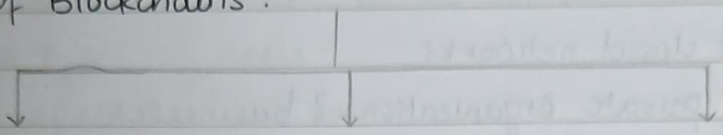
UNIT 3
Blockchain Platforms & Consensus In Blockchain

★ Types of Blockchains.



1) PUBLIC BLOCKCHAIN. (Bitcoin, Ethereum)

- open to public
- not owned by anyone.
- Anyone can participate as an node in the decision-making process.
- users may or may not be rewarded for participation.
- non-restrictive
- anyone ~~can~~ with internet access can sign on a blockchain platform to become an authorized node.
- anyone can access current & past records & conduct mining activities
- no valid record / transaction can be changed on the network
- anyone can verify transactions, find bugs or propose changes as source code is open source.

• Advantages.

1) completely independent of organizations. Even if organization ceases to exist the public blockchain will still be functional until computers are connected to it.
2) Network transparency - as long as users follow safety protocols, public blockchains are secure.

• Disadvantages:

1) network can be slow as access is not restricted
2) If hackers gain more than 51% of power of blockchain network, they can

alter data in the blockchain.

3) don't scale well. network slows down as more nodes join the network

2) PRIVATE BLOCKCHAIN.

- operate on closed networks
- useful for private organizations & businesses.
- open to only a group of individuals or organizations which decide to share the ledger.
- companies can used private blockchains to customize their authorization preferences & accessibility, parameters to the network, other security options etc.
- managed by only one authority.
- also known as permissioned enterprise blockchain.

• Advantages.

1) controlling authority sets permission levels, security, authorization & accessibility.
2) fast, as users & nodes are limited.

• Disadvantages.

1) difficult to put trust in the information as it is validated by the central node.
2) Less nodes means less security. Consensus can be compromised if few nodes go rogue
3) source code is closed & proprietary.
4) no anonimity.

3) CONSORTIUM BLOCKCHAIN.

- have both private & public components.
- multiple organizations will manage a single consortium blockchain network

- set up is complex but offer better security.
- optimal for collaboration with multiple organizations.
- consensus procedures are controlled by preset nodes.
- has validator nodes which validates, initiates & recieves transactions.
- member nodes can reciere or initiate transactions.
- has two types of users:

1) who can access the blockchain
2) who have control over who can access the blockchain.

- **Advantages**

1) more scalable, secure & efficient than public blockchain network.
2) offers access controls.

- **Disadvantages**

1) less transparent than public blockchain.
2) can be compromised if member node is breached.

Features	Public	Private	Consortium
Accessibility	Anyone	central authority	more than one incharge
Who can join?	Anyone	permissioned and known identities	Permissioned & known identities
Consensus mechanism	PoS/ PoW	Voting/ Multiparty consensus algo.	Voting or multi-party algorithm.
Transaction speed	slow	Lighter & faster	Lighter & faster
Decentralization	completely decentralized	less decentralized	less decentralized.

★ BITCOIN

- first application of blockchain technology.
- first cryptocurrency in the world.
- introduced by Satoshi Nakamoto in 2009.

• **Working**

- for using bitcoin, create an account.
- create a digital wallet on Bitcore, Coinbase etc.
- while creating the account, user has to provide a 'key' (password)
- by using the key, wallet generates a valid bitcoin Private key-Public key pair.
- public key is visible to all, & is the account ID of the user.
- private key is kept by the user to access the account.
- if a person loses his private key, he loses the access to his acc. & his money.

• **Bitcoin mining.**

- process by which new transactions are validated & added to the blockchain.
- miners → nodes who participate in the process.
- when transaction takes place, it is broadcasted on the network.
- miners engage in the transaction verification
- once the transactions are verified they are added to the block permanently.

