

Contents – Module C

What is Ethereum?

EVM and Gas

DAO Attack

Smart Contract

DAOs

ICO

Dapps

Hard and Soft Fork

Alt Coins



3:59:57 / 6:07:35 • Ether...



What is Ethereum?

- **Ethereum** is an open-source blockchain-based platform.

Bitcoin



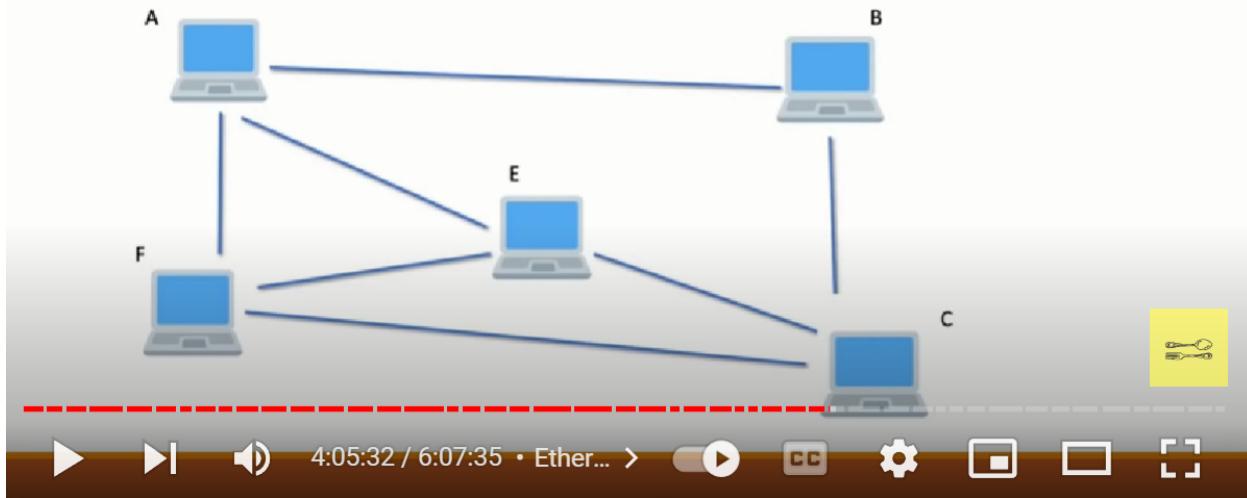
Ethereum



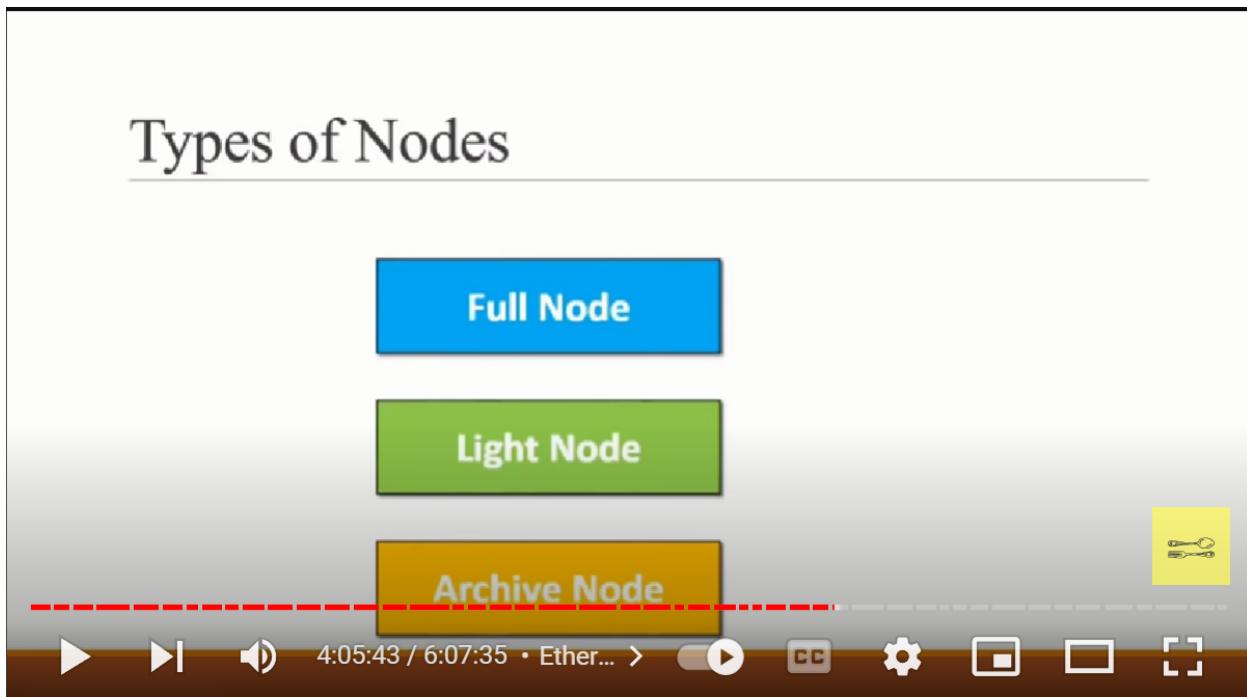
4:04:44 / 6:07:35 • Ether...



Ethereum Nodes

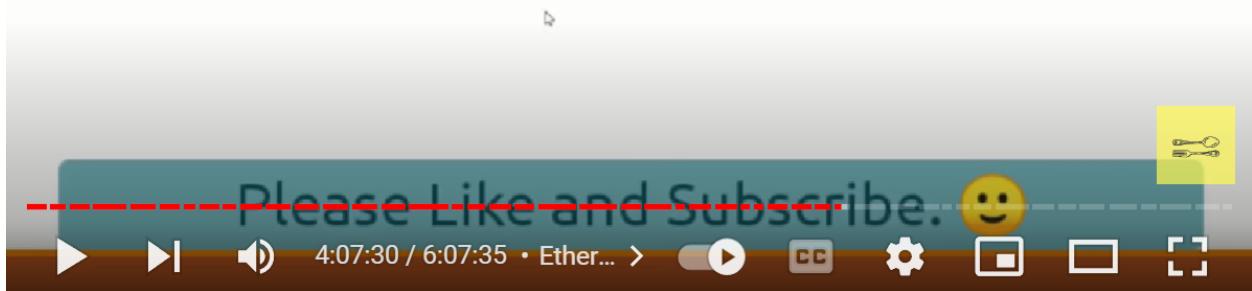


Types of Nodes



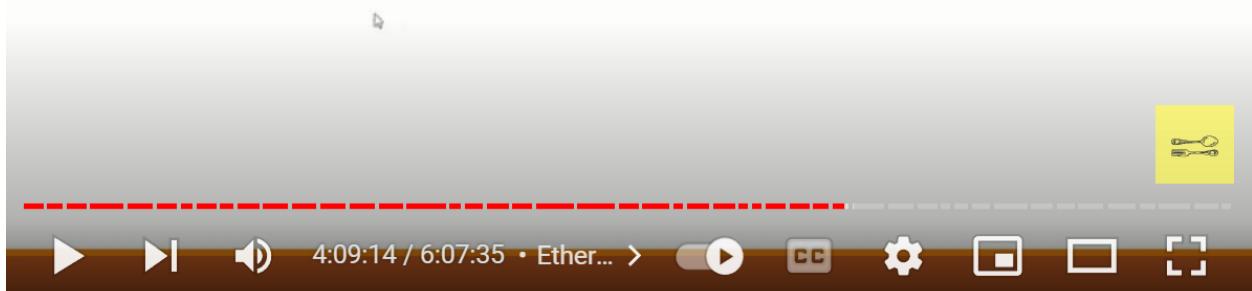
Full Node

- Locally stores a copy of the entire blockchain.
- Verifies and validates all the block.



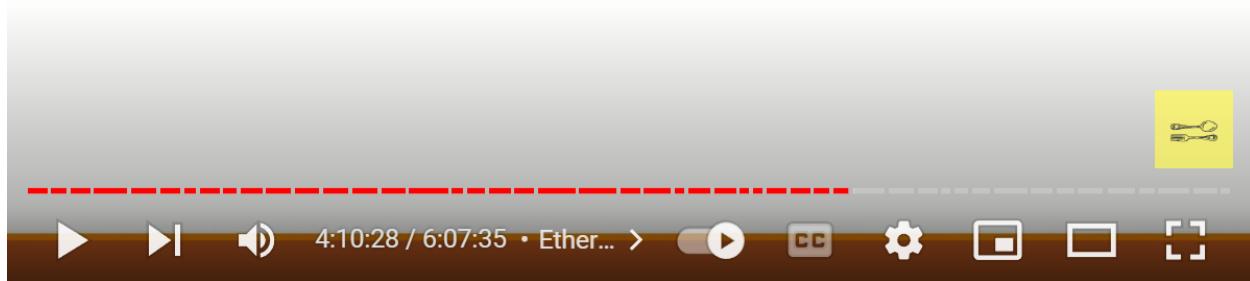
Light Node

- Stores only the block header. Depends on full node.
- For low capacity devices which cannot afford to store the gigabytes of data.



