

- ⑦ Transaction Complete → Then the transaction is finally complete

### Q3. Blockchain Consensus Mechanisms

There are different kinds of Consensus Mechanisms each of which work on different principles

- The proof-of-work (PoW) is a common consensus algorithm used by the most popular cryptocurrency networks like bitcoin and litecoin

It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain.

However, this whole mining mechanism of bitcoin needs high energy consumption and a longer processing time.

- The proof-of-stake (PoS) is another common consensus algorithm that evolved as a low-cost, low-energy consumption alternative to the proof of work (PoW) algorithm.

It involves the allocation of responsibility of maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held by it.

However this comes with a drawback

It incentivizes cryptocurrency hoarding rather than spending.

- While POW and POS are the most prevalent consensus algorithms in the blockchain space, there are other consensus algorithms too.

For example, Proof-of-Capacity (POC) which allows sharing of memory space by all of the contributing nodes on the blockchain network.

The more memory or hard disk space a node has, the more rights it is granted to maintain the ledger.

- Proof-of-Activity (POA), used in Decred blockchain is a hybrid that makes use of aspects of both POW and POS consensus algorithms.

- Proof-of-Burn (POB) is another consensus algorithm that requires transactors to send small amounts of cryptocurrency to inaccessible wallets, in effect, "burning" them out of existence.
- Another called Proof-of-History (POH), developed by Solana Project and similar to Proof-of-Elapsed Time (POET) encodes the passage of time cryptographically

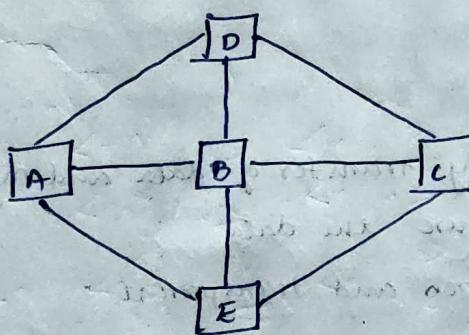
This helps achieving consensus without expending many resources.

- crypto economics model
  - Types of Block chain
  - consensus mechanism
- Bitcoin ethereum
- mining and validation
- hashing and digital signature
- layers of Block chain.

## ① Block chain and types of block chain:-

- Block chain technology is one of the latest and leading data base storage model in modern generation
- Block chain model contains blocks of individual data elements (or) groups of people data elements which are interlinked using nodes.
- By the help of this model. We can easily able to transfer the data from one node to another node. and that exchange data from one block to another block.
- Block chain model is the base for UPI transactions.

### Types of Block chains



→ This is a basic block chain structure where each blocks are connected to each other and transfer the data across the blocks.

Block chain technology is mainly developed for blockchain bitcoin technology and UPI transactions to make secure.

so they have classified block chain into ~~these~~ four major types.

- Public Blockchain
- Private Blockchain
- hybrid Block chain
- Consortium Block chain

## ② public block

### ① Public block chain:-

- It is a permissionless, non - restrictive block chain distributed technology.
- Any one with internet connectivity can sign up to that block chain model and make themselves one node of block chain process.
- each peer of node have distinct address and by address the data transfer takes place.

### advantages:-

- easy transfer of data and maintenance
- Secure the data
- open and transparent

### disadvantages:-

- each and every transaction is transparent we need to maintain proof of work
- Security part is the main issue in public block chain

## Private block chain:-

- It is a permission (or) request based block chain model where each block should ask request to another block to access the data.
- It is one customized model with some people can only access this data and with third party network no other people are allowed inside.

### advantages:-

- ① Speed of data processing is high as less people are available.
- ② security of the model is high and volatility increases.
- ③ Backup should be maintained and payslips are not required.

### disadvantages:-

- ① cost of making the block model is high.
- ② high use of power and maintenance.
- ③ scalability is less.

## hybrid block chain:-

- It is a combination of both private and public block chain model and they are interconnected.
- To access some blocks permission is required and to access both request and permission are not required.
- The volatility of data transfer and maintenance decreases.
- with public network we can directly get into block chain structure.

### advantages:-

- easy maintenance
- data transfer speed increases
- Security of the model is much developed than

### Private block chain

### disadvantages:-

- less scalability
- less volatility and should maintain some customised blocks
- Non-scalability.

### consoritium Block Chain:-

- It is a development of hybrid block chain and it is called decentralised block chain
- In this, various organisation can collaborate and be a part of complex model of block chain
- This is easy in developing complex block chain structure with scalability.

