Ethereum Blockchain: Genesis & Motivation

Table of Content

Introduction

Although the Bitcoin network provided a base for a medium of exchange, a 19-year-old programmer saw it as a method capable of challenging centralized entities across the economy. Further, unable to convince the Bitcoin community of the need for a scripting language, Vitalik and a like-minded group of people created Ethereum. The main motivation behind Ethereum was to support building decentralized applications on the powerful medium of blockchain

Vitalik Buterin published the Ethereum whitepaper in 2013, in which he introduced a novel, general-purpose blockchain network with a built-in Turing-complete language, which is a programming language that can be used to embed logic and complete more advanced transactions than simple payments. The introduction of this language has allowed developers to create and integrate applications into Ethereum, serving as the base layer of an open ecosystem capable of hosting smart contracts and decentralized applications (DApps). In reality, Buterin created a system of programmable money that revolutionized how people think about, create, and deploy blockchain technology.

Ethereum was initially released in 2015. Within two years of its release, it was ranked the second best blockchain network, after Bitcoin. The Ethereum network attained more global interest when China stated that it is the best blockchain network ever created.

What is Ethereum?

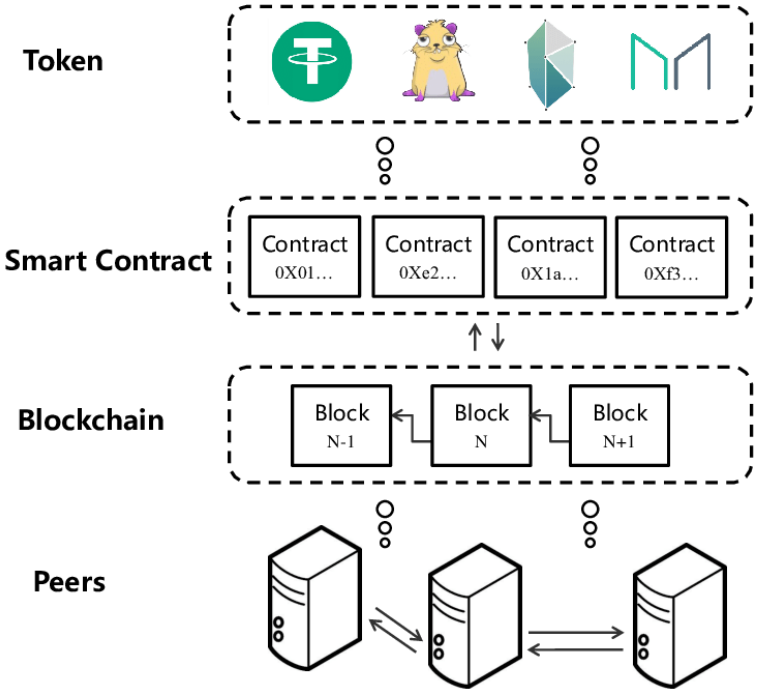
Ethereum is a decentralized blockchain platform that allows users to create and execute smart contract and decentralized applications (dApps). It helps ensure transparency and security through cryptographic techniques. Thus, Ethereum is a one-of-its-kind programmable blockchain rather than a cryptocurrency focused on payments. The platform utilizes a cryptocurrency called Ether (ETH) as its native currency. So, like Bitcoin, the Ethereum architecture also has two aspects:

- The cryptocurrency

- The Ethereum blockchain.

The official website's definition of Ethereum is as follows: "Ethereum is a global, open-source platform for decentralized applications. On Ethereum, one can write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world".

One significant contribution of Ethereum is that it liberated the blockchain technology from the financial limits of Bitcoin and expanded its scope. It showed the world how other industries could benefit from its application.



Ethereum's vision is to build a 'new internet.' One that would be decentralized as it was always meant to be. An internet in which,

- Peer-to-peer networks would replace the client-server model.
- Any data would be owned only by its creator.
- There would be no monopoly of data.
- Applications won't steal data in the name of 'tailor-made' services.

Key Characteristics of Ethereum

Ethereum offers several key characteristics that set it apart from other blockchain platforms:

Turing-Completeness

- Ethereum's programming language, Solidity, allows developers to create complex and versatile smart contracts. This feature gives Ethereum the ability to handle a wide range of computational tasks, making it highly flexible.

Decentralization

- Decentralization lies at the heart of Ethereum. It operates on a global network of computers called nodes, which collectively maintain the blockchain and validate

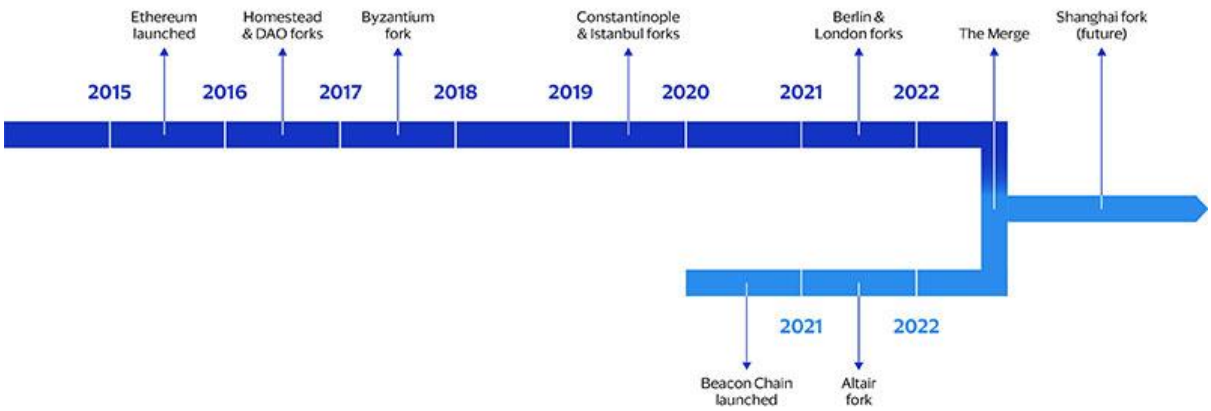
transactions. This decentralized architecture ensures the security and immutability of the platform.

Interoperability

- The Ethereum blockchain's design allows it to interact with other blockchains and platforms through various protocols and standards. This interoperability facilitates cross-chain operations and the integration of its assets into other blockchain ecosystems. Thus Ethereum provides a standardized framework for DApps to interact with each other. This interoperability fosters collaboration and enhances the overall functionality of the ecosystem.

Ethereum's Development Timeline

Unlike Bitcoin, the founders of Ethereum did not hide their identities. This makes tracing the origins of the Ethereum blockchain more straightforward than recording BTC's history.



2013-2014: Ethereum's creation

According to the Ethereum Foundation's official timeline, Ethereum's history began in 2013 when computer scientist Vitalik Buterin published his Ethereum Whitepaper. In this document, Buterin outlined many innovations that would set Ethereum apart from other cryptocurrencies and explained how Ethereum would let developers use blockchain tools such as smart contracts to build dApps (decentralized applications). The introduction of self-executing smart contract code helped expand the possibilities for blockchain technology. Instead of solely using blockchain to record financial transactions, Ethereum set out to decentralize the internet.

Before working on Ethereum, Buterin had already been a significant figure in the early crypto space. For instance, he co-founded Bitcoin Magazine and wrote multiple research papers on new crypto technologies, such as coloured coins.

Because Buterin wrote the Ethereum Whitepaper, he's often credited as the developer who founded Ethereum. However, there were many other computer scientists involved. Famously, Dr. Gavin Wood helped create Ethereum's Solidity coding language. Charles Hoskinson was also a key influence in Ethereum's early development. Today, Wood and Hoskinson run the competing Ethereum projects Polkadot and Cardano, respectively.

To turn the Ethereum Whitepaper into a reality, Buterin explained his vision for a new blockchain at 2014's North American Bitcoin Conference. The Ethereum team offered an ICO (initial coin offering) for ETH to early investors later that year. At the time, estimates suggest the Ethereum Foundation raised about $18 million in BTC.