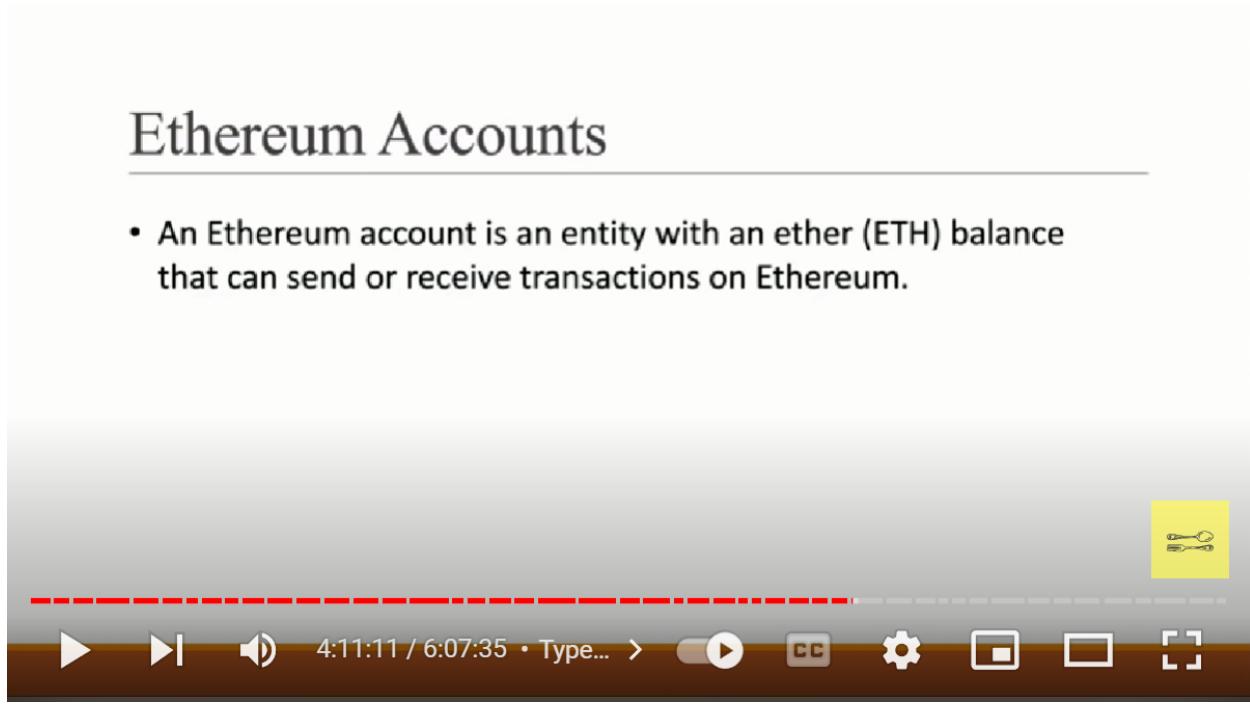
Archive Node

- Stores everything kept in the full node and built an archive of historical data.
- Requires terabytes of disk space.



Ethereum Accounts

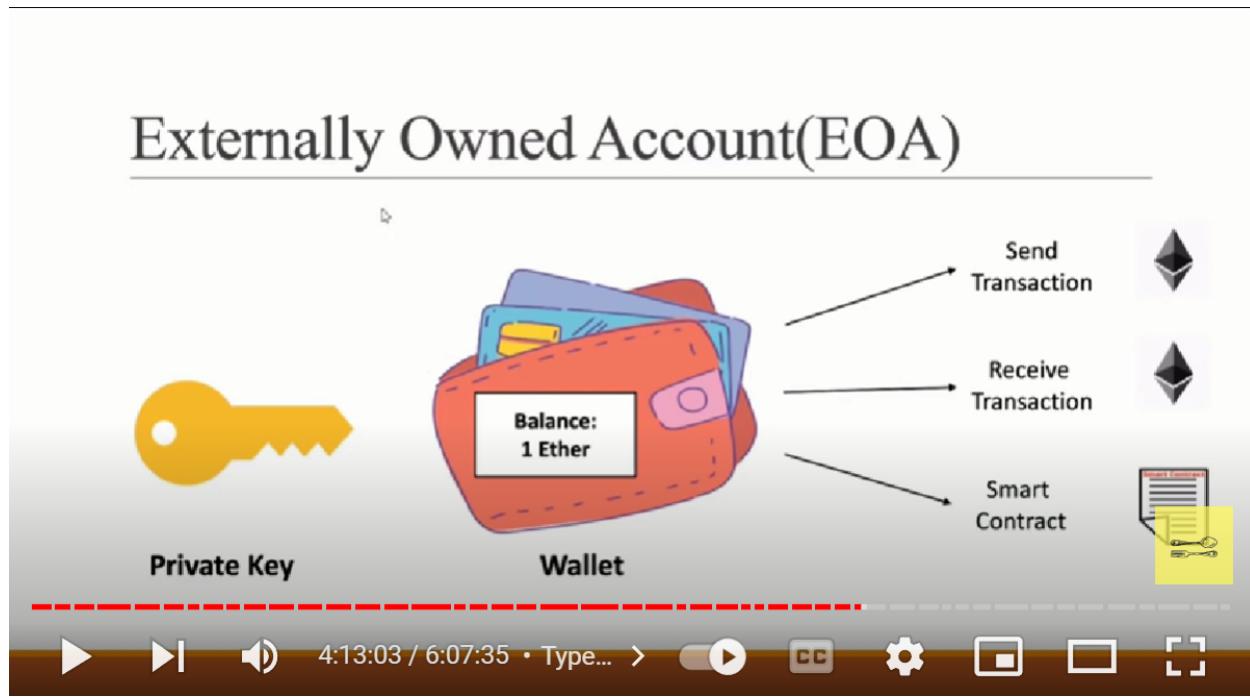
- An Ethereum account is an entity with an ether (ETH) balance that can send or receive transactions on Ethereum.



Types of Ethereum Accounts

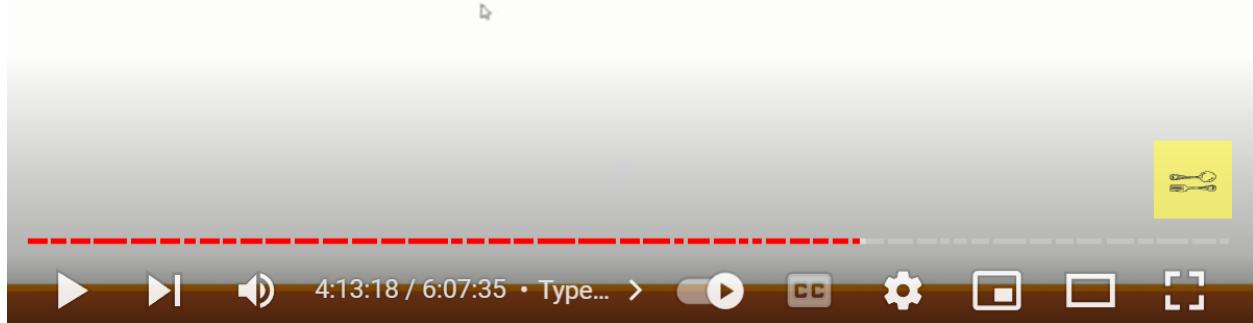


Externally Owned Account(EOA)



Contract Account (CA)

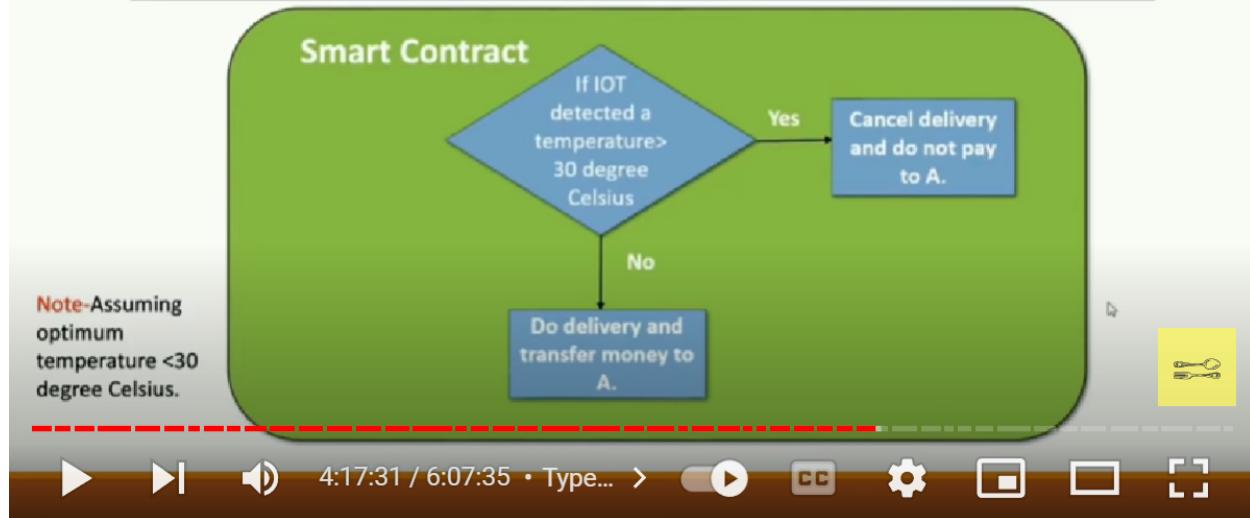
- Controlled by contract code.



