The actual Ethereum network on which the cryptocurrency transactions take place.

Test Network

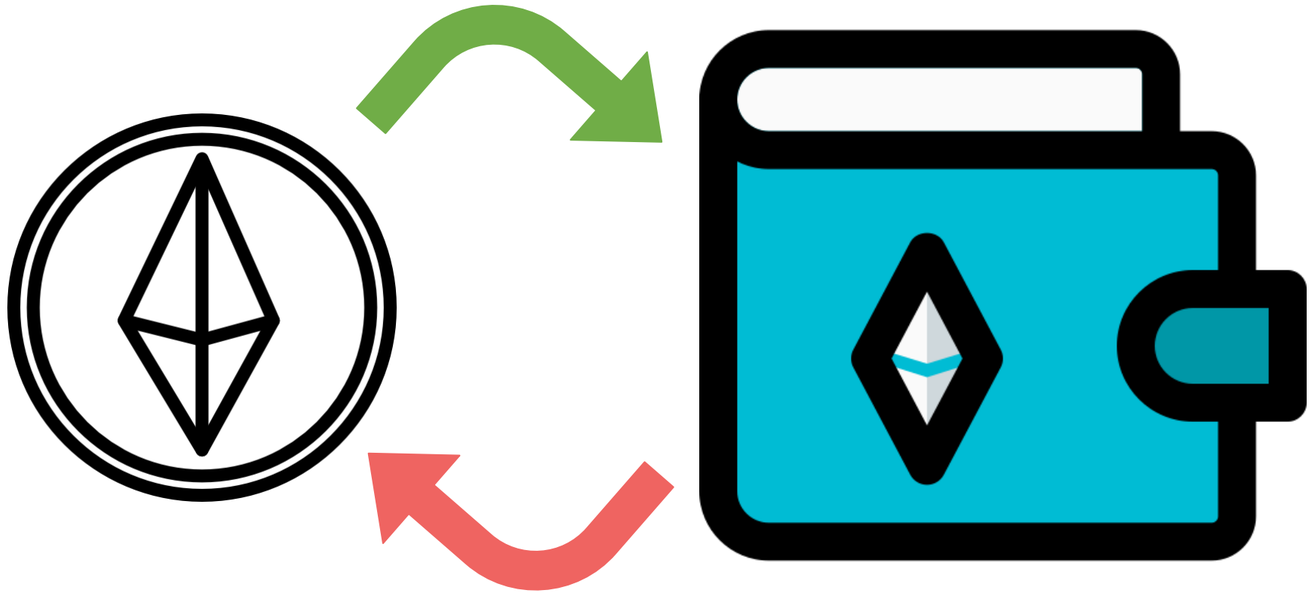
This network mimics the mainnet and can be used by developers to test their applications.

Private Network

This can be implemented by changing the parameters of the Ethereum network according to the needs of the user.

Main Network (Mainnet)

Mainnet is the live or production network of the Ethereum Blockchain. This is the network on which the actual monetary transactions take place, and the Dapps are hosted on.



Exploring the Ethereum Mainnet

Problem Statement: You are given a task to explore the Ethereum Mainnet.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to explore the Ethereum Mainnet:

1. Visiting the Etherscan website
2. Viewing and analyzing the latest block
3. Viewing and analyzing the data in a transaction

Test Networks

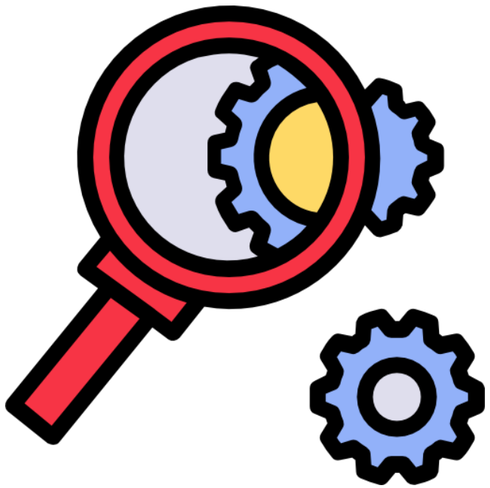
Ethereum provides a few test networks to developers which can be used to test their protocols, smart contracts, features, and applications before deploying them to the production network.

