→ Blockchain
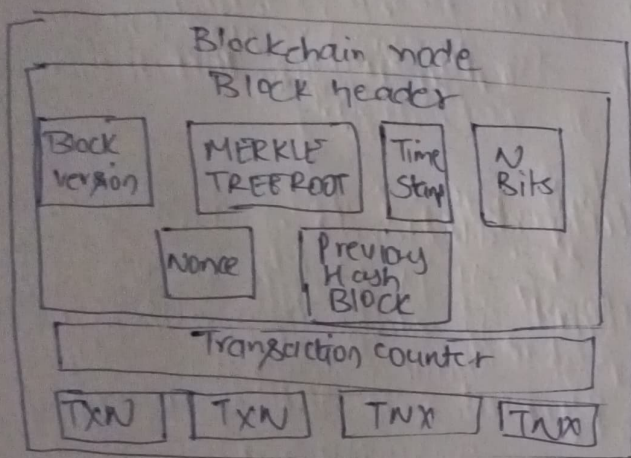
- It is a cryptographically secured record of transactions stored on decentralized network.
- It is a P2P (Peer-to-peer) network.
- It is a chain of a block.
- each block contains various trans" which are approved after complex consensus algo.
- It is a distributed decentralized network.
- Blockchain architecture

→ Que : What are diff. types of Platform in Blockchain.

A   . Public
    . Private
    . Consortium

- Public

. Permissionless (no permission is needed to, anyone can join (Read/write/participate).

. Fully decentralized.
. Open for all
. Participate in consensus
- Anonymous in nature.
. Transparent in nature
. Slow platform
. eg. Bitcoin, Ethereum

· Private

. Permissioned
. Partially decentralized
. low transaction fee
. Single organization has access.
. Read & write for single organi.
. High efficiency
. ex: Hyperledger fabric, Corda.

· Consortium

. Multiple organization have access.
. Typically used by banks, govt.
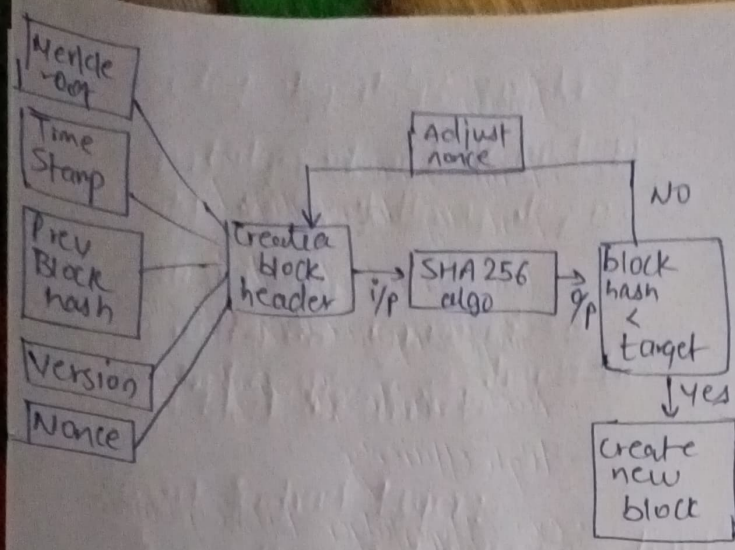. Semi-decentralized.
. eg: R3, energy web foundation.

→ Que : what is Consensus mechanism, explain some mechanism.

A   - It is a Mechanism for mutual agreement
    - All nodes must have same ledger
    - Distributed in nature
    - Peer-to-peer.
    - It is a tradeoff between consistency, Availability & fault tolerance.