• **What do miners do?**

- The mission is to find hash value for the new block.
- The miner who finds it first is rewarded with some bitcoins called block reward
- Anyone can find a hash value, it is not a big deal.
- & Difficulty level is associated with it to make the nodes compete with each other.
- Difficulty level is specified in terms of no. of zeros,.

- The miner has to find out hash value with specific no. of zeros.

* **Lifecycle of bitcoin transaction.**

Someone requests a transaction → Transaction broadcasted to P2P computers (nodes) → Miners validate the transaction

↓

Transaction is complete. ← New Block added to existing Blockchain ← Transactions combined to form a data block

* **Value of Blockchain Bitcoin**

- Value of bitcoin depends on demand & supply.

  T = Total bitcoin transaction / second

  D = Duration that a BTC needed by transaction.

  S = Supply of the bitcoin

  P = Price of the bitcoin.

  S/D = Bitcoins available per second

  T/P = Bitcoins needed per second.

- According to the demand-supply rule,
  when supply of bitcoin ↑, demand ↓ consequently & so does the price of the bitcoin
  when demand ↑, supply of bitcoin ↓, price ↑.
- Equilibrium state

$$\frac{S}{(D)} = \frac{T}{P}.$$

$$P = \frac{TD}{S}.$$

- ✱ strictly based on user transaction.

* Advantages

1) Protection from Payment Fraud.
Bitcoins are digital currencies which use algorithm & cryptographic protocols which makes it impossible to counterfeit.

2) Reduced possibility of Identity ~~threat~~ theft.
Bitcoin transactions are anonymous & do not require personal details.

3) Immediate settlement.
Bitcoin does not involve third party & hence funds cannot be put on hold or refunded

4) Direct transfer.
No third party involved, transaction takes place between the sender & reciever.

5) International Transactions.
Bitcoin is the easist method to initiate an international transaction Does not charge extra fees.

6) Security
Bitcoin payments have very strong security & it is impossible to counterfeit.

7) Transactions are tamper-proof.

* Disadvantages.

1) Scams & frauds
Fake websites & apps are selling bitcoin & fooling people

2) Blackmarket activity.
Due to complete anonymous feature, bitcoin is used in cyber hacking, drug deals & black market arm deals.

3) Price volatility.
The price of Bitcoin is volatile.

4) No refund.
Once payment is initialed it cannot be held & refunded.
Takes place directly betⁿ sender & reciever.

5) Cyber hacking

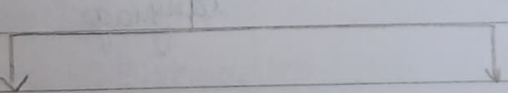
Hackers & illegal ransomwares use bitcoin as a payment system to extort money from the money to maintain anonymity.

★ ETHEREUM.

- Ethereum is Open source Blockchain platform.
- ~~It uses allows anon~~
- It allows anyone to develop & deploy Blockchain-based application.
- applications including cryptocurrency, wallet, tokens, social apps can be developed & deployed.
- not a single network, it is a protocol for inter-network communication.
- Many networks exist alongside.
- Ethereum like WWW brought all blockchain functionalities in a single network & avoided creation of individual blockchains for each purpose.

. How to be a part of Ethereum?

- Users.



- Every user having an account on Ethereum, ~~are~~ called Externally Owned Accounts.
- Every Dapp has an account address in ethereum called contract account.
- User can make transactions from Exterally owned Accounts as well as contract account.

- Dapp is Decentralized App running on the blockchain.
- They run on blockchain without any centralized control.
- Dapp uses shared ledger instead of server to record & store all the transactions.
- Dapps have backend code as well as user-interface.
- Backend codes contain smart contracts
- user-interface is for the user to interact with blockchain.
- smart contract deployment on blockchain → Dapp accessible in blockchain

then anyone on the blockchain can use the Dapp.