2015: Ethereum goes live

The Ethereum blockchain launched in July 2015 under the codename "Frontier." This was one of the pivotal moments in Ethereum's history, the creation of its Genesis Block, which marked the beginning of a decentralized world of smart contracts and decentralized applications (DApps). The Genesis Block is the foundational block of the Ethereum blockchain, serving as the starting point from which all subsequent blocks are built. It is the birthplace of the entire Ethereum network and holds a particular symbolic value as the genesis of a new era in blockchain technology. Within this first block lies the essential data that sets the initial state of the entire Ethereum ecosystem. It includes the initial distribution of Ether (ETH), the native cryptocurrency of Ethereum, and sets the rules and parameters that govern the functioning of the blockchain. As a result, the Genesis Block serves as a crucial reference point for the continued evolution and growth of the Ethereum network.

Vitalik Buterin and the core development team and early contributors meticulously prepared for the launch. They performed rigorous testing, audited the code, and addressed any last-minute concerns to ensure a smooth and secure launch.

With the Genesis Block launch began a remarkable journey for Ethereum. It showcased the power of collaboration, vision, and community support in transforming a groundbreaking idea into a tangible and thriving blockchain platform.

This first iteration of Ethereum used the same proof-of-work (PoW) consensus mechanism on the Bitcoin network. In this system, computers have to solve complex algorithmic problems to post new transactions on the blockchain. Whichever computer solves this puzzle first receives crypto rewards in the form of ETH.

Although Ethereum's consensus mechanism was the same as Bitcoin's, there's no maximum cap supply on ETH coins. Until the 2022 Ethereum Merge, ETH was an inflationary cryptocurrency. Buterin set the initial block reward for mining Ethereum at five ETH per block.

Also, Ethereum miners didn't need to use the large ASIC rigs that were commonly used to mine coins such as Bitcoin and Litecoin. Throughout its early history, Ethereum miners used computers with graphics processing units (GPUs).

2016: The 'DAO Hack' explained

Just one year after its launch, the Ethereum community faced a major controversy called the "DAO hack." In crypto, DAO, short for decentralized autonomous organization, refers to a community-driven open-source protocol. From voting to executing orders, all actions in a DAO

use autonomous smart contracts. The DAO at the heart of the 2016 hack was a specific smart contract protocol on Ethereum that raised $150 million in ETH. Everyone who had a stake in this DAO could have a say in how to use the crypto treasury. However, hackers noticed a few bugs in the DAO's code and stole roughly $50 million worth of ETH.

After news of the DAO hack broke, the Ethereum community split into two camps. The first group of developers wanted to create a new Ethereum chain to reimburse DAO investors. The second group argued that any outside influence on the Ethereum blockchain would go against the decentralized nature of cryptocurrency. Those who favoured this second "code is law" approach said it would be best to leave the Ethereum chain as is.

Eventually, most of Ethereum's developers created an offshoot chain (aka a fork) to erase the DAO hack. This new project became today's mainstream Ethereum chain. However, the original "hacked" Ethereum Classic chain is still operational.

2017-2021: Major upgrades before 'the Merge'

Following the DAO hack, Ethereum introduced new governance proposals and upgrades to its blockchain. For instance, the Byzantium Fork of 2017 reduced the block reward from five ETH to three ETH. This upgrade introduced new technology that made it easier for blockchains to build on top of Ethereum. These layer-2 blockchains (e.g., Polygon) have become an increasingly significant aspect of the Ethereum ecosystem.

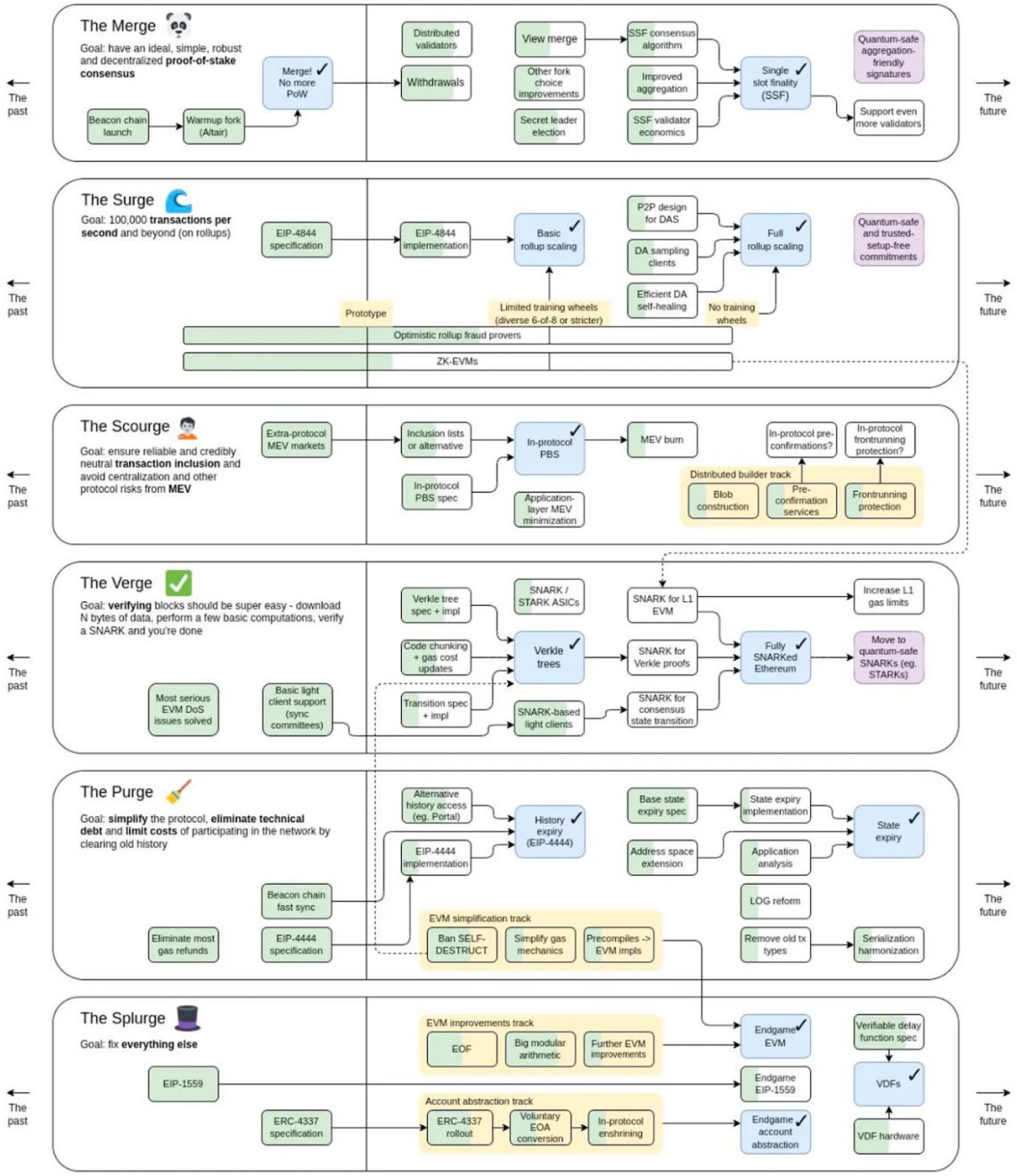
Ethereum NFTs (non-fungible tokens) also made headlines in 2017. Thanks to the NFT game CryptoKitties, activity on the Ethereum blockchain hit record highs. The trading volume for CryptoKitties was so high that the game's developers decided to create their own "Flow" blockchain. The 2017 CryptoKitties craze highlighted the growing interest in NFTs and Ethereum's speed and scalability concerns.