- Pow

- stands for Proof of work.
- It is used to select a miner for the next block gen".
- Requires lot of computational power
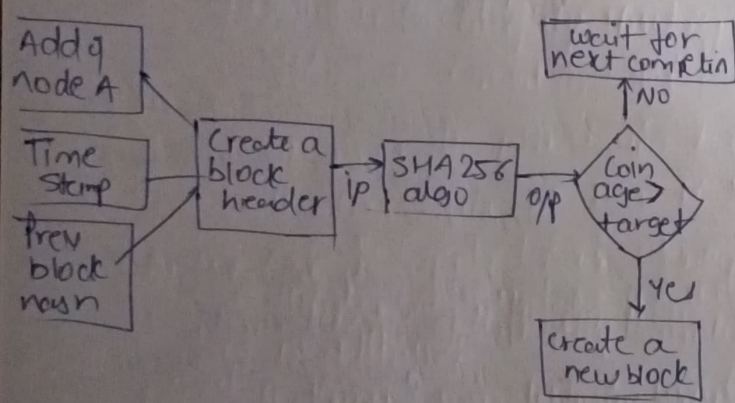- eg. Bitcoin, litecoin.

Block header diagram: Merkle root, Time Stamp, Prev Block hash, Version, Nonce → Create block header (i/p) → SHA 256 algo (o/p) → block hash < target → Yes → Create new block; No → Adjust nonce (loop back)

→ **POS**

- It is stands for Proof of Stake.
- It is most common alternative to POW
- It encourage validators/minners through an incentive mechanism.
- eg. Ethereum, PPcoin

Add g node A, Time Stamp, Prev block hash → Create a block header (IP) → SHA 256 algo (O/P) → Coin age > target → Yes → create a new block; No → wait for next competiton

→ **POA**

- It is stands for Proof of Activity
- It is a Combination of Pow + POS
- It starts with Pow
- Validity will POS
- eg. Decred (DCR)
- Reduces the energy Consumption.

→ **POB**

- It stands for Proof of Burn time.
- Here minners have to burn thein coin which regularly decays.
- Minners send their coins to verifiable unspendable address.
- Minneys earn virtual minning rig by burning the coin.
- eg. Slim coin.
- Does not require energy consumption.

→ **POC**

- It stands of Proof of Capacity
- It is storage oriented
- It stores the result of hash value. low amt.
- Require lot of energy consumption
- Comprises of 2 steps Plotting (stores) Minning (use)
- eg: Burst coin

→ **POET**

- Stands for Proof of Elapsed time
- dev by Intel (2016)
- Permissioned blockchain
- comprises random wait time
- Uses lottery system.

→ **POAT**

- Stands for Proof of Authority
- Permissioned blockchain
- high fault tawlerance
- Only Pre validated node can create blocks
- eg. Alpa

→ POI
- Stands for Proof of Importance
- Modification of POS
- Alternative measures like no. of transaction, size of trn & activity
. Clusters.
- eg. NEM.

Ques what is Smart contract?
- Smart contract are the code which are self-executable
- It act as a bridge between dapps & ethereum platform.
- Solidity language is used by developer to write smart contract.
- It gives the permission & controls the transaction whether it has to executed or not.
- each smart contract is provided by a address.
- Solidity has extension .Sol

Ques what is gas fee & gas limit?
- gas is a smallest cryptocurrency of ethereum recorded in way.
$$1 \text{ gwei} = 10^{-18} \text{ ethers.}$$

- Whenever we write smart contract certain amount of gas fee is deducted from our account as a transaction fees.

- we can mannually select the gas limit in solidity compiler while writing contracts & its also depends upon complexity of Smart Contract.

Ques what is hyperledger & hyperledger fabric?

- It is a Project hosted by Linux Found.
- It comprises of frameworks via we can built blockchains
- It is an open-source collaborative effort created to advance cross-industry blockchain technologies.
- This project includes leaders from finance, banking, IOT, Supply chains, manufacturi & Technology.

Hyperledger Fabric

- It is a private & confidential blockchain framework managed by Linux Foundation.
- Opensource platform for building distributed ledger solutions
- It has enterprise-level permission blockchain network
- For each & every Transaction in the fabric, following steps are followed
  (i) Creation of Proposal.
  (ii) endorsement of transaction
  (iii) Submission
  (iv) updating the ledger.
- It has faster transaction speed & better performance.

Q How does Hyperledger works?

A Hyperledger - based technology works using following layers.

- Consensus layer:
  which makes an agreement on order and confirms if transaction in a block are correct.

- Smart contract layer:-
  It processes and authorizes trans^ requests.