	Bitcoin	Ethereum.
1)	Bitcoin is a currency.	Ethereum is a computing platform
2)	Bitcoin is limited & there will be a total of 21 million bitcoin in production.	Ethereum supply is unlimited.
3)	Bitcoin is simple.	Ethereum has rich programming language.
4)	Smart contracts are not present	Smart contracts are written in Solidarity.
5)	Bitcoin runs on SHA-256 Hash Algorithm	Ethereum runs on Keccak-256 hash algorithm.
6)	The bitcoin community is large.	It has a smaller community.
7)	POW is the consensus mechanism used.	POS is the consensus mechanism used.

* HYPERLEDGER

- open source collaborative effort created to advance cross-country industry blockchain industry.
- global collaboration hosted by Linux Foundation including leaders in finance, banking, IOT, supply chains, manufacturing & technology.
- framework to create, deploy & maintain blockchains for businesses that ensure transparency & trust bet^n business partners
- Hyperledger permits permissioned & private transactions
- It is highly scalable.
- Hyperledger is not a blockthain platform.
- It is a consortium of organizations
- Hyperledger projects are vendor neutral, & can be deployed in products & solutions by any company anywhere in the world.
- Hyperledger Architecture has the following components:

i) Consensus Layer
Responsible for verifying blocks of transactions & agreeing on their order

ii) Smart contract Layer
responsible for transaction processing.

iii) Communication Layer
Responsible for P2P transport.

iv) Data store Abstraction
Responsible for different data-stores which can be used by other models.

v) Crypto Abstraction.
responsible for crypto algorithms.

vi) Identity service.
enables the establishment of a root of trust during setup of a blockchain instance, the enrollment & registration of identities during network operation & authentication & authorization.

vii) Policy Service
responsible for policy management.

viii) APIs required for interactions with applications.

* Hyperledger Foundation hosted projects.

1) Fabric.
- developed by Digital Asset & IBM.
- foundation for developing blockchain applications, products or solutions.
- private & permissioned system.
- delivers high degree of confidentiality, resilience, flexibility & scalability.
- Fabric has ledger & smart contract
- smart contract → chaincode.
Business logic is embedded in chain code.

2) Aires.

3) Iroha
- emphasis on mobile application development.
- written in C++
- built for high performance use-cases such as embedded systems

4) Sawtooth.
- contributed by Intel
- comes with support for permissioned & permission-less deployments.
- can use different consensus algorithms.
- uses Proof of Elapsed Time consensus.

5) Indy
- still under incubation
- developed to support independent identity on distributed ledgers.
- does not support smart contracts.

6) Burrow

7) Grid

8) Cello.

★ IOTA - Internet of Things Angles.

- IOT is a network of physical objects & devices such as gadgets, home appliances that can connect, exchange info with multiple devices in real world without the human need-to-human interaction
- IOTA is an open source, decentralized, highly scalable Decentralized Ledger Technology (DLT), designed to support frictionless data transport / transfer across network.
- IOTA empowers businesses to build IOT solutions using its open source IOTA framework & tech stacks.
- IOTA is a 'block' less Blockchain.
- It provides blockchain for IOT Products.
- does not have ~~blocks~~ chain of blocks.
- uses the concept of Directed Acyclic Graphs (DAG)
- DAG is a directed graph without cycles.
- IOTA protocol is also known as Tangle
- Tangle is DLT, provides features similar to blockchain
- IOTA Tangle is open source, feeless, scalable & light weight DLT.
- In Tangle,
  - vertices of graph → physical devices
  - edges directed from one vertex to another → transaction.

★ Features

1) It is scalable.
   - Tangle allows multiple gadgets to connect & communicate with each other at the same time.
   - IOTA supports parallel transaction processing.
   - IOTA can process 1000 transactions per second which is faster and more efficient than Bitcoin & Ethereum.
2) IOTA is feeless.
   - Before adding to the ledger, transaction fee is required for verification

& validation of transactions which can be unpredictable.
- IOTA's protocol is freee of transaction fees.
- IOTA is designed to manage Nano transactions & won't charge any transaction fees.