Smart Contract



Smart Contract



EOA VS CA

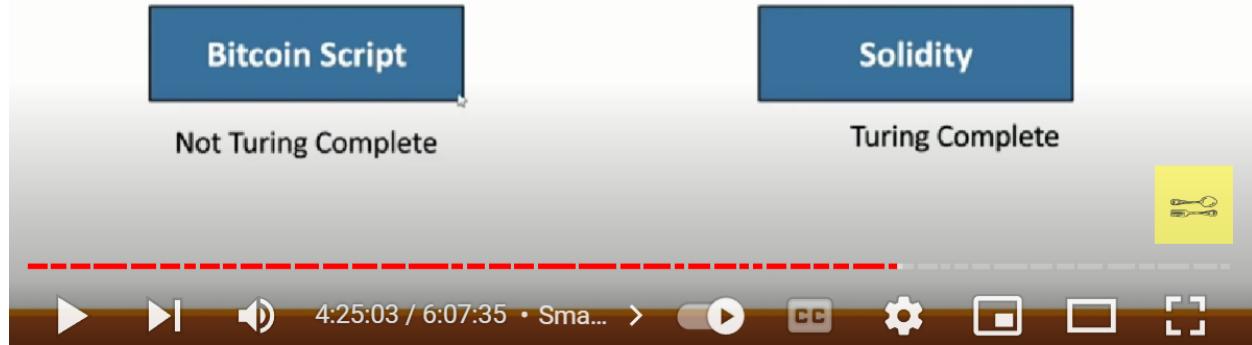
EOA	CA
Private Key is needed	No private or public key is needed.
Controlled by Human	Controlled by Contract code
No gas is associated	Gas is associated
Has a unique address	Has a unique address