- Communication layer:-
  It manages P2P (peer-to-peer) message transport.

- API layer:
  allows other appl^n to communicate with other

- Identity management:-
  validates the Identity of users of system.

Q use case in Supply Chain Management?

A Some benefits of Blockchain in Supply cm.

(i) More accurate Tracking:- - companies can digitize physical assets & create a reliable decentralized record of transaction.
  - which provide visibility from user end to manufacturing end.

(ii) better transparency:
  - It reduces fraud in Supply chain
  - Transparency in understanding how vital ingredients move from one manufacturer to other.
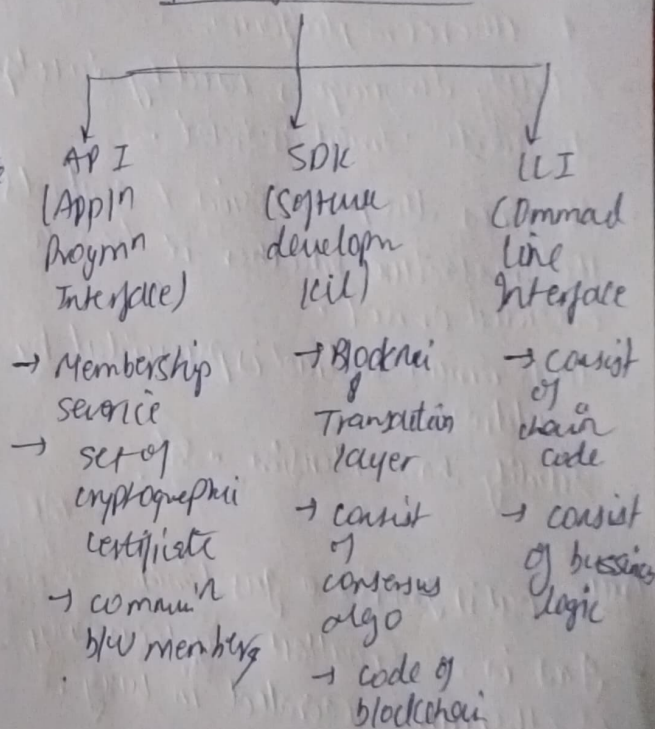
(iii) Contract Manufacturing

- All parties in a supply chain have access to same info.

- Reduce comm^n prob

(iv) Administration

- various administrative process like compliance, audit, credit check all done in distributed ledger.

→ Hyperledger Architecture

API (Appl^n Program Interface)	SDK (Software development kit)	CLI Command Line Interface
→ Membership service	→ Blockchai Translation layer	→ consist of chain code
→ set of cryptographic certificate	→ consist of consensus algo	→ consist of business logic
→ comm^n b/w members	→ code of blockchain	

Blockchain Unit-3

Q.1 what is Desktop wallet & how does it work? list some benefits & drawbacks of desktop wallets.

Ans

Desktop wallets

- software appl^n designed to manage & securely store their private & keys on computer harddrive.

- It provide a streamlined, easy-to-use interface for users to interact with their cryto holdings.

- These desktop wallet are non-custodif which means owner bear sole respo^n for safeguarding their pvt. keys.

- Some popular desktop wallet are: electrum, exodus, Atomic wallet.

Working of desktop wallet:

- It provide users setup with both public & private keys to sign & execute transactions.

- users access their desktop wallet with a simple username & password. like seed phrase or recovery phase.

- Once logged in, users are free to interact with multiple cryptocurrencs across Multiple blockchains.

Benefits!.

- convenient method of securely conducting crypto trans^n using a computer.

- easy to use & free to download.

- Non-custodial

Drawbacks!.

- can be vulnerable to viruses & malware.
- Lack of portablity.
- suspectible to hackers.

Q.2 what is App based wallet explain with example.

Ans - App based wallet is a software/hardware app^n to store your cryptocurrency.

- This is easy to use.
- secure & fast.
- ex = ZenGo, Binance, Coinbase.