The 2019 upgrades, Istanbul and Constantinople, focused on optimizing Ethereum's gas fee structure and introducing further scalability solutions. In addition to launching new solutions for layer-2 blockchains, the Constantinople upgrade paved the way for a smooth transition to the proof-of-stake (PoS) consensus mechanism. Unlike PoW, PoS requires validators to lock (or "stake") a native cryptocurrency on the blockchain. Anyone who stakes their crypto can confirm new blocks and claim crypto rewards. Buterin believed moving Ethereum to a PoS consensus would benefit the blockchain in many ways. Not only could PoS potentially lead to scalability upgrades, but it would also significantly reduce Ethereum's carbon footprint.

At the end of 2020, Ethereum introduced a PoS blockchain called the "Beacon Chain." Eventually, the Beacon Chain replaced Ethereum's PoW blockchain in an event called the Merge. Before this transition, anyone with 32 ETH could lock it on the Beacon Chain to start earning staking rewards. The Ethereum Foundation won't release any funds locked on the Beacon Chain's smart contract until it launches the Shanghai upgrade.

2022: Introduction of Ethereum 2.0

Vitalik Buterin has outlined the following roadmap for Ethereum 2.0:



The Ethereum 2.0 Roadmap

After countless tests and years of anticipation, the Ethereum team announced it would "merge" the PoW blockchain into the Beacon Chain in 2022. On September 15, 2022 at 6:43 AM UTC, Ethereum successfully transitioned to a PoS blockchain. Although the Merge was one of the most significant upgrades in crypto history, it didn't directly impact Ethereum's transaction speeds or fees. Instead, the PoS consensus laid the groundwork for further upgrades that could make Ethereum faster and cheaper. The most immediate effect of the Merge was a reduction in Ethereum's carbon footprint. Since there's no more need for GPU miners, Ethereum cut its electricity and net emissions by an estimated 99.95%. Thanks to Ethereum's PoS consensus, it went from being one of the biggest polluters to an eco-friendly blockchain.

The Merge also changed Ethereum's daily issuance. The Ethereum Foundation claimed approximately 1,700 ETH would enter circulation each day post-Merge. In contrast, Ethereum had a daily issuance rate of 13,000 ETH per day on the PoW network.

Another improvement brought by Ethereum 2.0 is the introduction of Sharding. Sharding will divide the Ethereum database amongst its network. This idea is similar to cloud computing, where many computers handle the workload to reduce computational time. These smaller database sections will be called shards, and shards will be worked on by those who have staked ETH. Shards will allow more validators to work at the same time, reducing the amount of time needed to reach consensus through a process called sharding consensus. Sharding is expected to be implemented sometime in 2023.

Despite the flawless implementation of the Merge, Chinese miner Chandler Guo favored miners and forked the Ethereum blockchain to preserve the PoW consensus method. This new fork is called ETHW or proof-of-work Ethereum, in which miners will continue to solve complex mathematical puzzles to receive ETH rewards (similar to Ethereum Classic).

Besides the Merge, Ethereum made headlines in traditional finance in 2022. In a press release, the Chicago Mercantile Exchange (CME Group) announced it would offer Ethereum futures trading. In 2017, the CME Group first introduced Bitcoin futures trading to derivatives investors. The launch of Ethereum derivatives gave more institutional investors access to ETH's price action.

Ethereum's future after the Merge

Ethereum is a significant player in the crypto space, as evidenced by its market capitalization and the vast array of solutions that entities have built on the Ethereum blockchain. However, the network has faced difficulty in scaling. Its transition over to the consensus layer aims to solve its challenges. However, only time will tell regarding the results.

Buterin outlined four critical stages in Ethereum's post-Merge development. While there are few concrete details on these upgrades, they serve as a blueprint for Ethereum's future.

The Surge: Next phase of the roadmap, "The Surge" likely to be introduced next year will begin incorporating a new technology called "sharding" into the Ethereum blockchain. "Shards" help offload data from the main Ethereum chain, which may improve transaction speeds and network efficiency.

The Verge: This stage is named after a new cryptographic technology called "verkle trees." Buterin believes this revolutionary infrastructure could help with Ethereum's data storage issues and increase the number of network validators.

The Purge: After introducing sharding and verkle trees, Ethereum will begin "purging" any unnecessary data clogging the network. By this time, Ethereum may reach a speed of 100,000 transactions per second (TPS).

The Splurge: Since the Splurge is so far off, Buterin has only vaguely hinted at what this term means. However, most assume Buterin may be referring to a "splurge" of new innovative applications building in Ethereum's ecosystem (e.g., NFT markets, play-to-earn games, and DeFi protocols). Nonetheless, it remains to be seen if upcoming updates would enable

Ethereum to more effectively manage a wave of arising regulatory issues over digital assets and public blockchains.

In short, Ethereum's journey from a whitepaper to a thriving blockchain platform has been nothing short of remarkable. It has reshaped general understanding of blockchain technology and opened doors to new possibilities in the decentralized world. As Ethereum continues to evolve and adapt, it remains at the forefront of innovation, inspiring countless developers and entrepreneurs to build a decentralized future.

What are Ethereum Transactions?

Transactions in Ethereum are cryptographically signed data messages that contain a set of instructions. These instructions can interpret to sending Ether from one Ethereum account to another or interacting with a smart contract deployed on the blockchain. Transactions are a simple but powerful concept that has allowed users worldwide to interact on a decentralized network.

A transaction usually consists of the following parameters: [nonce, gasPrice, gasLimit, to, value, data, v, r, s]. However, Ethereum has evolved to allow other transaction standards such as EIP-1559. The EIP-1559 transaction standard came from an improvement proposal to allow more predictable gas fees and a more efficient transaction market. transactions derive from Externally owned accounts (EOA) or Smart contract accounts. Ethereum utilizies the elliptic curve digital signature algorithm (ECDSA) to prove authentication (i.e., prove that we have a private key for our public address) and verify that our transaction comes from the account signing the transaction and is not fraudulent.

Transaction States

Pending: Transactions broadcasted to the network waiting to be mined. If the transaction is taking longer than expected, it's possible that your gas fee is not high enough to meet execution at the current time.

Queued: A transaction that cannot be mined yet due to another pending transaction in the queue first or an out of sequence nonce.

Cancelled: Can no longer be mined. Replaced by a transaction with a higher gas fee, same nonce value, and a null value for the data and/or value field.

Replaced: Can no longer be mined. Used to replace current pending orders for faster execution or modification of values and data. This also consists of using the same nonce as the transaction you want to cancel and a higher gas fee.

Failed: A transaction that resulted in an error due to a revert error, bad instructions, illogical code, or not enough gas to run the remainder of a function call.

Transaction Architecture

The transaction format for Ethereum was originally one standard but has evolved over time to allow other transaction formats. The set of instructions in a transaction object looks like this:

from - the sending address.

to – the receiving address (if EOA, the transaction will transfer value. If a smart contract account, the transaction will use contract code).

value – the amount of ETH to be sent from the sending address (denominated in Wei)

data – can contain code or a message to the recipient.

gasLimit – the maximum amount of gas units that can be used.

nonce - a number used to track ordering of transactions and prevent replay attacks

maxPriorityFeePerGas - the maximum amount of gas to be included as a tip to the miner.

maxFeePerGas - the maximum amount of gas willing to be paid for the transaction (including baseFeePerGas and maxPriorityFeePerGas).

signature – derived from the sending account's private key and is created when the sender signs the transaction.

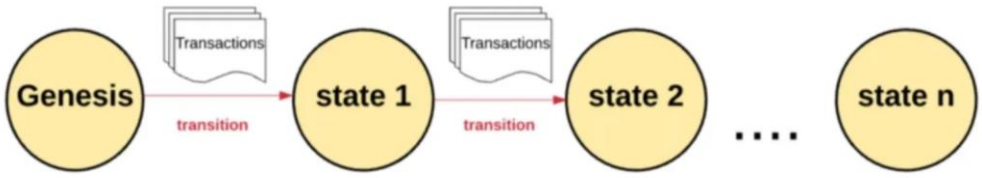
Transaction Lifecycle

The transaction lifecycle can be simplified to:

1. An external account creates a transaction object.
2. The account sending the transaction verifies it by signing which creates a transaction hash
3. The transaction is broadcasted across the network using an Ethereum node
4. The transaction execution is idle until the transaction is mined and added to the block or replaced/cancelled.