Holds ETH balance

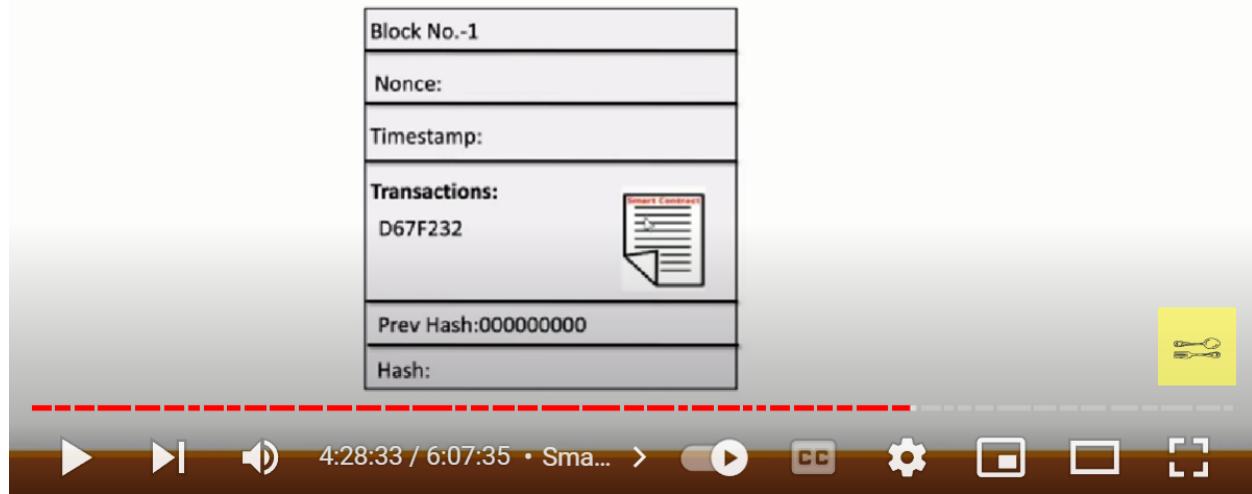
Holds ETH balance

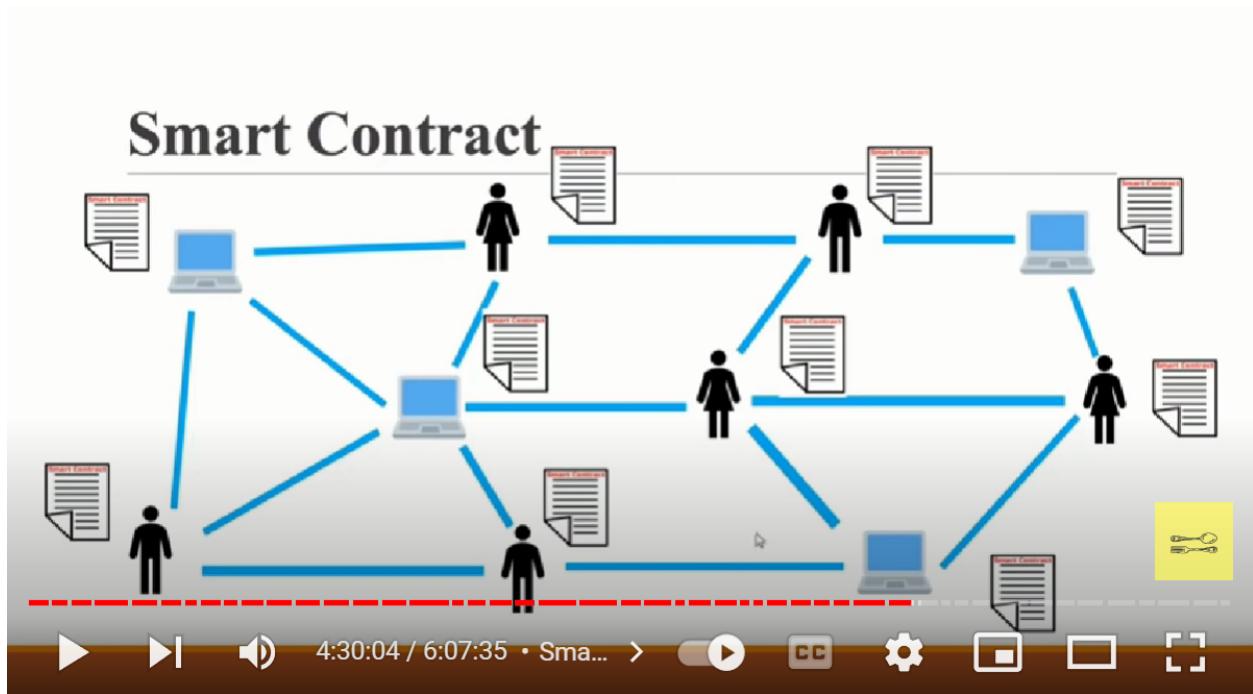


Smart Contract



Smart Contract

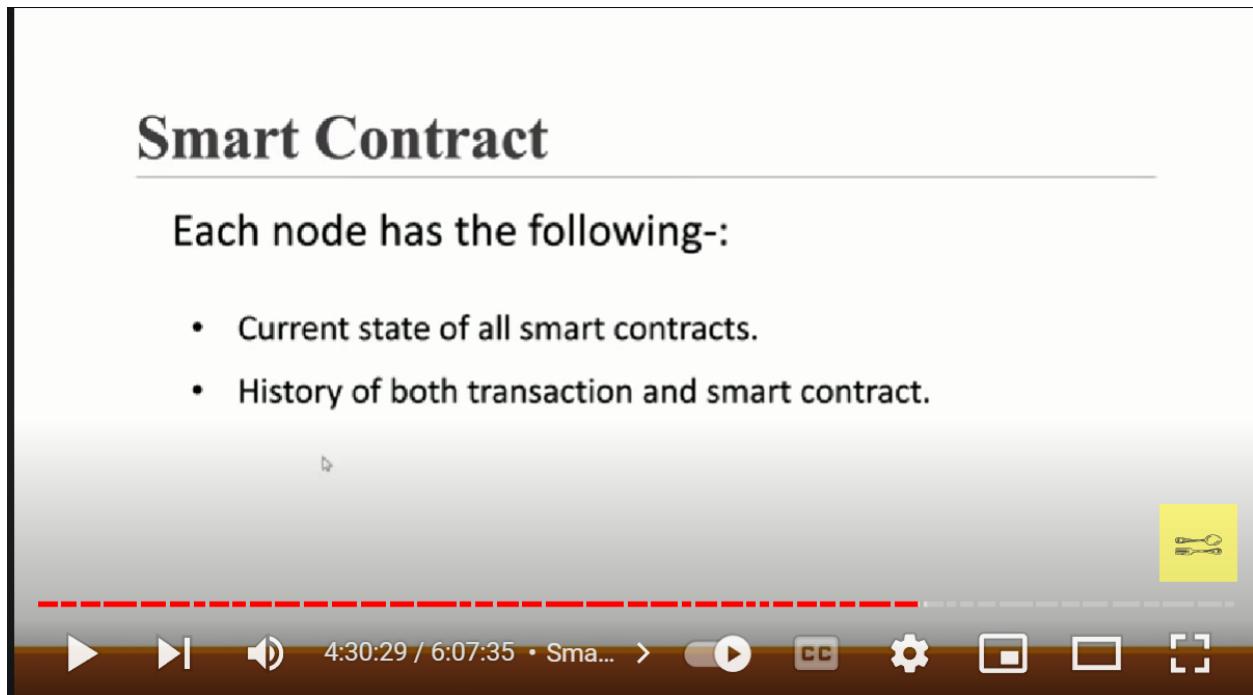




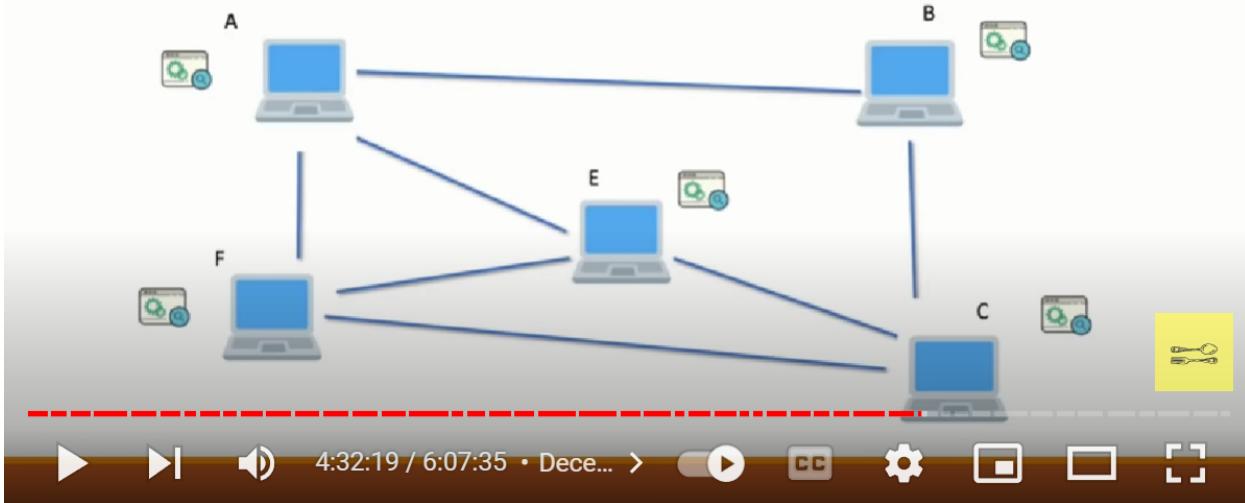
Smart Contract

Each node has the following:-

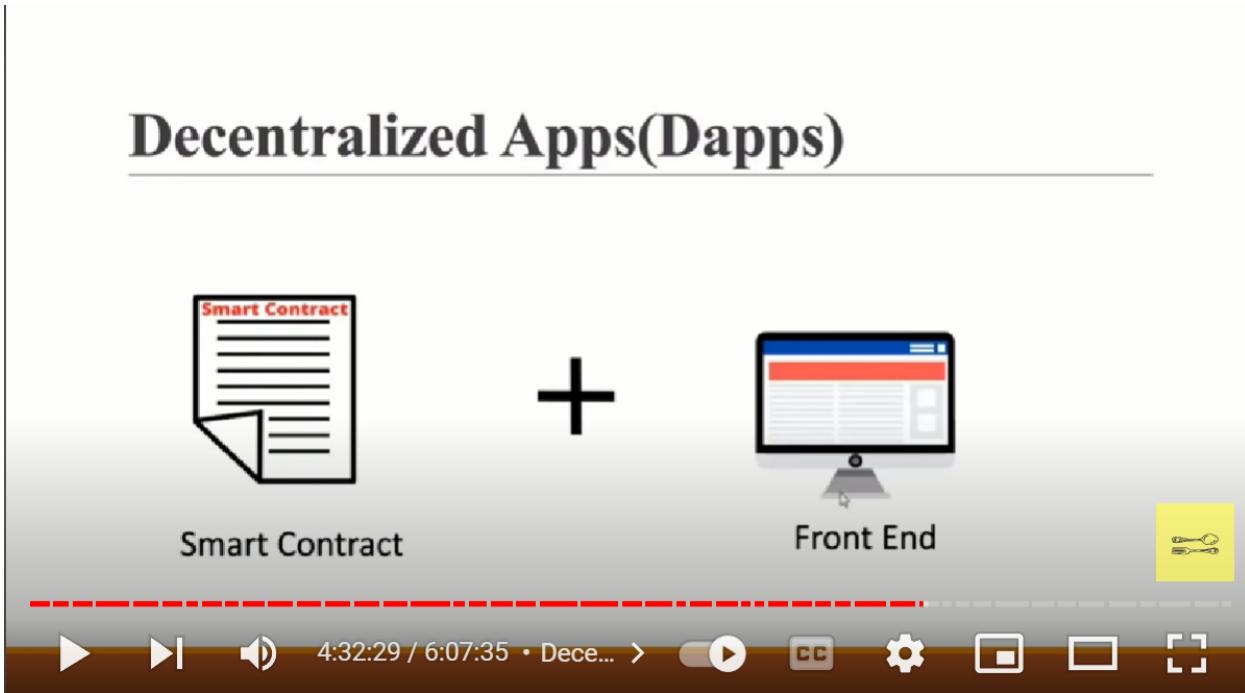
- Current state of all smart contracts.
- History of both transaction and smart contract.



Decentralized Apps(Dapps)

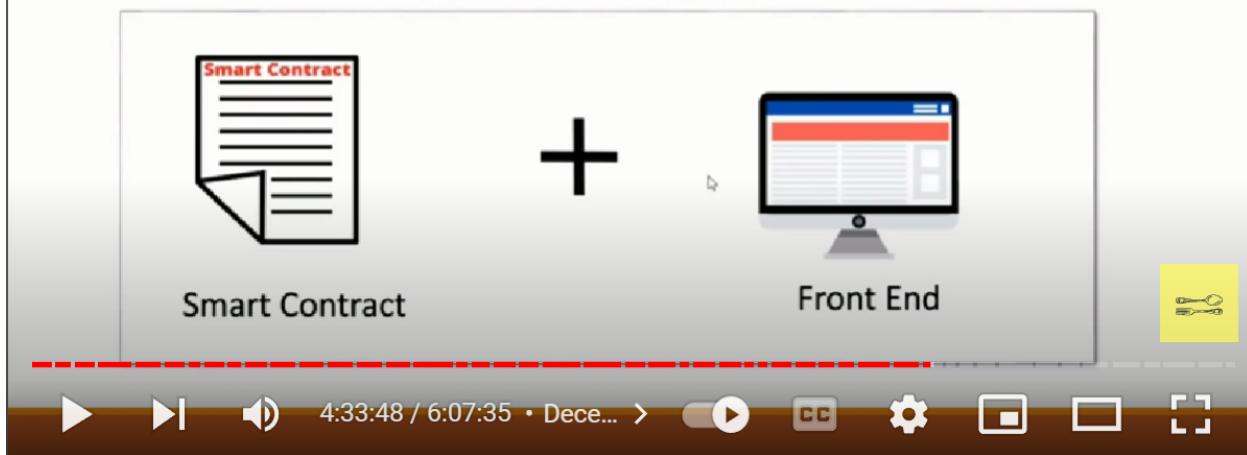


Decentralized Apps(Dapps)



Decentralized Apps(Dapps)

Decentralized Network



Decentralized Apps(Dapps)

Search Engine



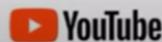
Presearch

Social Media



LBRY

Video Platform



D.tube

▶ ▶| ⏪ 4:34:16 / 6:07:35 • Dece... > 🔍 CC ⚙️



Decentralized Apps(Dapps)

Centralized Apps	Decentralized Apps
Not Trustworthy	Trustworthy
Censorship	No censorship
You pay	They pay
Go down	Can never go down

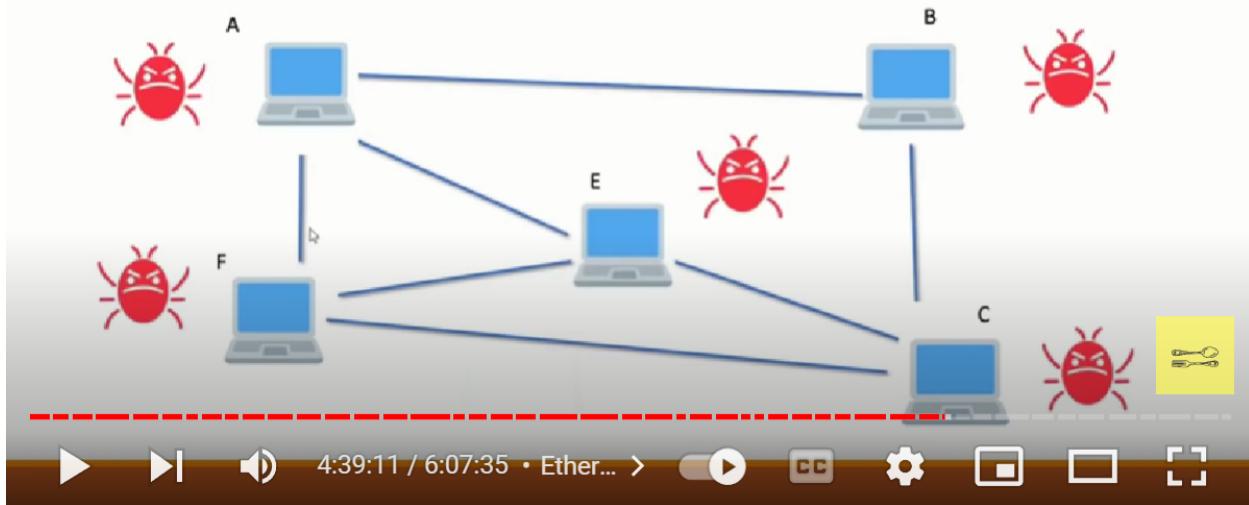
▶ ▶| 🔍 4:35:18 / 6:07:35 • Dece... > ⏴ CC ⚙️ 🖊️ 🖊️ 🖊️