3) No miners in IOTA Network.
- No miners or mining process is involved in IOTA Network.
- Verification is done by the node itself who generates the transaction with a validation algorithm.
- Before that, the node has to validate two other random transactions in the network using the same validation algorithm.

4) Quantum Proof Security
- uses Masked Messaging Technique for data security & maintaining data integrity.
- Data transfer through the IOTA tangle is encrypted & thus protected from external attacks.

5) IOTA is flexible
- Many DLTs are either private or public ledgers.
- IOTA is flexible & enables both.

R3 Corda.

- Corda is a distributed ledger technology which is neither completely decentralized nor fully transparent blockchain.
- Corda aims to build a financial ecosystem where corporates & multinational companies participate to bring transactions directly into business using smart contract privacy features
- Issues regarding privacy, identity, transaction fees, cumbersome paper work etc are resolved in enterprise blockchain.
- Corda is an Enterprise Blockchain.
- Corda provides a network of blockchain for banks, supply chain, finance, insurance industries etc.

- helps to maintain shared ledger of transactions by eliminating the need for the involved parties that constantly check their transactions after every interaction.
- Corda is a private blockchain where trusted parties have their own identity & & license.
- It has Oracle & SQL server database integration.

* Features

1) Open source - Open source platform built on JVM
2) Data Privacy - provides a significant feature where transactions are private.
3) Developers Community - rapid growth in technology by inculcating new features & functionality.
4) Scalability - Corda is flexible platform designed to scale with business needs.

* Consensus in Blockchain.

- primary part of blockchain technology.
- used to guarantee ~~tat~~ that the "main chain" at every node is the same.
- results in consistent state of the blockchain across all nodes.
- they guarantee that a state, value or piece of information is correct & agreed on by most of the nodes.

* Objectives.

1) Fair & Equitable.
- consensus mechanisms enable everyone to participate in the network & use the same fundamentals.
- justifies the property of open source & decentralization.

2) Unified agreement
The protocols in the network make sure that the data is genuine & accurate & status of ledger is up-to-date.

3) Alignment of economic incentive
A consensus blockchain protocol rewards good behaviours & punishes bad actors.

4) Prevention of double spending.
Consensus ensures that transactions which are verified & validated are present in the public transparent ledger

5) Fault tolerant.
Consensus ensures block-chain is fault-tolerant, consistent, tested & reliable.

---

* Types.
1) Proof of Work (POW)
2) Proof of Stake (PoS)
3) Practical Byzantine fault tolerance (PBFT)
4) Delegated Proof of Stake (DPOS)
5) Proof of Burn (PoB)
6) Proof of Activity (POA)
7) Proof of authority.
8) Proof of Elapsed Time (PoET)
9) Proof of Weight (PoWeight)
10) Proof of Trust (PoT)
11) Proof of Capacity (PoC)
12) Proof of Importance (POI)

---

* Why is consensus needed?
- When a transaction occurs, it is validated by some nodes.
- After verifying validity, block holding transaction is added to the chain which can be identified by all other nodes.
- A node can append a block by distributing it to another node which has requested to add the block to current chain.
- If every node requests it's preferable node, then it will