Ropsten

Proof-of-Work network, which mimics the mainnet

Kovan

Proof-of-Authority network for OpenEthereum clients



Görli

Proof-of-Authority network for all clients

Rinkeby

Proof-of-Authority network for Geth clients

Explore an Ethereum Test Network

Problem Statement: You are given a task to explore one of the Ethereum test networks.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to explore an Ethereum test network:

1. Visiting the Etherscan’s Ropsten web URL
2. Viewing and analyzing the latest block
3. Viewing and analyzing the data in a transaction

Ganache: Local Network

- Ganache is a lightweight replica of the Ethereum Blockchain.
- It can be installed on any operating system and replicates the actual Blockchain network.
- It is mainly used by developers for smart contract unit testing.

Installing Ganache Blockchain

Problem Statement: You are given a task to Install Ganache Blockchain network on your system.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to install Ganache Blockchain:

1. Downloading the latest version of Ganache from their website
2. Providing the required permissions to the Ganache image file
3. Running the Ganache software on your computer

Exploring Ganache Blockchain

Problem Statement: You are given a task to Explore Ganache Blockchain network.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to explore Ganache Blockchain:

1. Quickstarting the Ganache instance and exploring the network
2. Creating a private Blockchain in Ganache with custom parameters

Private Network

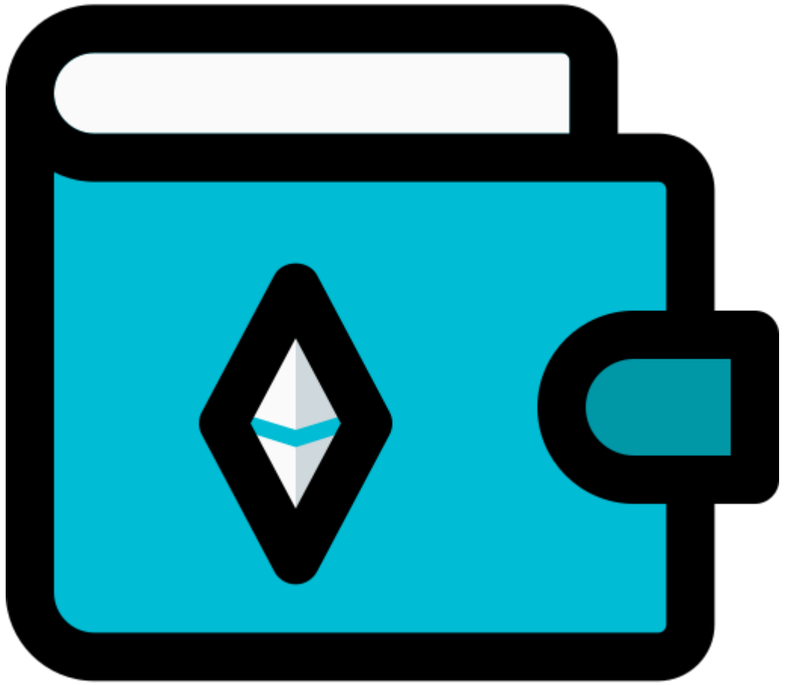
Ethereum does provide the capability to create your own private network with custom parameters. Private networks are not very popular in Ethereum but they do exist.

TECHNOLOGY

Ethereum Wallets

Ethereum Wallets

Ethereum wallets help in connecting with the Ethereum Blockchain network, storing Ether, and performing monetary transactions from one account to another.



Types of Ethereum Wallets

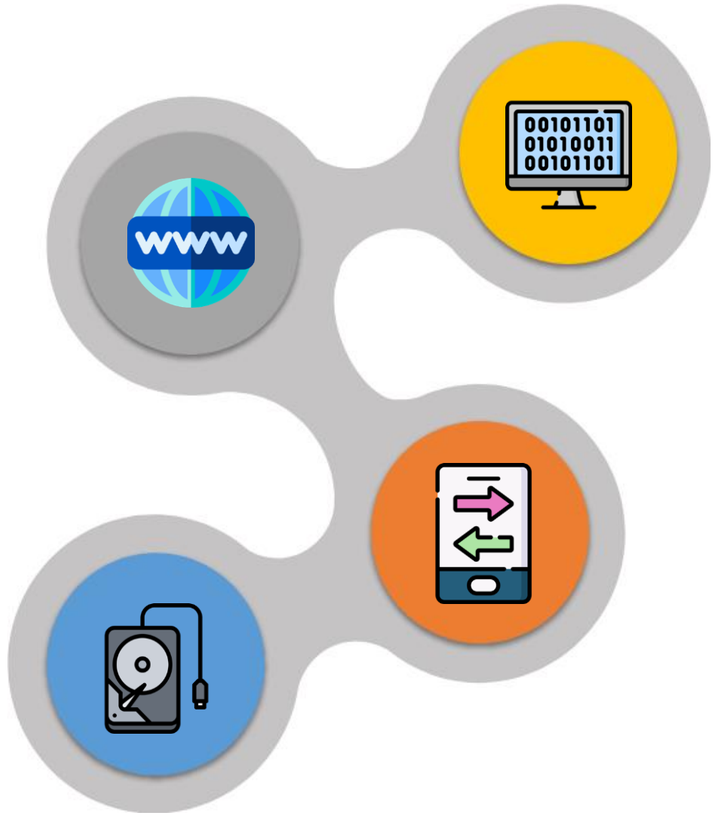
Ethereum wallets are mainly categorized into the below types:

Web Wallets

Installed as an extension to web browsers

Hardware Wallets

Most secure as they store keys in physical devices



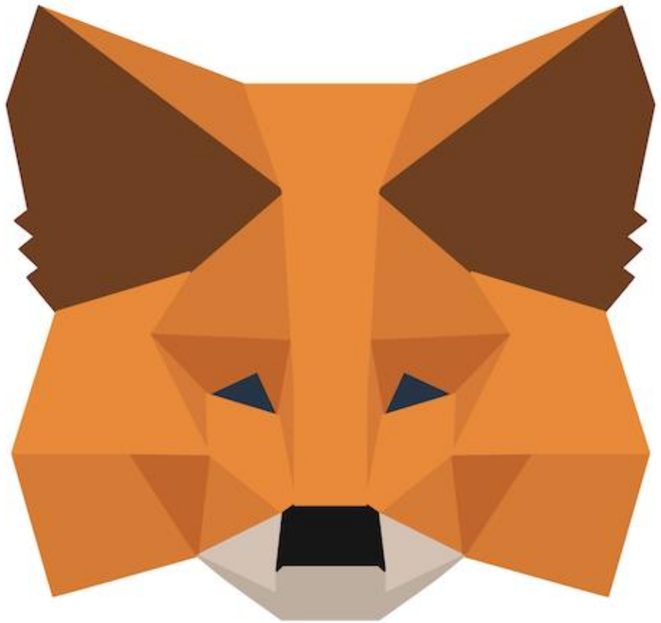
Desktop Wallets

Installed on desktops to perform transactions

Mobile Wallets

Light-weight mobile applications

Metamask



- Metamask is a web wallet that allows users to send and receive Ethers and other Ethereum-based cryptocurrencies.
- It also acts as a gateway to interact with other decentralized apps.
- It keeps the private information secure, and uses randomly generated multi-word phrases as opposed to traditional single-word passwords.

Install Metamask and Set up the Wallet

Problem Statement: Add the Metamask extension to your browser, create an account, and configure your Ethereum wallet.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to install and set up Metamask wallet:

1. Adding the Chrome extension to the browser
2. Setting up the account security and initializing a wallet account

Connect Metamask to a Ganache Test Network

Problem Statement: You are given a task to connect your Metamask wallet to a Ganache test Blockchain network.

password in the respective fields, and click Login.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to connect Metamask to Ganache test network:

1. Configuring Metamask to connect to the Ganache localhost
2. Adding an account from the local network to the wallet

Mist Wallet

- It is a web and desktop wallet developed by the founders of Ethereum.
- It was initially developed as a browser for accessing Dapps and the wallet was a Dapp built into the browser.
- It is used for transacting, and storing Ethers, creating multi-signature wallets, and deploying smart contracts.

Install and Explore the Mist Wallet

Problem Statement: You are given a task to install and configure the Mist wallet.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to install and explore the Mist wallet:

1. Visiting the Mist website and downloading the latest release
2. Creating an Ethereum account using Mist
3. Performing a mock transaction using Mist wallet

Ethereum Clients

Ethereum Clients

Ethereum clients provide an interface to become full nodes. They can then verify transactions, parse Blockchain and smart contract data, and mine and create blocks.

