Introduction to Ethereum

Definition

Ethereum is a decentralized, open-source blockchain with **smart contract** functionality.

A **smart contract** is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code controls the execution, and transactions are trackable and irreversible. Vending machines are mentioned as the oldest piece of technology equivalent to smart contract implementation.

Ether (ETH) is the native cryptocurrency of Ethereum. The purpose of ether is to allow for a market for computation. Such a market provides an economic incentive for participants to verify and execute **transaction requests** and provide computational resources to the network.

The **Ethereum Virtual Machine (EVM)** is the runtime environment for transaction execution in Ethereum. The EVM is **isolated** from the other files and processes on the node's computer to ensure that for a **given pre-transaction state and transactio**n, every node produces **the same post-transaction state**, thereby enabling network **consensus**.

Gas is a unit of account **within the EVM** used in the **calculation of a transaction fee**, which is the amount of ETH a transaction's **sender** must **pay to the miner** who includes the transaction in the blockchain. When creating a transaction, the sender must specify a gas limit and gas price. The **gas limit** is the maximum amount of gas the sender is willing to use in the transaction, and the **gas price** is the amount of ETH the sender wishes to pay to the miner per unit of gas used.

Consensus Mechanism

Consensus mechanisms allow distributed systems (networks of computers) to work together and stay secure. A consensus mechanism allows a cryptoeconomic system to agree on the state of the network, and helps prevent certain kinds of economic attacks. In theory, an attacker can compromise consensus by controlling **51%** of the network. Consensus mechanisms are designed to make this "**51% attack**" unfeasible.

Ethereum, like Bitcoin, currently uses a **proof-of-work (PoW)** consensus protocol. Proof-of-work is done by miners, who compete to create new blocks full of processed transactions. The winner shares the new block with the rest of the network and earns some freshly minted ETH. The race is won by whosever computer can solve a math puzzle fastest – this produces the cryptographic link between the current block and the block that went before. Solving this puzzle is the work in "proof-of-work". The network is kept **secure** by the fact that you'd need 51% of the **network's computing power** to defraud the chain. This would require such huge investments in equipment and energy; you're likely to spend more than you'd gain.

Proof-of-stake is done by **validators** who have **staked ETH** to participate in the system. A validator is **chosen at random** to create new blocks, share them with the network and earn rewards. Instead of needing to do intense computational work, you simply need to have staked your ETH in the network. This is what incentivises healthy network behavior. A proof-of-stake system is kept **secure** by the fact that you'd need 51% of the **total staked ETH** to defraud the chain. And that your stake is slashed for malicious behavior.

Ethereum 2.0 / Eth2

Open-source development is currently underway for a major **upgrade** to Ethereum known as Ethereum 2.0 or Eth2. The main purpose of the upgrade is to increase **transaction throughput** for the network from the current of about **15? transactions** per second to up to **tens of thousands of transactions** per second.

The stated goal is to increase throughput by splitting up the workload into many blockchains running in parallel (referred to as **sharding**) and then having them all share a common consensus **proof-of-stake** blockchain, so that to maliciously tamper with any singular chain would require one to **tamper** with the **common consensus**, which would **cost** the attacker far more than they could ever gain from an attack.

Applications

Non-fungible tokens (NFTs)

Ethereum allows for the creation of **unique** and **indivisible** tokens, called non-fungible tokens (NFTs)

A non-fungible token (NFT) is a **non-interchangeable** unit of data stored on a blockchain, that can be sold and traded.
Types of NFT data units may be associated with digital files such as photos, videos, and audio. Because each token is uniquely **identifiable**, NFTs differ from blockchain cryptocurrencies, such as Bitcoin.

Decentralized finance (DeFi)

It offers traditional **financial instruments** in a decentralized architecture, outside of companies' and governments' control, such as money market funds which let users earn interest.

*References

https://en.wikipedia.org/wiki/Ethereum
https://en.wikipedia.org/wiki/Smart_contract
https://www.investopedia.com/terms/s/smart-contracts.asp
https://ethereum.org/en/developers/docs/intro-to-ethereum/
https://ethereum.org/en/developers/docs/consensus-mechanisms/