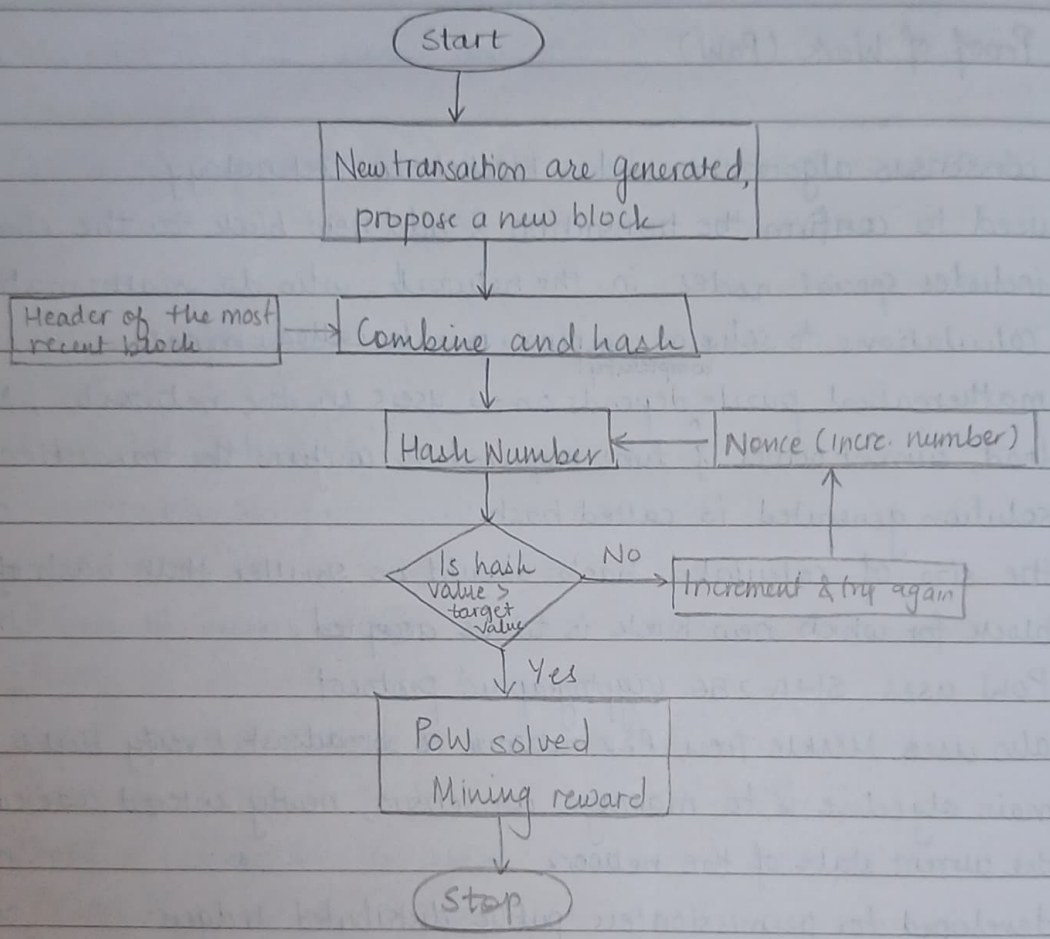
create a chaos in the system.

- To prevent this, consensus algorithm is introduced which holds agreement made betⁿ all nodes about which blocks should be appended.

★ Proof of Work (PoW)

- consensus algorithm used in blockchain technology.
- used to confirm the transaction & add new block to the chain.
- includes special nodes in the network who do mathematical calculations to solve a complex puzzle called miners.
- mathematical puzzle depends on (complexity) → users in the network, network load, current power & time required to confirm the transaction.
- solution generated is called hash
- the size of calculated hash should be smaller than hash of the block for which new block is to be accepted.
- PoW uses SHA-256 cryptographic protocol.
- also uses Merkle Trees, P2P network to broadcast & verify blocks.
- main objective is to manage consensus, newly entered code can detect the current state of the network
- developed for permissionless public distributed ledgers.
- consumes more computational resources
- to construct a new block, miner hash to solve a cryptographic puzzle & the user who solves the puzzle first will avail the reward by broadcasting the result in the network.
- protocol maintains transactions in a block in a linear fashion.
- cryptographically signed transaction will be accepted only if signature is validated & verified in the network
- protocol fairly dishibutes # a reward.
- presents mining that involves a step for validation of block in the network by providing computational proof of completed work.

- Once transaction is started, available miners in the network compete to find the solution of cryptographic puzzle & form the block.
- The solution of the block is broadcasted by the miner who solves the puzzle & solution is verified to make new block on the chain.