Types of Ethereum Clients

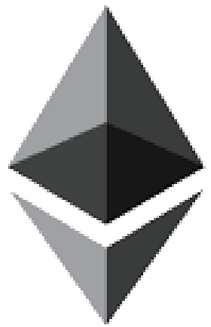
Ethereum clients are mainly categorized in the below types:

Command Line Interface

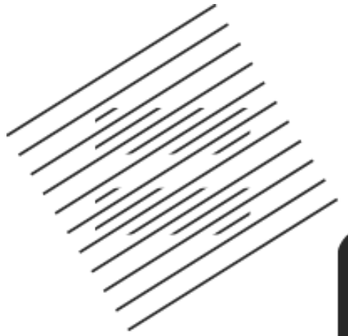
A terminal-based application which is used to perform the functions of a full node

Graphical User Interface

A visual interface that can be used as a web/desktop application to perform full/light node activities



Go Ethereum



parity

Go Ethereum (Geth)

Geth is a terminal-based Ethereum client implemented in the Go language. It was developed by the Ethereum foundation and provides a command line interface for exercising full node powers.

Features of Geth

- Mine blocks and earn Ether
- Perform transactions and transfer funds
- Validate transactions and interact with smart contracts
- Update and maintain Blockchain history

Connecting to Ethereum Using Geth

Geth allows us to connect to Ethereum mainnet, Ropsten, and Rinkeby network. Geth does not allow us to connect to the Kovan network. We need to use Parity for that.

Command to connect to the Main network

```
geth
```

Command to connect to the Ropsten network

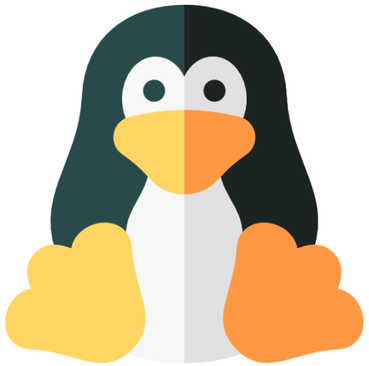
```
geth --ropsten
```

Command to connect to the Rinkeby network

```
geth --rinkeby
```

Geth Data Storage

Geth client connects with the other peers and downloads the latest Blockchain data to the local machine. Data gets stored in below locations and it can be changed with the **--datadir** parameter.



Linux

~/.ethereum

Windows

~/AppData/Roaming/Ethereum

Mac

~/Library/Ethereum

Install Geth Client

Problem Statement: You are given a task to install Geth client and explore the basic commands.

password in the respective fields, and click Login.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to install Geth client:

1. Installing Geth client using the terminal

Set up a Private Blockchain Node Using Geth

Problem Statement: You are given a task to set up a private Blockchain node in your machine using Geth.

password in the respective fields, and click Login.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to set up a private Blockchain node using Geth:

1. Installing the Geth client in our machines
2. Configuring the Geth client to emulate light node functionalities

Parity

Parity is a light-weight, fast, and multi-network Ethereum client written in the Rust language. This is one of the most commonly used third-party Ethereum clients.

Features of Parity

- Clean, modular codebase for easy customization
- Minimal memory and storage footprint
- Synchronize the updated Blockchain in a few hours as compared to a few days in other clients

Connecting to Ethereum Using Parity

Parity client allows us to connect to the Ethereum mainnet, Ropsten, and Kovan network.

Command to connect to the Main network

```
parity --chain=mainnet
```

Command to connect to the Ropsten network

```
parity --chain=ropsten
```

Command to connect to the Kovan network

```
parity --chain=kovan
```

Parity Data Storage

Parity is a lightweight Ethereum client that helps connect to the peers and synchronize the latest Blockchain data into the local machine. It stores the Blockchain data into the following folders:

Linux ~/home/you/.local/share/io.parity.ethereum

~/AppData/Local/Parity/Ethereum **Windows**

Mac ~/Library/Application Support/io.parity.ethereum

Key Takeaways

- Ethereum is a decentralized platform that has its own cryptocurrency called Ether and also introduces smart contracts.
- Ethereum runs on an EVM, and a certain transaction fee called Gas must be paid to conduct Ether transactions.
- Ethereum wallets help in storing and transferring Ethers.
- Ethereum clients are software that connect to the Ethereum network and perform the functions of a full/light node.

Ether Transaction in Metamask

You have been asked to transfer 2 Ethers from one Metamask account to another. Perform the following steps:

1. Installing Metamask and creating a wallet
2. Installing Ganache and configuring a private Blockchain
3. Connecting the Metamask account to Ganache or a test faucet to obtain Ethers
4. Performing an Ether transaction from one Metamask account to another

LESSON-END PROJECT