### advantages:-

- ① easy maintenance
- ② more data accessibility at single place
- ③ data transparency and redundancy.

### disadvantages:-

- ① More power consumption
- ② maintenance is difficult as complex structure and should maintain proof of work.

## (2) Crypto & economics model:-

- crypto economics state the study of economic interactions
- economic transactions are difficult to do in p2p network processing model as no person and server acts as centralised data maintenance part.
- so by block crypto economics model we can able to do transactions easily and securely.

### mechanism of crypto & economic model

① proof of work:- It is a consensus mechanism of the Bitcoin network similar to block chain.

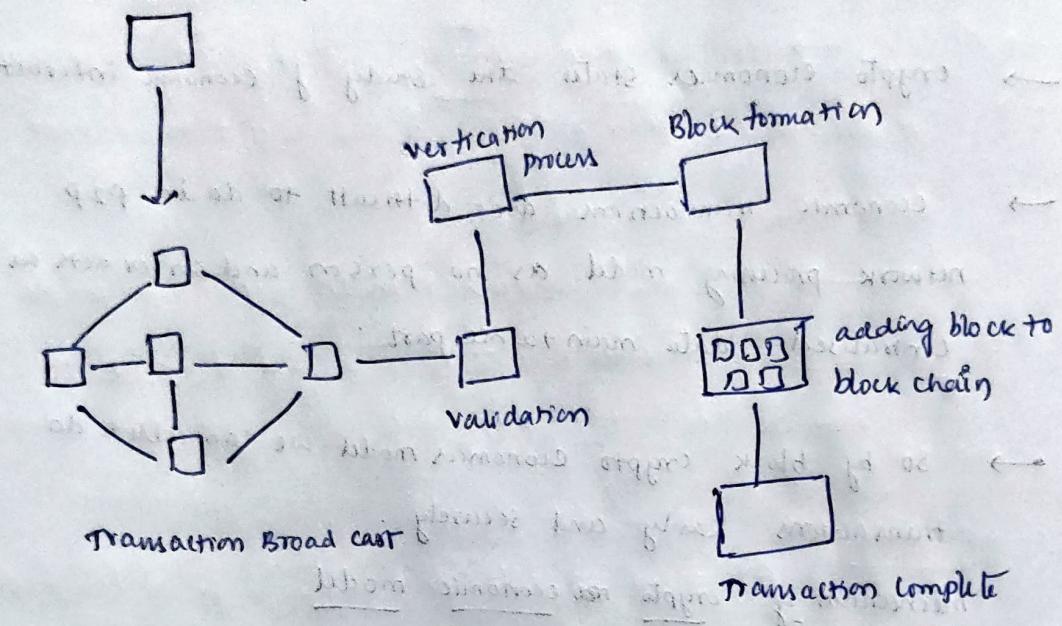
→ It is a set of rules and processes that define the multiple nodes aggregate on true state network.

→ As there will be proof of work there is no way to skip the transaction, pay slip and the money (or bitcoins) are secure.

### Crypto economic model:-

- transaction Request
- Transaction Broadcast
- Transaction validation
- verification process
- Block formation
- Adding the block to block chain
- Transaction complete

### Transaction Request



→ Transaction Request- Transaction Request states that activating processes of transaction. To accomplish transaction we should have wallet and that contains money and bitcoins model.

### → transaction Broadcast-

- As the request is broadcasted over various computers connected in p2p model and which person accepts the request get the notification
- now the both Requests get connected to some Primary network and that is first written in Proof of work.

### → validation-

- As the user accepts the Requests the system by default check the validation and authentication of the request sent
- As all the nodes are linked the validation checks for connectivity and encrypts the data

## → Verification process:-

- Verification process helps in checking both the sender and receiver are properly connected to data lines
- Previous history of both the transactions done before.
- Verification is done then block formation gets enabled.

## → Creating a Block:-

- As the transaction request is formed the Request Sender is now made into block and thus help in tracking transactions by ledger

- The ledger authenticates and complete the transactions
- Adding the block to the block chain:-

- Now this block transaction is added to the central block chain as the transaction status is stored
- The updation of values from changing money is in blocks of transactions is maintained at block chain central model
- With this entire proof of work statement is developed with all the attributes and requests.

- Transaction Complete:- After completing all the processes it gives us transaction complete