How does Ethereum work?

Ethereum can be described as a blockchain-based network operating as a “state machine.”



Ethereum as a State Machine

The official Ethereum documentation defines Ethereum in the following way:

“Instead of a distributed ledger, Ethereum is a distributed state machine. Ethereum’s state is a large data structure which holds not only all accounts and balances, but a machine state, which can change from block to block according to a pre-defined set of rules, and which can execute arbitrary machine code. The specific rules of changing state from block to block are defined by the EVM.”

In other words, we can define Ethereum as follows:

- Ethereum is not just a distributed ledger (Bitcoin). It is a distributed state machine.

- State is a large data structure that can contain not only an account balance, but also a variety of other information represented by a computer.
- It is the predefined rules and executable code that change the state of Ethereum, and the user's commands to execute them are contained in blocks in the form of 'transactions'.

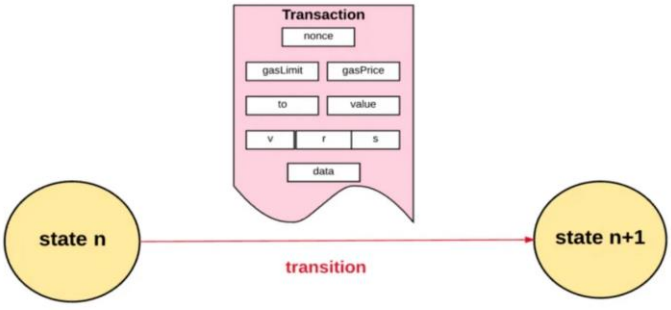
To simplify things a bit more, Ethereum is a decentralized database with various "states," or the rules and code used to change these states are the smart contracts, and the user's instructions to execute the smart contracts to change the state of Ethereum are the "transactions."

There are users who want to use the Ethereum network. As mentioned earlier, using the Ethereum network means changing the "state" of Ethereum, which means changing the balance of a particular token, changing the level of a game character, or anything else in the state information recorded on Ethereum.

In Ethereum, when a node receives a transaction, it does not execute it immediately, but instead sends it to a waiting room called the mempool. This is because the Ethereum blockchain, is made up of many anonymous nodes, and no single node should be able to process a request at will. Transactions not yet included in a block will stay in the mempool as pending. Ethereum nodes need to reach a "consensus" on who should process the transactions they receive from users, in what order, and when, or Ethereum will split into countless branches every minute.

The nodes participating in Ethereum reach a consensus to establish a unified "Ethereum." The newly created block is then propagated to other validator nodes, who rerun the transactions in the block and validate the data signatures. If they find it valid, they submit a vote to the Ethereum network to attest to the block. Based on these blocks and attestations, the network builds a consensus to continue the chain.

The instruction or the transaction that you sent to Ethereum to change the state of an account is now in a block and officially part of the network. The instruction in the transaction will either change the balance or, through the smart contract code, change the state of the Ethereum network. This process is called "execution."



Ethereum state transition through a transaction

So, who changes the state of Ethereum? The Ethereum Virtual Machine (EVM) is actually responsible for processing transactions. The EVM is a Turing-complete virtual machine, which means it can compute code at the same level as a regular computer — it's a giant "world computer" with distributed nodes behaving identically. Transactions in Ethereum's blocks contain more than just requests to send tokens — they also contain requests to execute smart

contract code. Smart contracts are code that contains business logic to change state, so executing them means changing the state of Ethereum.

Ethereum nodes execute the instructions (transactions) contained in the blocks in an ordered sequence through the EVM, the world computer, and change the state of the Global state.

In this way, Ethereum has implemented various features to make the blockchain work as a world computer beyond a distributed ledger.

Ethereum consists of several key components, namely:

- Smart contracts: Rules governing under what conditions money can change hands
- The Ethereum blockchain: A record of Ethereum's entire history – every transaction and smart contract call is stored in its blockchain
- Consensus mechanism: The method for validating and recording data on the blockchain; it also helps to secure the network and is responsible for issuing new tokens into circulation
- The Ethereum Virtual Machine (EVM): The part of Ethereum that executes the rules of Ethereum and makes sure a submitted transaction or smart contract follows the rules
- Ether: Ethereum's token, which is required to make transactions and execute smart contracts on Ethereum
- Decentralized applications (Daaps): Dapp has its backend code running on a decentralized peer-to-peer network. It can have a frontend and user interface written in any language to make calls and query data from its backend. They operate on Ethereum and perform the same function irrespective of the environment in which they get executed.
- Decentralized autonomous organizations (DAOs): It is a decentralized organization that works in a democratic and decentralized fashion. DAO relies on smart contracts for decision-making or decentralized voting systems within the organization.

Smart contracts

A smart contract is simply a programmable agreement that runs on a blockchain. This technology allows users to digitize conditions governing the relationship and interactions between the two parties involved in a transaction. Once these conditions are programmed and launched on the blockchain as smart contracts, they self-execute (that is, they initiate and complete the set of transactions that they govern, as long as the predefined conditions are met). The smart contract's primary feature is that once it is executed, it cannot be altered, and any transaction done on top of a smart contract is registered permanently—it is immutable.

For instance, Alice decides to borrow from Bob 1,000 tether (USDT) only if Bob deposits ether worth $2,000 as collateral. Using a smart contract, Alice could independently define the conditions that validate this deal, instead of trusting a middleman that would broker the deal. If done right, such a smart contract would autonomously release 1,000 USDT to Bob after he had deposited and locked $2,000 as collateral. Also, when Alice repays the loan, the smart contract would release the collateral and send it back to Bob.

As such, the smart contract offers a trustless system where Alice or Bob do not need to worry about counterparty risks. It also eliminates the need for middlemen. Here, Alice and Bob do not need to pay an extra fee to an intermediary or escrow service before they can conduct peer-to-peer transactions.

Interestingly, Ethereum was the first blockchain to discover and implement smart contracts as part of the functionalities of blockchains. Subsequently, this innovation unlocked more blockchain use cases and ultimately brought about the explosion of decentralized applications.

Anyone on the Ethereum network can create these contracts. The contract consists primarily of the terms and conditions mutually agreed on between the parties (peers).

Blockchain

Ethereum shares some similarities with Bitcoin in that it relies on a blockchain to store and secure transactions. A blockchain is a chain of chronologically ordered blocks containing the data of confirmed transactions. Think of it as a ledger where all the activities executed in a network or platform are being recorded. Importantly, this ledger is publicly available, meaning network participants and even outsiders can easily track its content. Also, copies of this ledger are distributed across a global network of computers known as “nodes.” These nodes perform a variety of tasks on the network, including verifying and recording transaction and smart contract data.

This architecture allows participants to own a copy of the blockchain and collectively verify the validity of the content added to it. Some of the benefits of this include:

- No single point of failure
- Data is completely transparent, reliable and immutable
- Censorship resistant

However, where Ethereum is different to Bitcoin is that nodes just do not have to verify and record transaction data, they also have to keep track of the network’s “state.” Ethereum’s state is the current information of all the applications running on top of it, including each user’s balance, all the smart contract code, where it is all stored and any changes that are made.

Here’s a summary of what’s stored in each node:

- Accounts: Each user can have an account, which shows how much ether the user has
- Smart contract code: Ethereum stores smart contracts, which describe the rules that need to be met for money to be unlocked and transferred
- Smart contract state: The state of the smart contracts

Consensus mechanism

Ethereum and Bitcoin used to use the same consensus protocol for validating data and adding it to the blockchain – known as proof-of-work (PoW). This involves mining nodes competing against one another using energy-intensive machines to win the right to add the next block to the blockchain. This happens roughly once every 10 minutes.