Ethereum Virtual Machine



▶ ▶| 🔍 4:39:03 / 6:07:35 • Ether... > ⏴ CC ⚙️ 🖊️ 🖊️ 🖊️

Ethereum Virtual Machine



Ethereum Virtual Machine



Ethereum Gas



Ethereum Gas

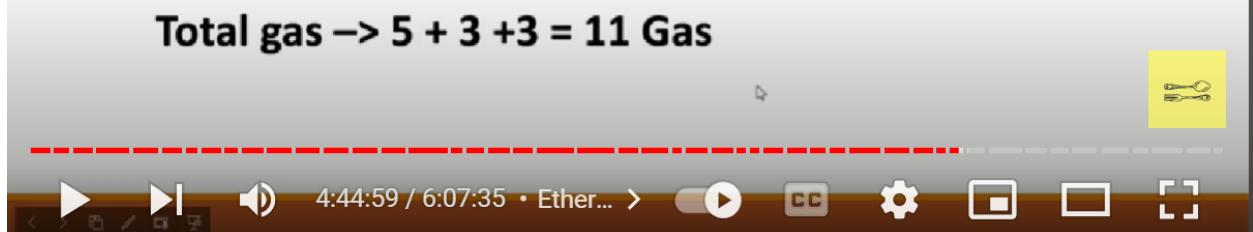
$$10 * 3 - 6 = ?$$

Multiplication – 5 gas

Subtraction – 3 gas

Equal to – 3 gas

Total gas → 5 + 3 +3 = 11 Gas



Ethereum Gas

Some important points to note -

- Any transaction that modifies the blockchain costs gas.
- The user that generated the transaction pays for the gas.



Gas Price



Petrol – 10 liters

Total price= ?

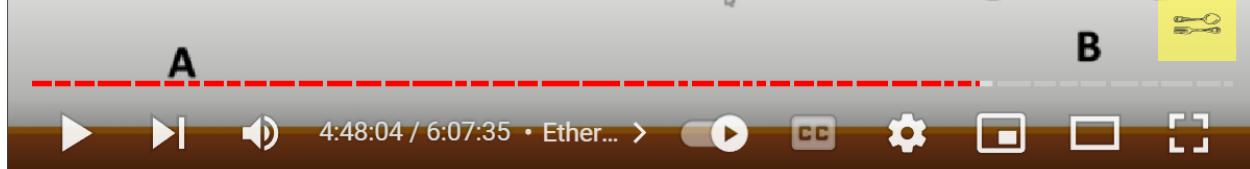
1 liter – Rs.5

Total price= $10 \times 5 =$
Rs. 50



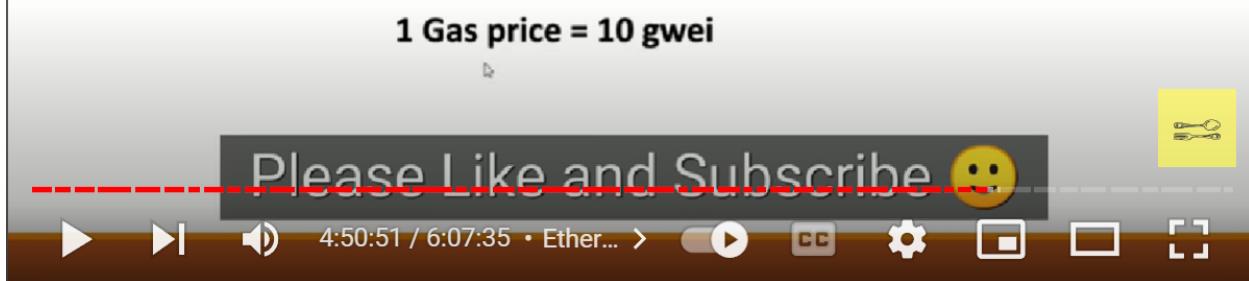
A

B



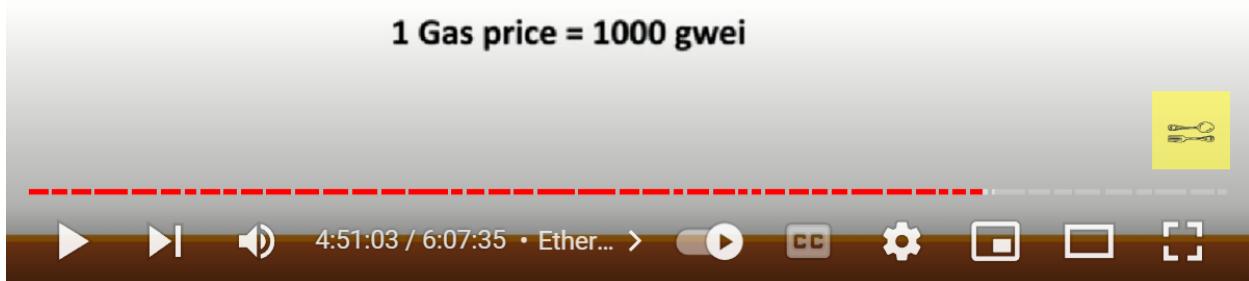
Gas Price

- It is the amount the sender wants to pay per unit of gas to get the transaction mined. `gasPrice` is set by the sender.
- Gas prices are denoted in gwei. ($1 \text{ gwei} = 10^{-9} \text{ ETH}$)



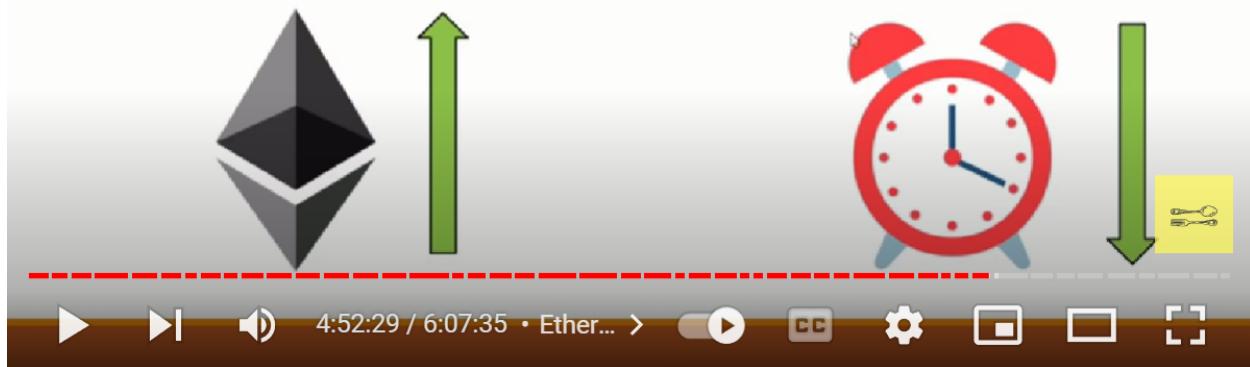
Gas Price

- It is the amount the sender wants to pay per unit of gas to get the transaction mined. `gasPrice` is set by the sender.
- Gas prices are denoted in gwei. ($1 \text{ gwei} = 10^{-9} \text{ ETH}$)



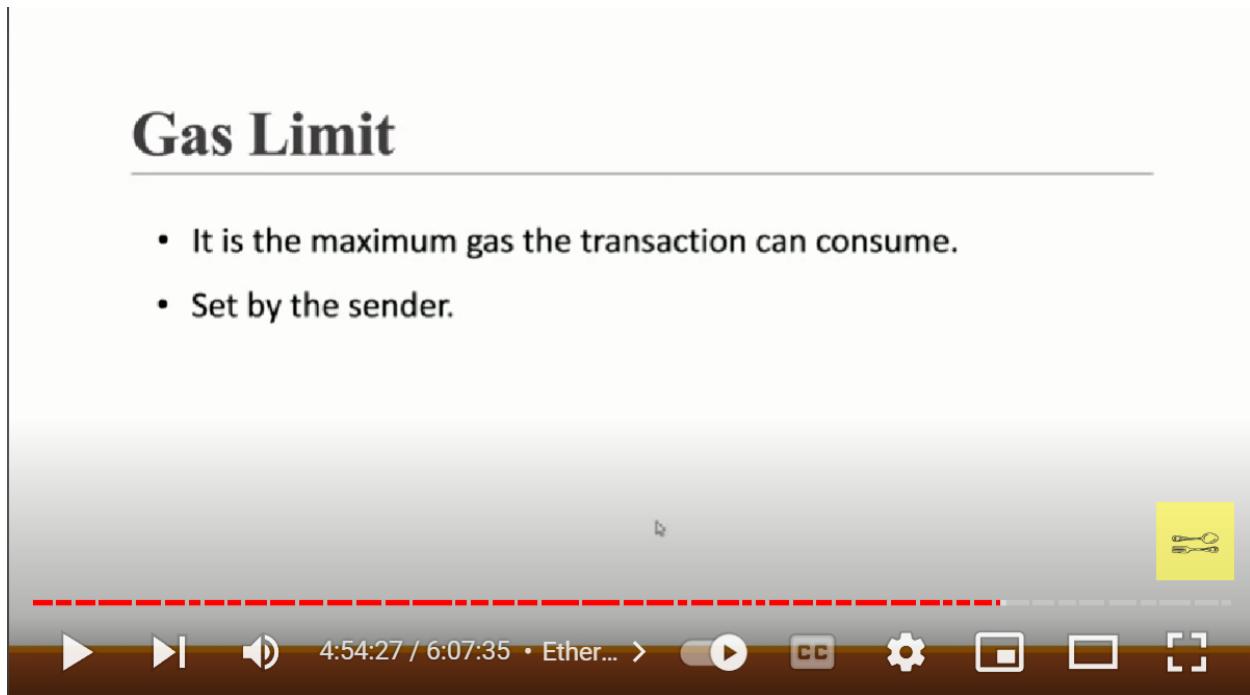
Gas Price

- The higher the gas price the faster the transaction will be mined. It just like the transaction in Bitcoin.