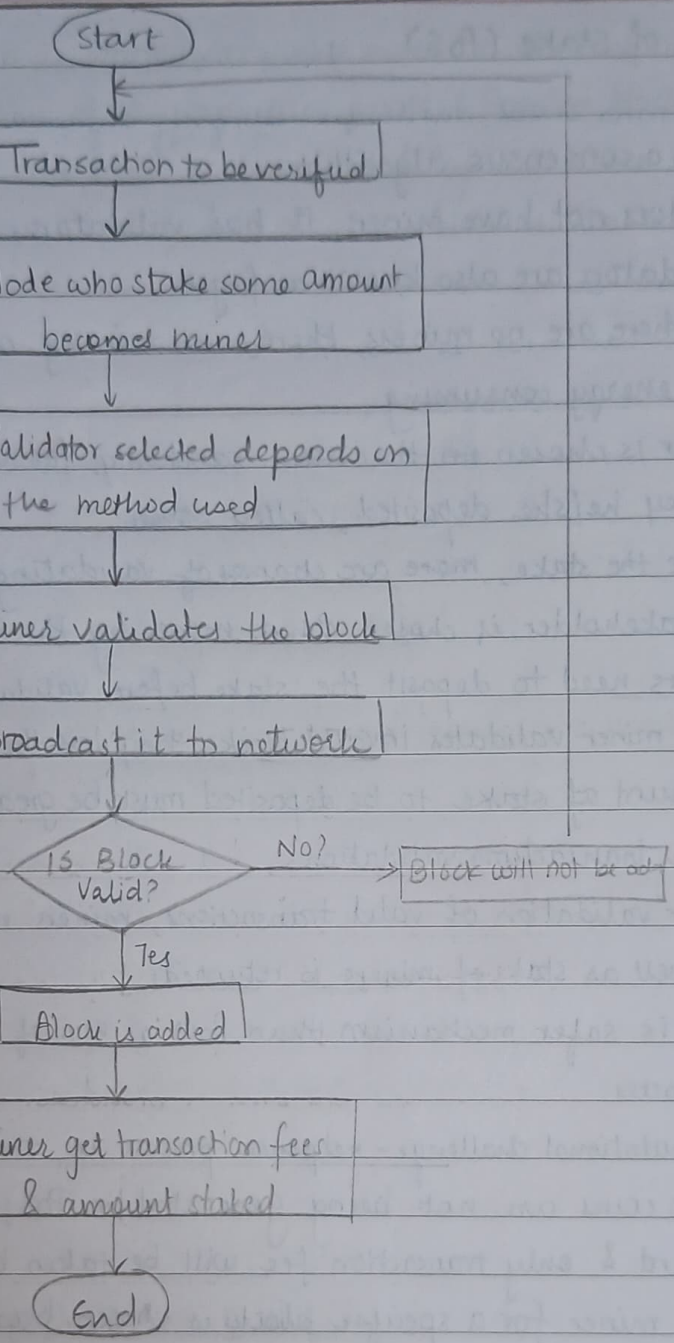


* Disadvantages

1) power-consuming protocol
2) requires vast amount of computation power.
3) difficulty level increases & along with it power reqd. also increases.
4) extremly vulnerable to Dos attacks, Sybil attacks etc.

Proof of Stake (PoS)