However, in 2022, Ethereum underwent a major transition known as "The Merge" which migrated the network to a proof-of-stake blockchain (PoS.) Instead of requiring mining nodes to run expensive equipment to discover new blocks, the new PoS system requires users to

deposit and lock away 32 ether – the native cryptocurrency of Ethereum (see below) – to become network validators.

There are three main benefits to the transition:

- Ethereum's new PoS blockchain supports the implementation of new "shard chains." These will be 64 smaller blockchains that will each handle their own batches of data, allowing for Ethereum to process significantly more transactions per second.
- The new Ethereum blockchain uses 99.95% less energy than the proof-of-work version.
- Because validators will not need to purchase and operate expensive mining equipment, it will reduce the barrier for entry for people to participate in the network. This should help to improve overall decentralization and network security.

The Ethereum Virtual Machine (EVM)

The EVM is Ethereum's native processing system that allows developers to create smart contracts and lets nodes seamlessly interact with them. Ethereum developers write smart contracts with Solidity, a programming language much like Javascript and C++. These smart contracts written in Solidity can be read by humans but not computers. It, therefore, has to be converted into low-level machine instructions – called opcodes – which the EVM can easily understand and execute.

It is important to know every Ethereum node has its own EVM. When a person sends a transaction to a smart contract deployed on Ethereum, every node runs the smart contract and the transaction through their own EVM. In this simulated environment, each node can see what the end result will be and whether the outcome produces a valid transaction or not. If all nodes reach the same valid outcome, the changes are made and the updated Ethereum state is recorded on the blockchain.

Ether

Ethereum's token Ether, serves multiple purposes. It acts as a digital currency for transactions on the network, provides security through staking in Ethereum 2.0, and serves as an incentive for miners and validators. So it is needed for doing just about anything on Ethereum. When it is used to execute smart contacts on the network it is often referred to as "gas." The amount of gas needed to pay is determined by the type of transaction someone plan on executing and the number of Ethereum transactions waiting to be verified. The more complex the transaction, the higher the gas fee.

Ethereum uses accounts to store the ether, analogous to bank accounts. Accounts on the Ethereum network differ from traditional accounts. These accounts can be created by anyone. Accounts can be user-controlled or deployed as smart contracts. Their main purpose is to hold the Ether and send transactions. Ethereum has two types of accounts: An externally owned account (EOA), and a Contract account. These are explained as following below:

Externally owned account (EOA): The accounts that normal users use for holding and sending ether. Externally owned accounts are controlled by private keys. Each EOA has a public-private key pair. The users can send messages by creating and signing transactions.

Contract Account: These separate accounts are the ones that hold smart contracts, which can be triggered by ether transactions from EOAs or other events. Contract accounts are controlled

by contract codes. These codes are stored with the account. Each contract account has an ether balance associated with it. The contract code of these accounts gets activated every time a transaction from an EOA or a message from another contract is received by it. When the contract code activates, it allows to read/write the message to the local storage, send messages and create contracts.

Architecture of an account

Regardless of whether considering an externally owned account (a user account controlled by a private key) or a contract account (an account controlled by code), each Ethereum account has a basic state that always comprises the following four elements:

- Firstly, there is the **nonce**. In the case of externally owned accounts, nonces represent the number of transactions sent from the account's address. For contract accounts, the nonce is the number of contracts created by the account.
- Then there is **balance**, which refers to the amount of wei owned by the account address. There are 10^18 wei per one unit of ether.
- The third constituent is the so-called **storageRoot**, which is a 256-bit hash that encodes the account's stored contents.
- The last part is the **codeHash**, which is the hash of the account's EVM code. Since hashing is deterministic, the codeHash is immutable and cannot be altered after generation. When it comes to externally owned accounts, which contain no smart contract code, an empty string is hashed to create the codeHash.

Decentralized Autonomous Organizations (DAOs)

A DAO is a digital organization that operates without hierarchical management; it works in a decentralized and democratic fashion. So basically, a DAO is an organization in which the decision-making is not in the hands of a centralized authority but preferably in the hands of certain designated authorities or a group or designated people as a part of an authority. It exists on a blockchain network, where it is governed by the protocols embedded in a smart contract, and thereby, DAOs rely on smart contracts for decision-making—or, we can say, decentralized voting systems—within the organization. So, before any organizational decision can be made, it must go through the voting system, which runs on a decentralized application.

Here is how it works. People add funds through the DAO because the DAO requires funding in order to execute and make decisions. Based on that, each member is given a token that represents that person's percentage of shares in the DAO. Those tokens are used to vote in the DAO, and the proposal status is decided based on the maximum votes. Every decision within the organization must go through this voting process.

Decentralized applications (DApps)

Decentralized applications, commonly known as DApps, are software applications that run on a decentralized network of computers, typically utilizing blockchain technology. Ethereum, with its robust smart contract functionality, stands out as a leading platform for Dapp development. Unlike traditional applications that are hosted on centralized servers controlled by a single entity, DApps operates on a peer-to-peer network, distributing both data and processing power across a network of nodes.

Anyone with the right knowledge can theoretically build a dApp or web service on the network. As a result, since launching in 2015, Ethereum has become the unifying ecosystem for thousands of unique organizations. Roughly half of all functioning dApps in the market are based on the Ethereum network. Ethereum's DApps range widely, from decentralized credit services and financial exchanges to blockchain-enabled web browsers and data markets.

Since the advent of Ethereum, a number of other blockchain projects focused on smart contract-deployed DApps have sprung up. However, Ethereum continues to be the most widely adopted platform of its kind. And as today, the Ethereum blockchain remains the second largest, in large part because of the project's success in attracting developers to build dApps on its network.

An Ethereum DApp is a web app with specific features. These features are as follows:

- Ethereum DApp projects are based on open-source software.
- One can code the front-end in any language. However, the backend of DApp for the platform he or she use must have smart contracts coded in the relevant language.
- One must run an Ethereum DApp on a decentralized Ethereum network.
- The user community of a DApp platform determines its future. One cannot modify a DApp without the consent of the user community. Smart Contracts, the most vital part of the Ethereum dApp development, are coded for implementing business logic & functionality in the dApp.
- Ethereum runs autonomous decentralized applications (DApps).
- An Ethereum DApp must store data in a decentralized Ethereum blockchain. It must adhere to established cryptographic standards when storing data.
- A DApp must have a cryptographic token. One need to create this crypto token following the established cryptographic algorithm.

Applications of Ethereum

Real-World Applications of Ethereum

- **Voting:** Voting systems are adopting Ethereum. The results of polls are available publicly, ensuring a transparent fair system thus eliminating voting malpractices.
- **Agreements:** With Ethereum smart contracts, agreements and contracts can be maintained and executed without any alteration. So, in an industry that has fragmented participants, is subject to disputes, and requires digital contracts to be present, Ethereum can be used as a technology for developing smart contracts and for digitally recording the agreements and the transactions based on them.
- **Banking systems:** Ethereum is getting adopted widely in banking systems because with Ethereum's decentralized system; it is challenging for hackers to gain unauthorized access to the network. It also allows payments on an Ethereum-based network, so banks are also using Ethereum as a channel to make remittances and payments.
- **Shipping:** Deploying Ethereum in shipping helps with the tracking of cargo and prevents goods from being misplaced or counterfeited. Ethereum provides the provenance and tracking framework for any asset required in a typical supply chain.
- **Crowdfunding:** Applying Ethereum smart contracts to blockchain-based crowdfunding platforms helps to increase trust and information symmetry. It creates many possibilities for startups by raising funds to create their own digital cryptocurrency.