ZenGo

- most secure non-custodial.
- Removed private key vulnerablity.
- I^st wallet to offer advanced security features 3FA
- limited range of Cryptocurren

Q. What is Browser or web based wallet. Explain with example. Is Metamask a based wallet?

Ans

- A browser-based wallet or wallet service is an online acc with an external provider where bitcoins can be stored.

- **ex:** - accounts on currency exchange Markets.
  - Online services
  - ecommerce trans" processors.

- Metamask is a popular crypto--currency wallet appl" available in both webbrowser & mobile device as an app.

Q. What is metamask? Write down the steps to create an account in metamask.
- Browser based wallet.
- One of the leading crypto wallet.
- Metamask is a cryptocurrency wallet that enables users to store ether & other ERC-20 token
- Also used to interact with decentralized appln or dapps.
- we can create multiple accou within same account.
- It relies on browser integration & good design to serve as as one of the main gateway to the world of webs., (Defi) decentralized finance & NFTs.
- we can also import other account from ur browser using private key.

Steps to create Acc on metamask.

1- Download & Install official Metamask extension.

2- Upon seeing Splash screen, click 'Get Started' button to begin creating your ethereum wallet using metamask.

3- click "Create an wallet".

4- Pick a Password.

5- Metamask will then present you with your 12-word backup phrase. This 12-word phrase will work as your recovery wallet.

6- Confirm your backup phrase & confirm once done.

7- we can create multiple acc withi same acc. or import acc.

Q. What is faucet in wallet? Briefly discuss the use of faucet to fund wallet?

Ans

- Faucet stands for the meaning rewards which are small, just like small drop of water dripping from faucet.

- In the case of crypto faucet, tiny amount of free or earned cryptocurrency are sent to a user's wallet.

- Most faucet wallet will have min threshold.

- Allows to collect small amt of cryptocurrency with little to no effort.

Q what is Ethereum & How does it work?

- It is a decentralized global software platform. (ETH)
- Scalable, programmable, secure, & decentralized.
- Natively supports Smart Contracts.
- Ethereum changed from Proof-of-work to proof of-Stake.
- It is the foundation for many emerging technological advances based on blockchain.

—— || ——

- It works on Roof-of-Stake Mechanism.
- It uses finalization protocol called Casper-FFG & algo LMD Ghost combined into consensus mechnasim called Gasper.

- validator who act dishonestly are punished under proof-Stake

- Validators who attempt to attack the network are identified by Gasper.

Q How does Ethereum Makes Money? Is ethereum a Cryptocurrency?

Ans - ethereum not a centralized organization that makes money.
- validator who participate in the ethereum network earn ETH reward for their contribution.
- ethereum has two accounts ① externally owned acc.
② Smart contract acc.

(I)
- ethereum platform has a native cryptocurrency, known as ether, ETH.

- Ethereum itself is a blockchain technology platform that supports a wide range of dapps.

- The ETH coin is commonly called ethereum.

—— u ——

→ **Q** what is Remix IDE.

- It is an Integrated development environment which gives us a medium or platform to write smart contract.

- Remix is easiest and quickly way to deploy smart contract.

- It comprises of featured plugin which helps to deploy smart contract under plugin manager.

- All the smart contract written in solidity are provided with address and run in Remix IDE.

- IDE can be found in remix.ethereum.org.

- we can manually select the version of compiler under solidity compiler.

Q Explain different kinds of ethereum network?

→ Ethereum network are diff environment used for development testing, or production.

→ It is mainly categorized into 2
- Public network
- Private network

Private

Development network
- designed specifically for local development & implementation of ethereum.
- eg. Ganache
- used to test dapp.

Consortium network
- It is like a Private Intrenet
- network is controlled by pre-defined set of rules.

Public

ethereum Mainet
→ Primary Public ethereum Production blockchain
→ Actual transaction Occurs.
- For appln development
- Fast to Sync & running a node require minimal storage.
- testing of validating & Staking ←Goerli
- longer to Sync & requires more storage.

ethereum Testnet
→ used by blockchain developers to test protocol upgrades.
→ ETH is required in testnet.
→ which can be taken from faucet funds like Rinkey & Goerelli.
→ Some testnet are ←Sepolia