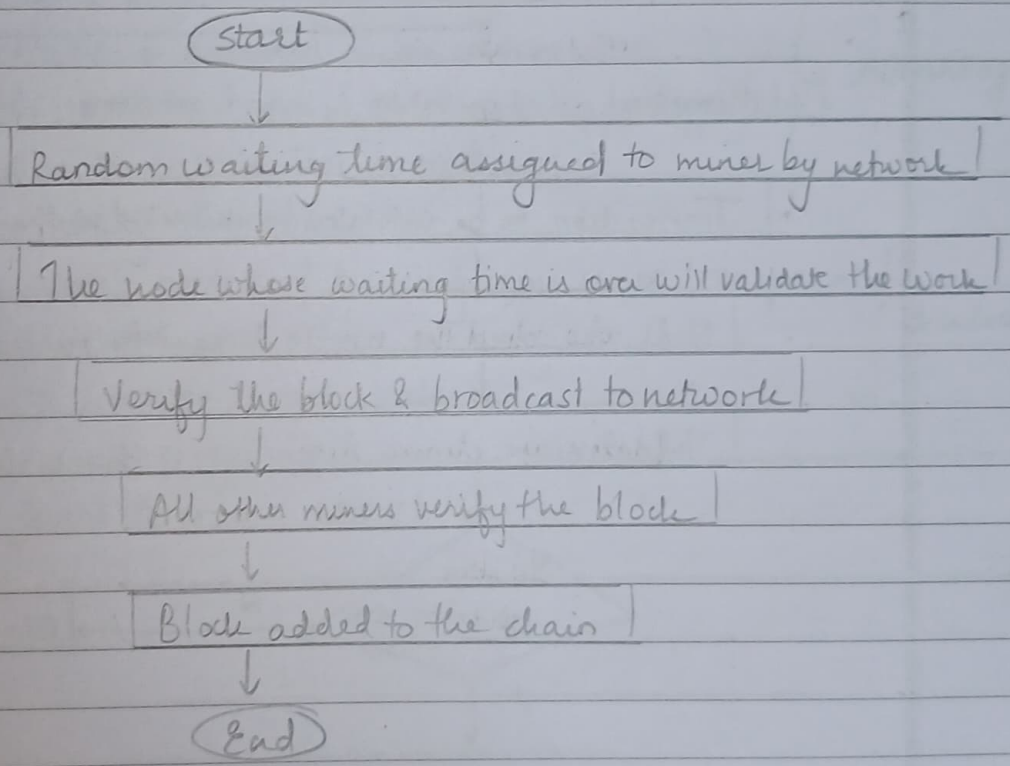
- It is a consensus algorithm
- It does not have miners, it has validators
- Validators are also known as forgers.
- as there are no miners, there is no mining competition & therefore less energy consuming.
- miner is chosen ~~on the basis~~ randomly for validation which depends on money he/she deposited, called stake.
- more the stake, more are chances of validating transaction
- a stakeholder is chosen as a miner by the network.
- miners need to deposit the stake before validating the transaction.
- if a miner validates invalid block, they lose the deposited money.
- amount of stake to be deposited must be greater than the reward recieved after transaction validation.
- after validation of valid transactions, miners recieve the transaction fees as well as stake of miners is returned.
- PoS is safer mechanism than PoW as 51% of a network needs to be owned by hacker.
- computational challenge-response process in the protocol is minting.
- new coins are not being generated in PoS, hence there is no block reward & only transaction fee will be taken by the miner in PoS.
- The miner for a specific block is chosen based on the economic stake in the network
- Ethereum is influenced by PoS to reach consensus.
- Other cryptocurrencies → Peercoin, Navvcoin, Dash, Pivx etc.
- PoS is eco-friendly protocol as it requires negligible amount of computation.
- does not need specialized hardware for ~~activation~~ active participation.
- it is energy efficient.



★ Proof of Elapsed Time (POET)

- private blockchain consensus algorithm.
- lottery system followed for choosing miners.
- Random waiting time slot is provided to the miners.
- After waiting time is finished, miners can mine the block.
- During random waiting time, miner's processor can go to sleep, hence