- **Domain names:** Ethereum name service allows crypto users to buy and manage their own domain names on Ethereum, thus simplifying decentralized transactions without putting users to remember long, machine-readable addresses.
- **Prediction market:** The prediction market is another wonderful use case of Ethereum Smart Contract. The platforms like Gnosis and Augur use Ethereum for this purpose.
- **Digital Identity Management:** Digital identities can be managed by using smart contracts which solve the major issues of identity theft and data monopoly.
- **NFTs:** It is the primary platform for NFTs, representing ownership of unique digital assets like digital art, collectibles, and virtual real estate. This platform facilitates the creation, trading, and ownership of NFTs.
- **Decentralised Exchanges (DEXs):** The blockchain hosts Decentralised Exchanges (DEXs), which allow users to swap cryptocurrencies directly without relying on centralized exchanges.
- **Tokenization:** This platform enables tokenizing real-world assets, including real estate, stocks, and commodities. These tokens provide fractional ownership and increase liquidity in traditionally illiquid markets.
- **DApps**: DApps based on this platform help enhance supply chain transparency, traceability, and authenticity verification for products and goods. Moreover, it supports blockchain-based gaming and virtual worlds, allowing users to own, trade, and use in-game assets.
- **Healthcare:** This blockchain's dApps aims to improve patient data management and access while maintaining privacy and security.

Ethereum has not only transformed the blockchain world but has also helped the evolution of many other industries. Few Examples:

- Santander Bank, in collaboration with ConsenSys, has developed a cash tokenization utility system. It enables the user to make domestic or international within seconds using the Ethereum platform.
- uPort is building a universal ID which could be used to log into various platforms. The ID would be an address on Ethereum.
- GridPlus is using Ethereum to digitize the power grid to reduce the cost of electricity.

What are the Advantages of Ethereum?

Ethereum's most notable advantage is its pioneering role in introducing intelligent Smart Contracts to the blockchain world. This platform supports these smart contracts. Smart contracts on Ethereum establish clear, self-executing agreements, eliminating the need for interpretation and ensuring stronger contracts. These self-executing contracts enable the automation of various processes and agreements without intermediaries. This innovation has opened doors to various industries, including finance, supply chain, gaming, and healthcare.

The advantages of the Ethereum blockchain are:

- **Decentralisation:** The Ethereum network operates in a decentralised method across nodes located globally. This means no single entity or central authority controls the platform, making it resistant to censorship, manipulation, or single points of failure. Decentralisation enhances security and fosters trust among users, ensuring that transactions and data are recorded transparently and immutably on the blockchain.

- **Transparency and Security**: All transactions and Smart Contracts executed on Ethereum are recorded on a public ledger, providing unparalleled openness. This transparency lowers the chance of fraud and corruption, as anyone can verify the authenticity of transactions. Moreover, Ethereum's security features, such as cryptographic encryption and decentralised consensus mechanisms, make it highly resistant to attacks.
- **Flexibility and Customisation:** Ethereum's flexibility allows developers to create various decentralised applications and tokens to suit different use cases. Ethereum's programming language, Solidity, supports Turing-complete Smart Contracts, enabling the creation of complex and customisable applications. This adaptability has led to the emergence of various innovative projects, including Decentralised Finance (DeFi) platforms, Non-Fungible Token (NFT) marketplaces, and more.
- **Community and developer support:** Ethereum boasts a large and active community of developers, enthusiasts, and stakeholders deeply committed to its growth and improvement. This strong community support results in continuous development, research, and upgrades to address issues and enhance the platform's capabilities. Its ecosystem includes decentralized finance platforms, non-fungible token marketplaces, and more.
- **Ethereum's growing ecosystem:** Ethereum has fostered a thriving and rapidly expanding ecosystem. Its open-source nature has encouraged collaboration and innovation, resulting in many projects, protocols, and initiatives built on the platform. Ethereum-based tokens and DApps have gained widespread adoption, attracting users and investors. The network effect generated by this growing ecosystem reinforces Ethereum's position as a leader in the blockchain space.
- **Interoperability and standards:** Ethereum's adoption of common standards like ERC-20 (for fungible tokens) and ERC-721 (for non-fungible permits) has contributed significantly to the interoperability of blockchain assets. These standards have become widely accepted, facilitating the creation and exchange of tickets across different DApps and platforms. This has streamlined the development and integration of blockchain-based solutions.
- **Global Accessibility:** The Ethereum network is accessible to anyone with an internet connection, allowing for global participation. This opens up opportunities for individuals from all over the world to engage in economic activities and access financial services.
- **Economic incentives:** Ethereum's native cryptocurrency, Ether (ETH), is a fuel for executing Smart Contracts and a store of value. This financial incentive system encourages participants to secure the network, validate transactions, and develop DApps, creating a self-sustaining ecosystem.
- **Ethereum 2.0 transition:** Ethereum is actively addressing its scalability and energy consumption issues with Ethereum 2.0. This multi-phase upgrade involves transitioning from a Proof-of-Work (PoW) to a more energy-efficient Proof-of-Stake (PoS) consensus mechanism. It also includes shard chains to improve scalability. Once fully implemented, Ethereum 2.0 is expected to enhance the platform's performance and sustainability significantly.
- **Finality:** A blockchain’s consensus algorithm secures confidence that the record of transactions remains tamper-proof and canonical. Ethereum offers customizable

consensus mechanisms including RAFT and IBFT for different enterprise network instances, ensuring immediate transaction finality and reducing the required infrastructure that the Proof of Work algorithm demands.

- **Rapid deployment:** On Ethereum decentralized networks, enterprises can easily deploy and manage private blockchain networks instead of coding blockchain implementation from scratch.
- **Private transactions:** Enterprises can achieve granularity of privacy in Ethereum by forming private consortia with private transaction layers. On Ethereum, private information is never broadcast to network participants. Private data is encrypted and only shared directly with relevant parties.

What are the Disadvantages of Ethereum?

The disadvantages are as follows:

- **Scalability issues:** Ethereum has faced significant scalability challenges, especially with high network congestion. As the number of users and transactions on the network increases, it can lead to slower confirmation times and higher transaction fees. Swarm Scalability is an issue, so there is a trade-off with decentralization Private block chains are likely to proliferate.
- **Regulatory challenges:** As Ethereum and the broader cryptocurrency space continue to gain traction, they face increasing regulatory scrutiny from governments and financial authorities worldwide. Regulatory ambiguity can challenge Ethereum-based projects as they must navigate evolving compliance requirements and legal frameworks.
- **Security concerns:** While Ethereum is considered secure, Smart Contract vulnerabilities can lead to significant losses. Several high-profile hacks and exploits have occurred on Ethereum-based applications and Decentralised Finance (DeFi) platforms. Smart Contract security is a critical concern that requires ongoing attention and auditing.
- **Competition and network congestion:** Ethereum faces a rigid contest from other blockchain platforms that offer different features and scalability solutions. Venues like Binance Smart Chain, Solana, and Polkadot have gained popularity by addressing Ethereum's scalability issues. Network congestion during periods of high demand can lead to delays and higher transaction fees, discouraging users and developers.
- **Complexity of development:** Development on Ethereum can be complex and resource-intensive, particularly for newcomers. Innovative contract development requires expertise in Ethereum's architecture and programming language, Solidity. Auditing Smart Contracts for vulnerabilities is critical but challenging, requiring additional time and resources.
- **Bumpy Transition to Ethereum 2.0:** While Ethereum 2.0 promises solutions to scalability and energy consumption issues, its transition is a complex, multi-phase process that is still ongoing. Delays or unexpected challenges could impact the network's performance. There needs to be more certainty regarding the success of Ethereum 2.0 and how it will affect the existing ecosystem.

- **Expensive Storage and Bandwidth costs:** Developing and deploying a full Ethereum node can be resource-intensive regarding storage and bandwidth requirements. As the Ethereum blockchain grows, these costs may become prohibitive for some users and node operators.
- **Governance challenges:** Ethereum's governance model is evolving, and decisions regarding upgrades and changes to the network can be contentious. Disagreements among stakeholders have the potential to impact the platform's development and direction.
- **User Experience and accessibility:** Interacting with Ethereum and its DApps can be challenging for non-technical users. Managing private keys, understanding gas fees, and navigating decentralised applications can be intimidating for newcomers. Improving the User Experience remains a priority for Ethereum developers.
- **Extensive Ecosystem:** The Ethereum ecosystem is extensive. It can be challenging for its assets and applications to interact seamlessly with other blockchain platforms.