Gas Limit

- It is the maximum gas the transaction can consume.
- Set by the sender.



Gas Limit

Let say A wants to send B 2 ETH. So what will be the total fees A that has to pay ?

Case 1: When transaction gas limit is 21,000 units.

A sets the gas price per unit = 100 gwei.

Transaction gas limit = 21,000 units. ↴

Total fee will be: Gas units(limit) * Gas price per unit

Total fee will be: $21,000 * 100 = 210,0000$ gwei or 0.0021 ETH



Gas Limit

Let say A wants to send B 2 ETH. So what will be the total fees A that has to pay ?

Case 2: When gas transaction limit < 21000 units.

Transaction gas limit = 20,000 units. ↴

Transaction Fail



Gas Limit

Let say A wants to send B 2 ETH. So what will be the total fees A that has to pay ?

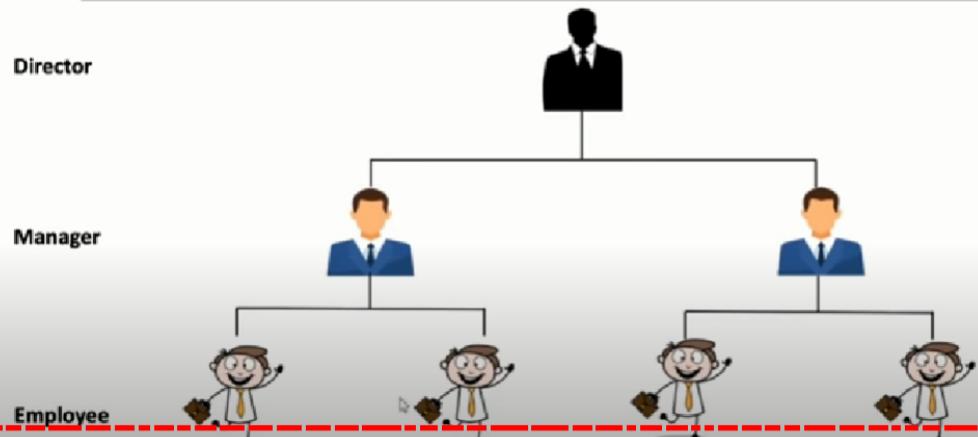
Case 3: When gas transaction limit > 21000 units.

Transaction gas limit = 22,000 units.

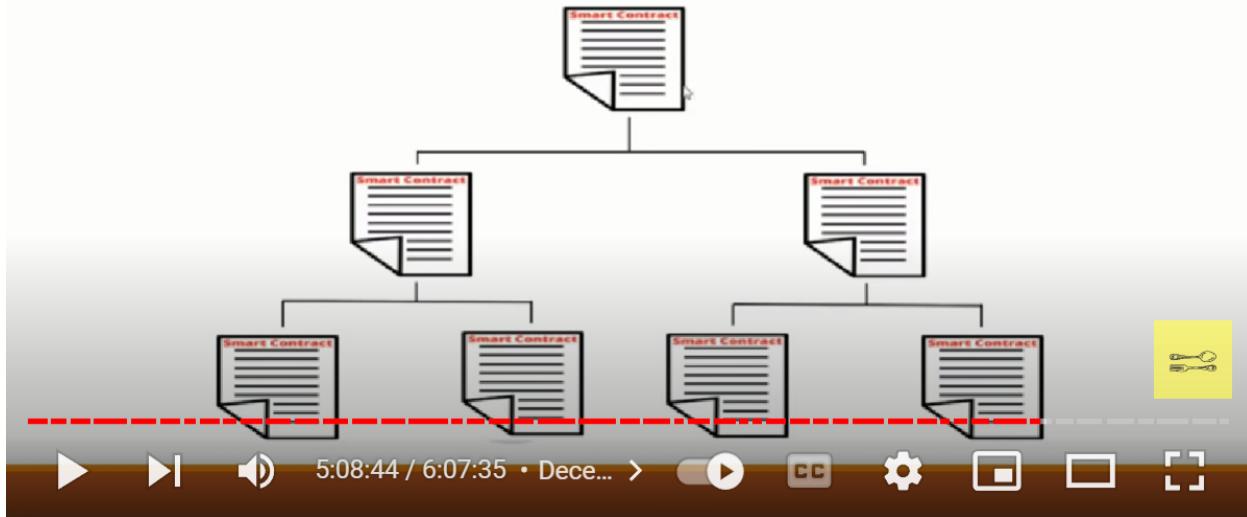
22,000 – 21000 = 1000 will be returned



Decentralized Autonomous Organization (DAOs)



Decentralized Autonomous Organization (DAOs)



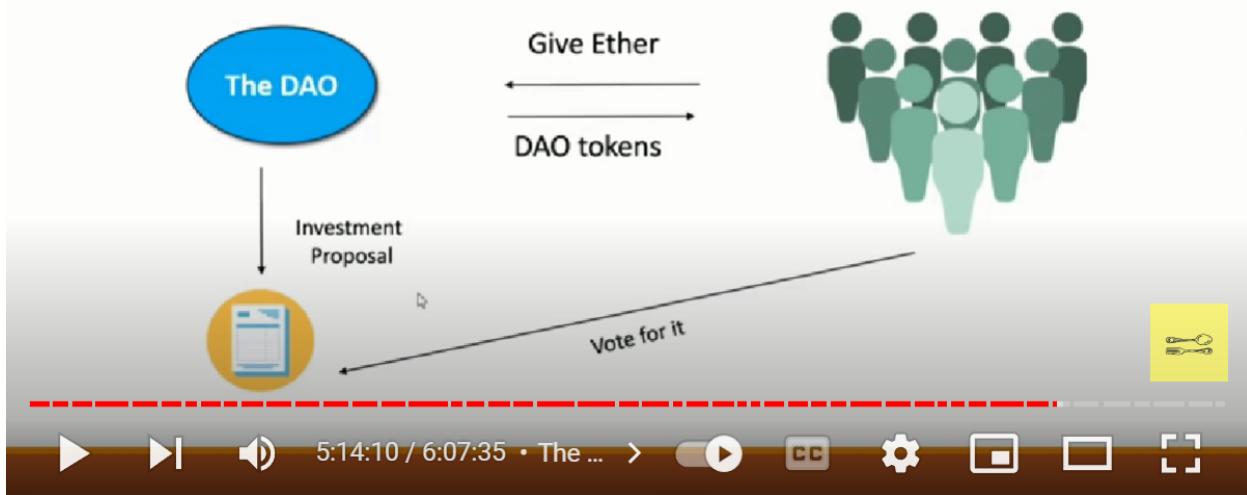
DAO vs Organization

DAO	A traditional organization
Fully democratized.	Usually hierarchical.
Voting required .	Voting may or may not require.
No trusted intermediary to count vote.	Outcome of voting must be handled manually.
Services offered are handled automatically.	Requires human handling, or centrally controlled automation.
All activity is transparent and fully public	Activity is typically private, and limited to the public.

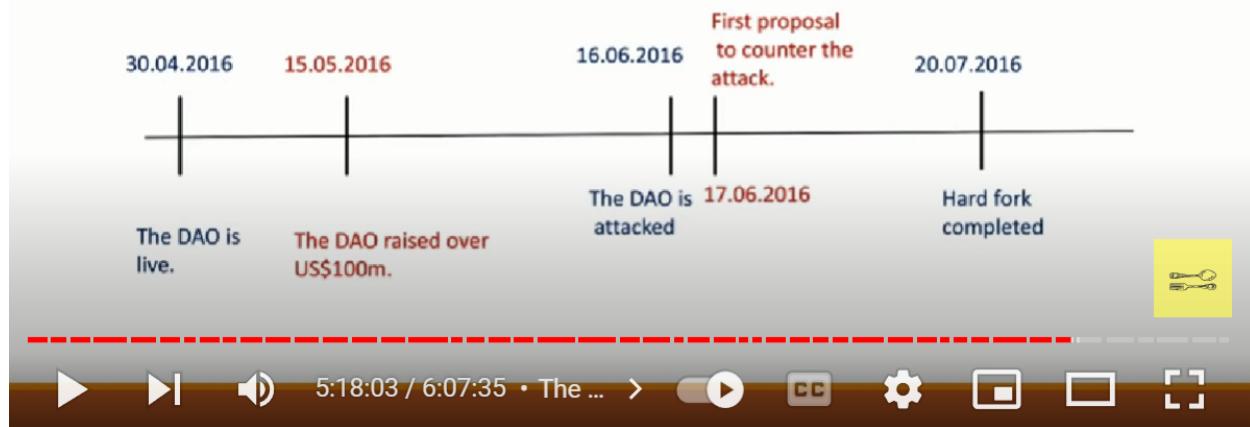
Decentralized Autonomous Organization (DAOs)