Ethereum vs. Bitcoin Blockchain network

Here is the main difference between Ethereum and Bitcoin Blockchain network:

Parameter	**Bitcoin**	**Ethereum**
Definition	Bitcoin (abbreviation: BTC; sign: ₿) is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network.	Ethereum is a decentralized global software platform powered by blockchain technology. It is most commonly known for its native cryptocurrency, ether (ETH).
Inception Year	Satoshi Nakamoto	Vitalik Buterin
History	The word bitcoin was defined in a white paper published on 31 October 2008. The currency began use in 2009.	Ethereum was conceived in 2013 by programmer Vitalik Buterin, and then went live on 30 July 2015.
Purpose	The purpose of bitcoin was to replace national currencies during the financial crisis of 2008.	The purpose of Ethereum was to utilize blockchain technology for maintaining a decentralized payment network and storing computer code.
Primary Use Case	Store of Value, Peer to Peer Transactions	Smart Contracts, DApps, DeFi, NFTs
Blockchain Technology	Transaction – Based UTXO Model	Smart Contracts, Ethereum Virtual Machine (EVM)
Scalability	Lightning Network, sidechains	Layer – 2 scaling like zk rollups, optimistic rollups and state channels, sidechains
Smart Contracts	Although bitcoin do have smart contracts, they are not as flexible or complete as Ethereum smart contracts. Smart contracts in Bitcoin does not have all the functionality that	Ethereum allows us to create smart contracts. Smart contracts are computer codes that is stored on a blockchain and executed when the predetermined terms and conditions are met.

	a programming language would give them.	
Smart Contract Programming Language	Smart contracts on Bitcoin are written in programming languages like Script, Clarity.	Smart contracts on Ethereum are written in programming languages like Solidity, Vyper, etc.
Transactions	Generally, bitcoin transactions are only for keeping notes.	Ethereum transactions may contain some executable code.
Hash Algorithm	Bitcoin runs on the SHA-256 hash algorithm.	Ethereum runs on the Keccak-256 hash algorithm.
Consensus Mechanism	The Proof-of-Work (PoW) is the consensus mechanism used by the Bitcoin network.	The Proof-of-Stake is the consensus mechanism used by Ethereum.
Block Creators	Block creators are known as miners. To become a miner, participants need to buy energy and equipment.	Block creators are known as validators. In order to become a validator, participants need to buy coins or tokens.
Block Time	The block time of bitcoin is 10 minutes.	The block time of Ethereum is 14 to 15 seconds.
Block Limit	The bitcoin blockchain has a block limit of 1 MB.	The Ethereum blockchain does not have a block limit.
Popularity	Bitcoin is the most popular digital currency in the market to date.	Ether, native currency of Ethereum is the second-largest cryptocurrency after bitcoin to date.
Energy Consumption	Energy consumption is very high.	Energy consumption is very low as compared to bitcoin
Structure	Structure of bitcoin is simple and robust.	Structure of Ethereum is complex and feature rich
Assets	Assets of Bitcoin is BTC.	Assets of Ethereum is Ether.
Developer Community	Active, with contributions from BIPs	Active, focused on DApps, DeFi and EIPs
Security Features	Robust security and immutability	Smart contract vulnerabilities, ongoing improvements
Applications	Bitcoin uses blockchain technology for monetary transactions and allows nodes and messages to be attached to each transaction.	Ethereum takes it a step further by using the blockchain to create a decentralized computer.
Real-world Applications	Cross-border remittances, hedge against inflation	DeFi, NFTs, Supply chain, identity verification, etc
Industry Adoption and Partnerships	Investment from institutions, payment processor integration	Enterprises exploring use cases, EEA

Summing up

As one of the most ambitious blockchain projects, Ethereum and its native token ether (ETH) have been growing steadily since the platform launched in 2015. Unlike Bitcoin, Ethereum is more than just a blockchain-based cryptocurrency — it is a programmable blockchain pioneer that has fuelled the creation of many Dapps, helped to launch hundreds of new coins, and has become a DeFi leader. Despite its significant benefits such as safety, confidentiality, the

technology is relatively new to users and still faces limitations from government regulations. However, this blockchain can be the mover and shaker of the fourth industrial revolution.

References

https://www.globalxetfs.com/ethereum-the-basics/

https://www.guru99.com/ethereum-tutorial.html

https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-ethereum

https://www.globalxetfs.com/ethereum-the-basics/

https://www.sofi.com/what-is-ethereum/

https://www.investopedia.com/terms/e/ethereum.asp

https://www.wallstreetmojo.com/ethereum/

https://www.theknowledgeacademy.com/blog/advantages-and-disadvantages-of-ethereum/

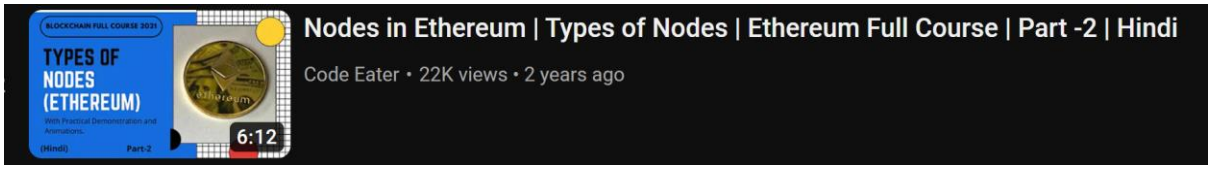
https://www.geeksforgeeks.org/what-is-ethereum/

https://worldcoin.org/articles/history-of-ethereum

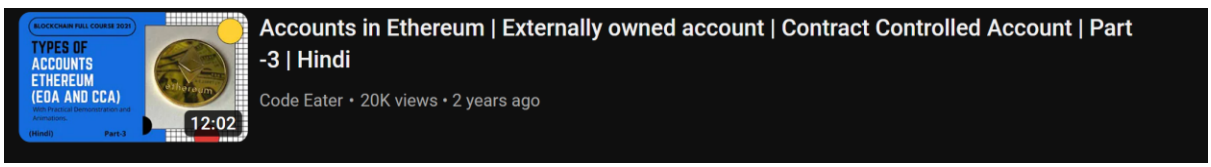
https://www.inx.co/learn/beginners/ethereum-vs-bitcoin-a-comprehensive-comparison-of-blockchains-big-two/

Videos

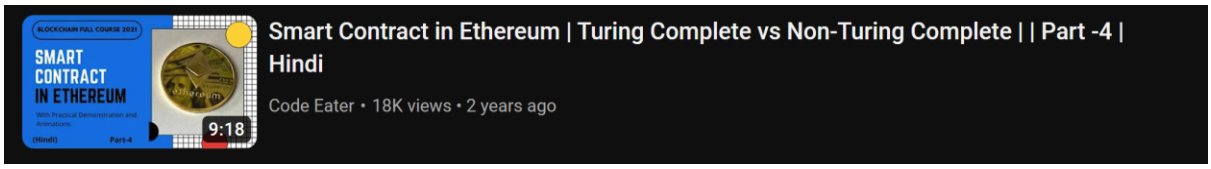
https://www.youtube.com/watch?v=XRl3MW4DFt4&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=1



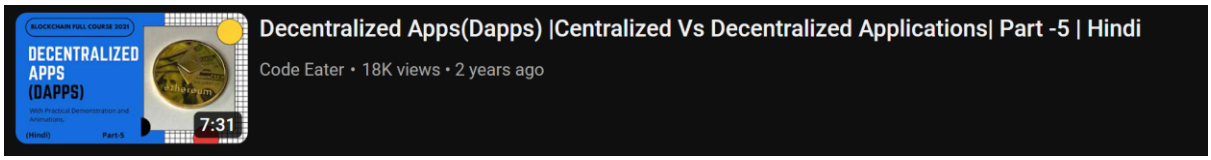
https://www.youtube.com/watch?v=FYITGhfs_ng&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=2



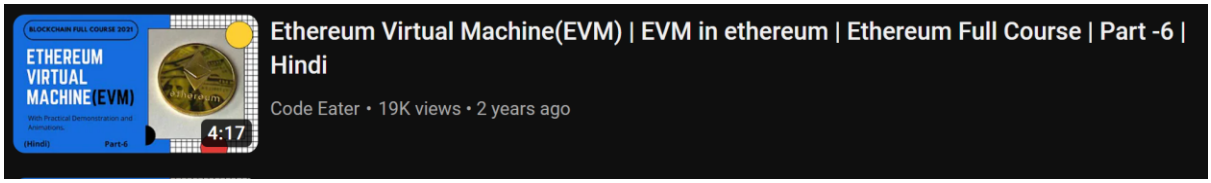
https://www.youtube.com/watch?v=EpAXK3_Eaog&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=3



https://www.youtube.com/watch?v=vZQaX2MsZT4&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=4



https://www.youtube.com/watch?v=8lRm2e9omy8&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=5

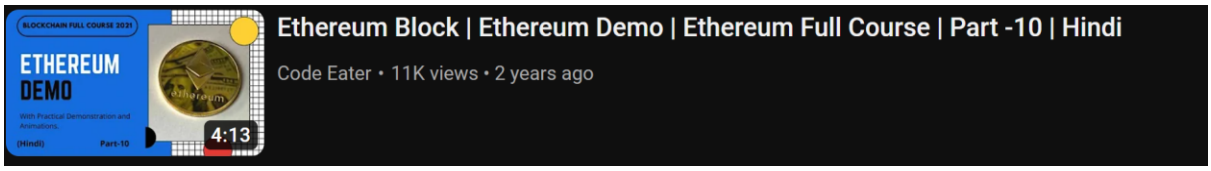


https://www.youtube.com/watch?v=k_QyvLCXRRM&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=6

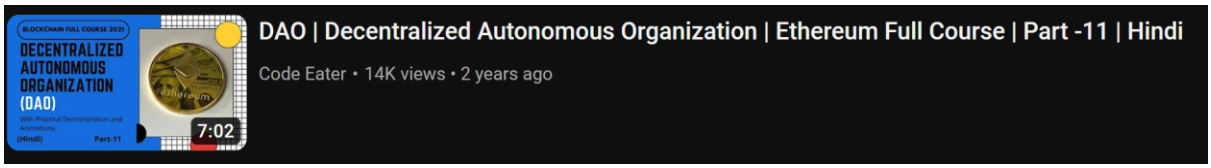
https://www.youtube.com/watch?v=_4BroqQ3h7M&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=7

https://www.youtube.com/watch?v=1GT3qQkt34c&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=8

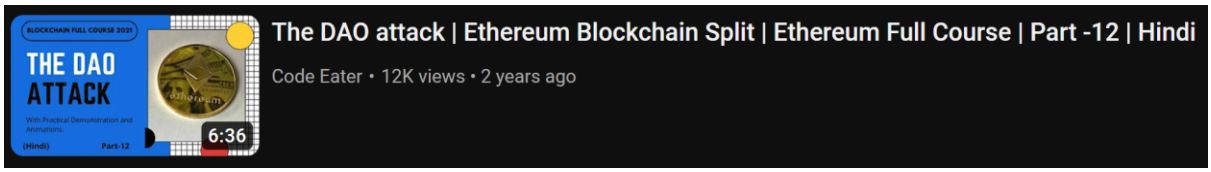
https://www.youtube.com/watch?v=fN87w9U86gI&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=9



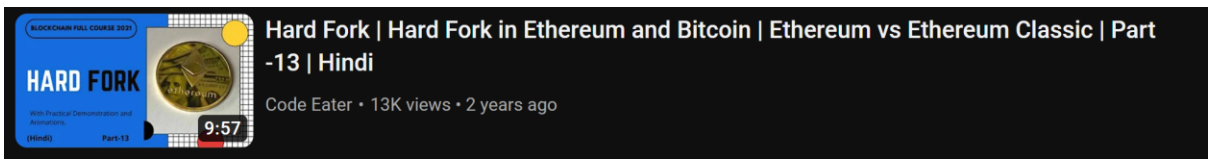
https://www.youtube.com/watch?v=lKNEPySpb6s&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=10



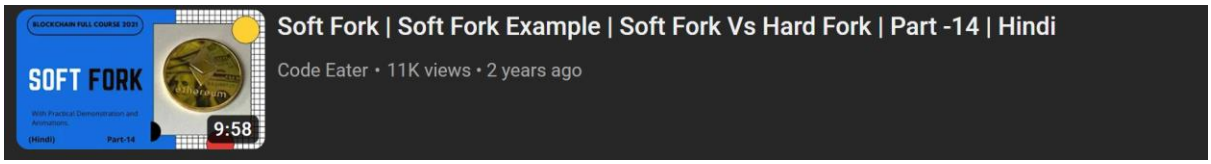
https://www.youtube.com/watch?v=SV6cIrozxK4&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=11



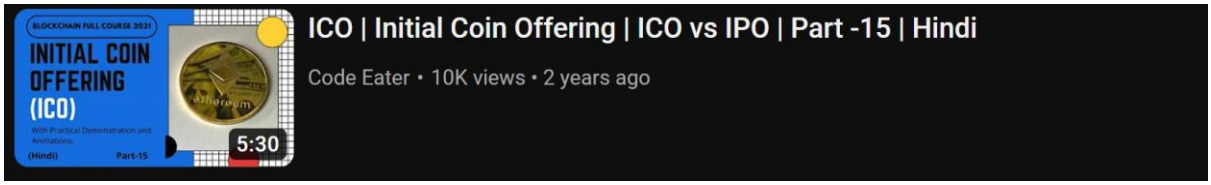
https://www.youtube.com/watch?v=_fIjUmwOhtU&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=12



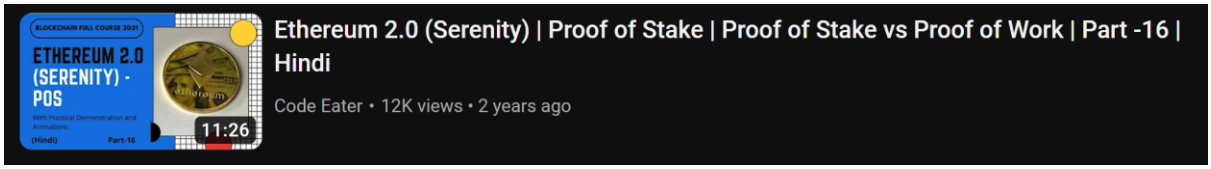
https://www.youtube.com/watch?v=KhKwt3SIIgE&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=13



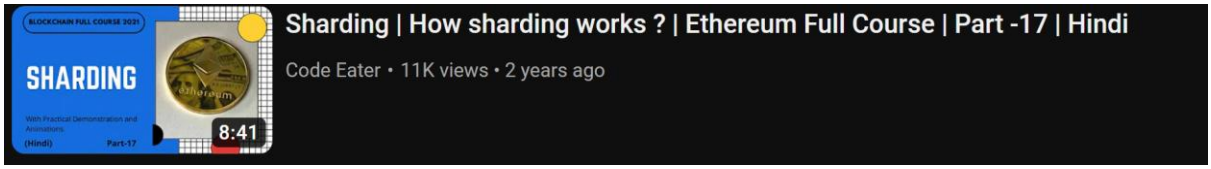
https://www.youtube.com/watch?v=3KI6JgY1JAA&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=14



https://www.youtube.com/watch?v=ZCBlxjo_sG0&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=15



https://www.youtube.com/watch?v=tyroSaq2OC4&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=16



https://www.youtube.com/watch?v=jVZarNPsW9Y&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=17

https://www.youtube.com/watch?v=W8ybR0NR_aY&list=PLgPmWS2dQHW9FmqNqug3M5ooNuRqP-alu&index=18