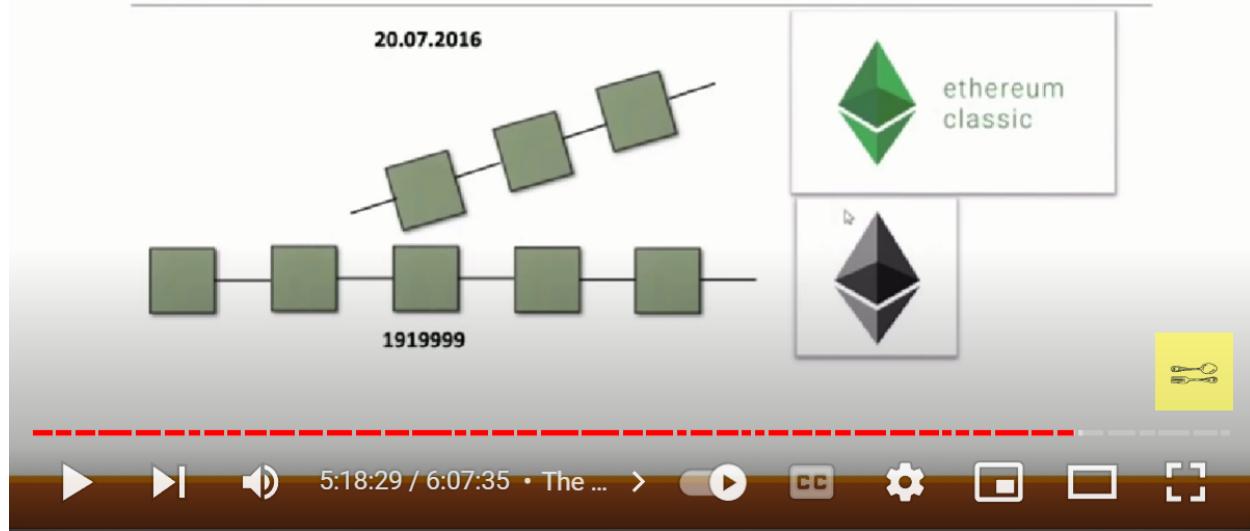
The DAO Attack



The DAO Attack



The DAO Attack

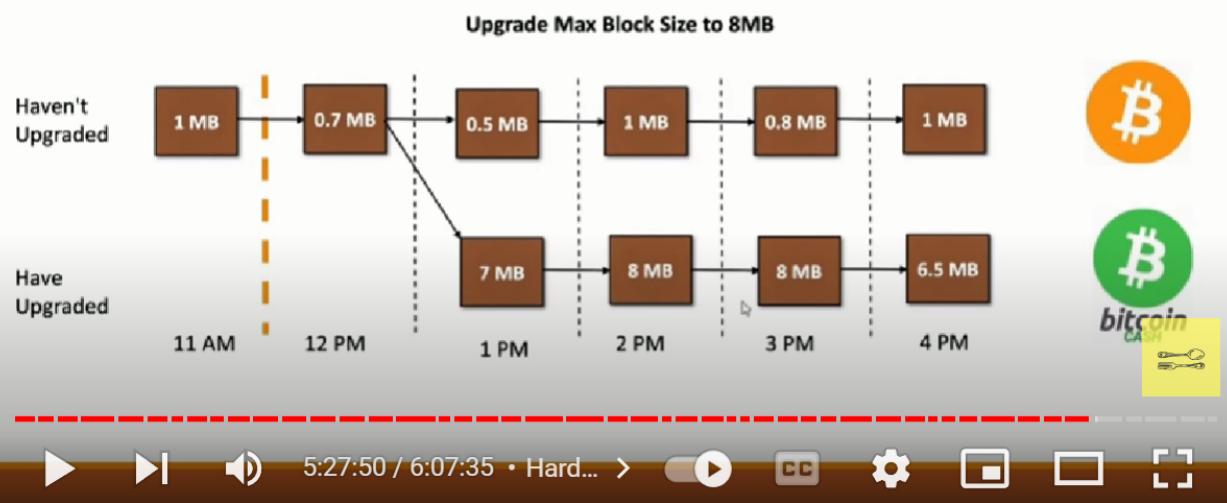


Hard Fork

- During a hard fork, software implementing a protocol and its mining procedures is upgraded.
- Once a user upgrades their software, that version rejects all transactions from older software, effectively creating a new branch of the blockchain.
- However, those users who retain the old software continue to process transactions.



Hard Fork



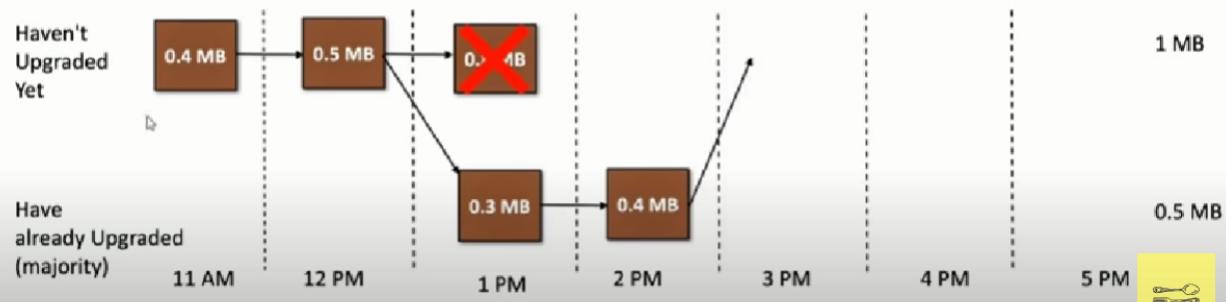
Soft Fork

- Soft forks are a change to the protocol, **but the end product remains unchanged.**
- A soft fork is a *backward-compatible* upgrade, meaning that the upgraded nodes can still communicate with the non-upgraded ones.
- Old nodes(not upgraded nodes) could still validate blocks and transactions (the formatting didn't break the rules), but they just wouldn't understand them.

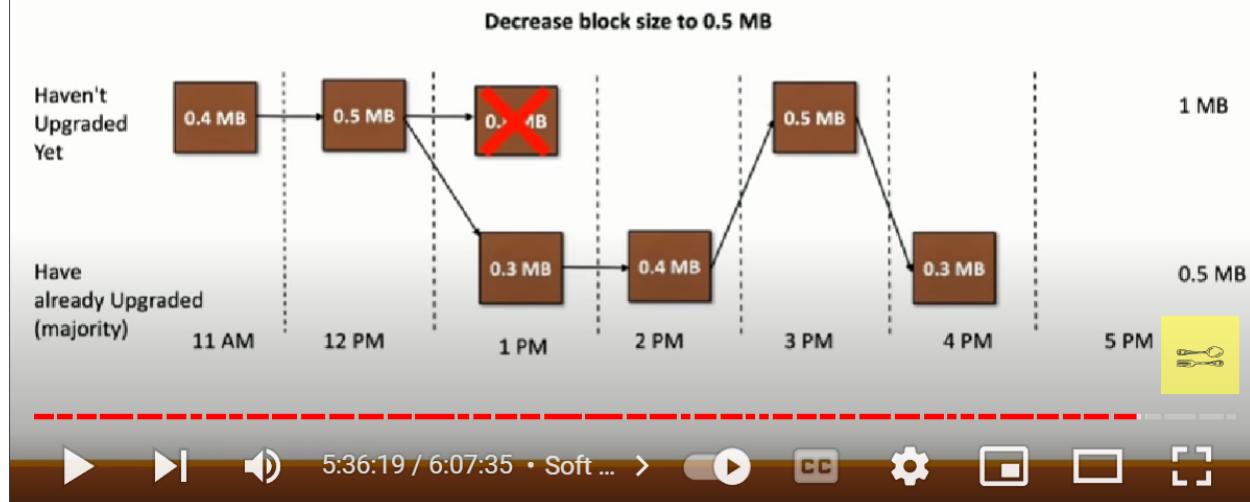


Soft Fork

Decrease block size to 0.5 MB



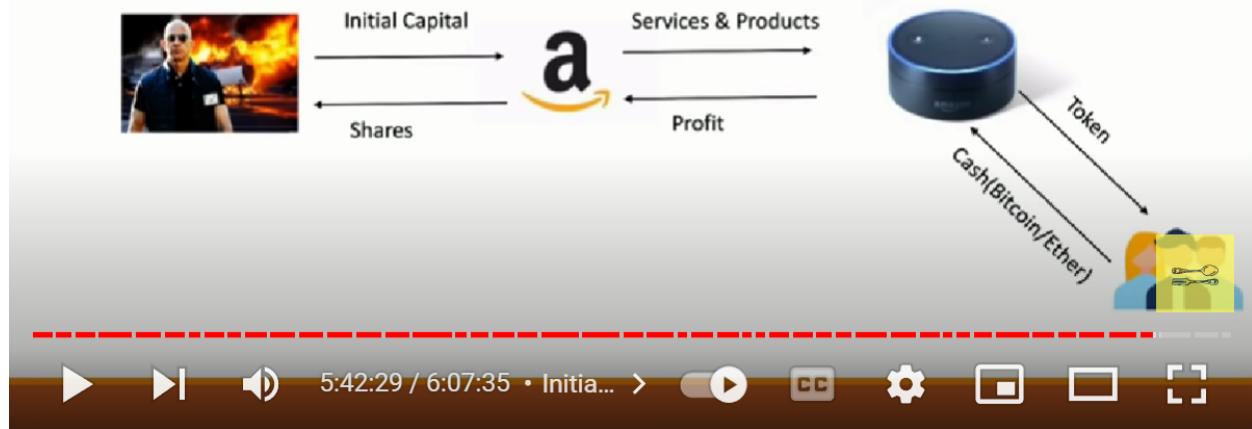
Soft Fork



Initial Coin Offering (ICO)



Initial Coin Offering (ICO)



ETH 2.0

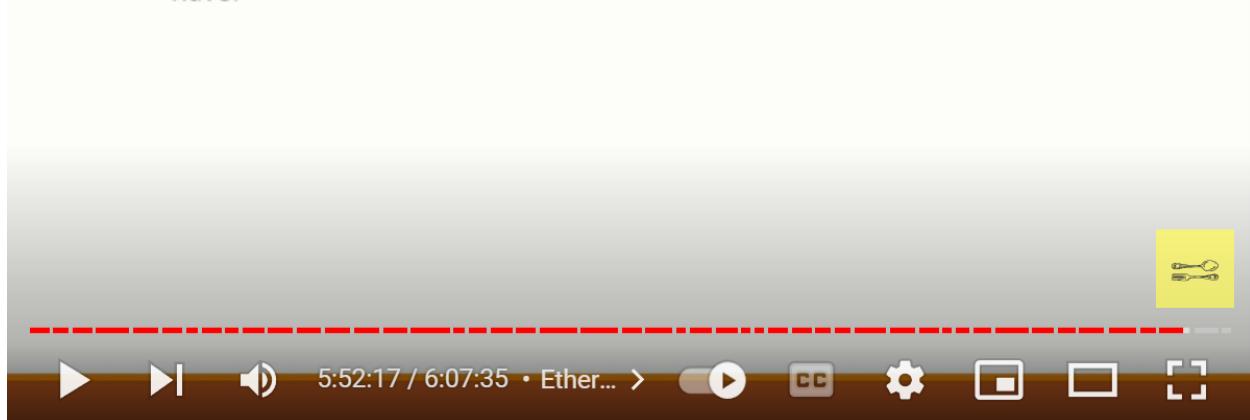


Proof of Stake



Proof of Stake

- The more ether you pay the more chances of getting randomly selected you have.



Proof of Stake

Proof Of Work(PoW)	Proof Of Stake(PoS)
Miners	Validators
High performance hardware required.	Mobile or Laptop are enough.
Lots of electricity required.	Not much electricity is required.
The more hashing power you have the more blocks you can validate.	The more ETH you stake the more blocks you can validate.
Attack to happen 51% hashing power is required.	Attack to happen 51% of stake is required.

Competition is there.

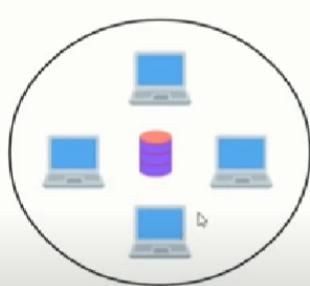
Random selection is there.



5:54:38 / 6:07:35 • Ether...



Sharding



Network A



Network B



Network C

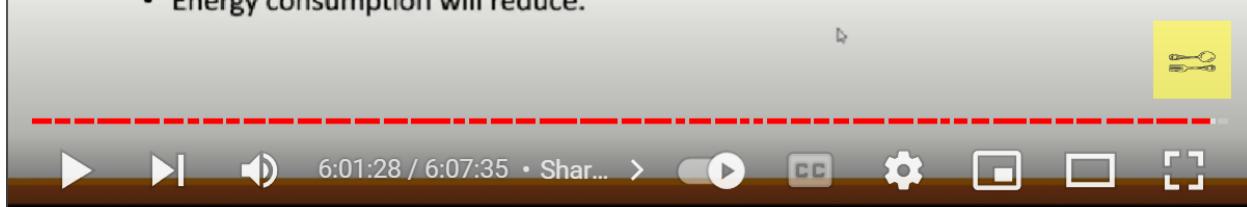


6:00:26 / 6:07:35 • Shar...



Major benefits

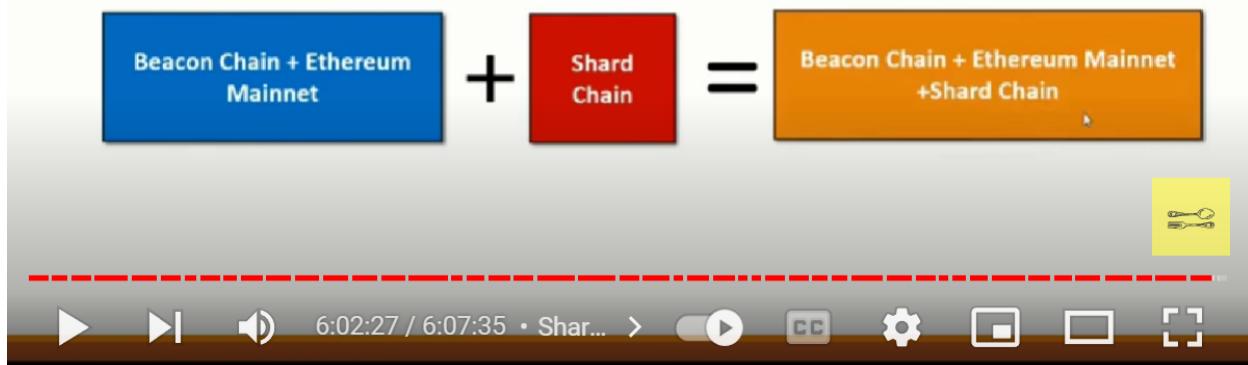
- Transactions per second increase.
- Powerful and expensive computers will not be needed.
- More validators will join.
- Energy consumption will reduce.



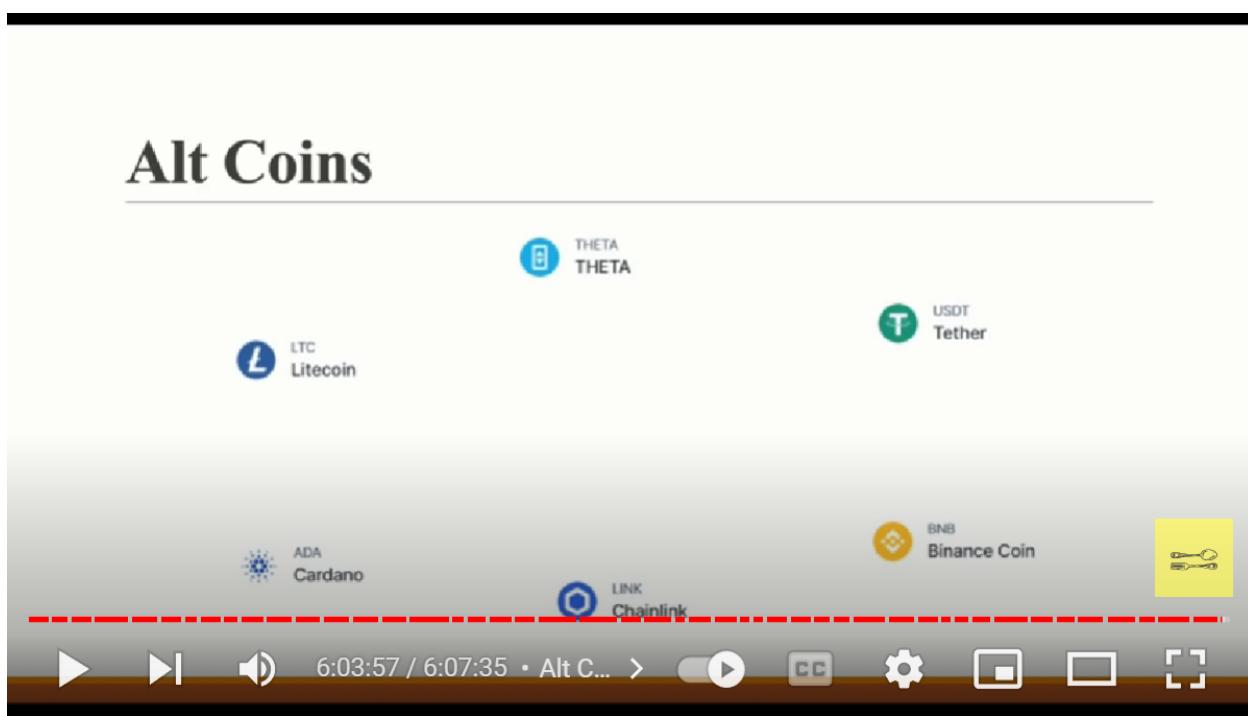
Sharding



Sharding



Alt Coins



Alt Coins

- Consensus Protocol.
- New Capabilities.
- As of March 2021, there were almost 9,000 cryptocurrencies.
- Ethereum and Binance Coin were the largest altcoins by market capitalization as of March 2021.