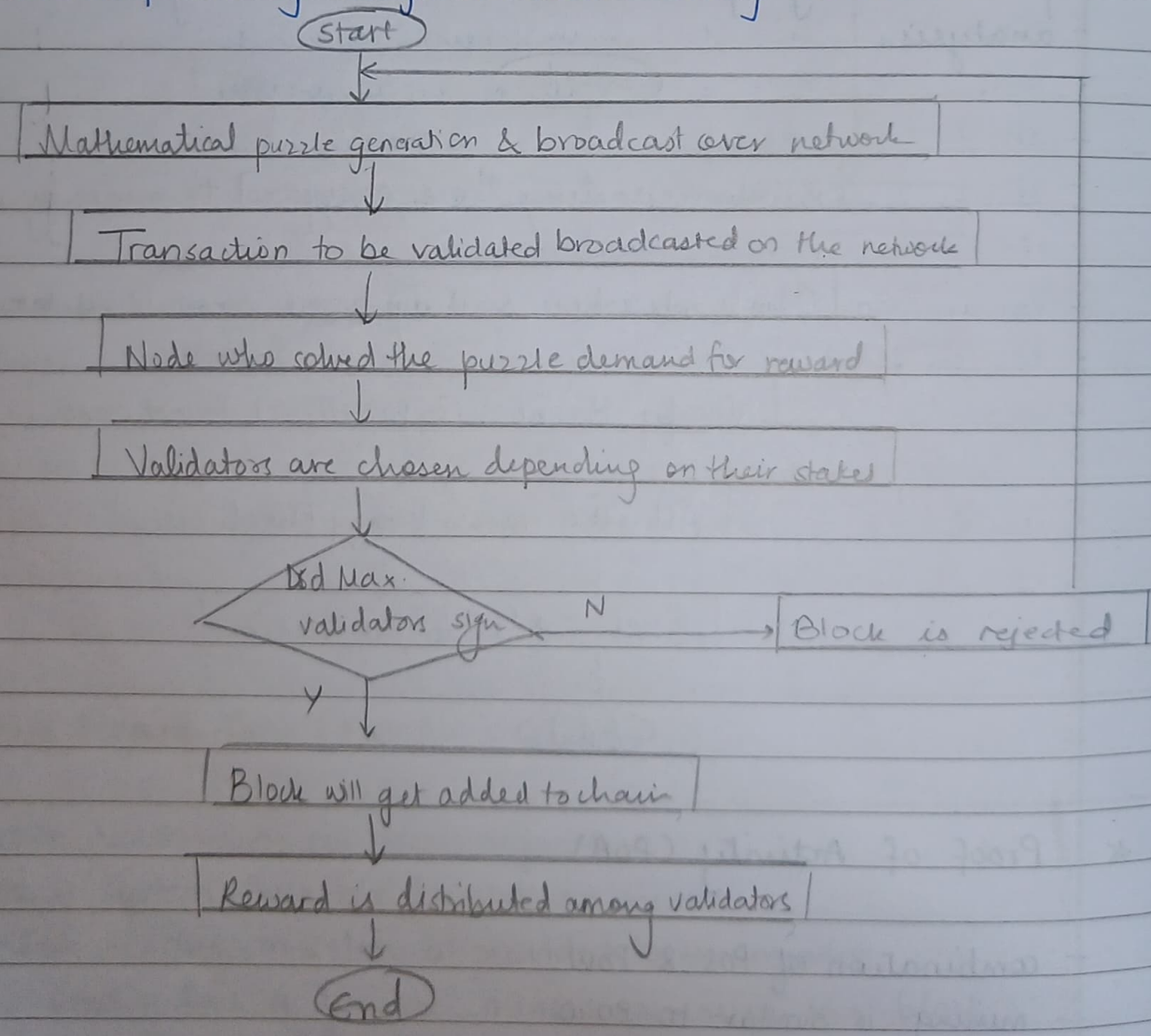
increasing efficiency of the system.
- uses Intel based hardware which is designed for ~~private distri~~ public dlts.
- participants & transaction logs are transparent & sustainable.
- In the PoET protocol,
  - each validator is assigned a random 'T' time to construct the block & is tracked by it.
  - creation of the block in the network is done by the validator who has successfully completed waiting time
- protocol follows both first come first serve & random lottery scheme.
- protocol is highly vulnerable to various security attacks & lacks security analysis.



★ Proof of Activity (PoA)

- combination of PoS & PoW.
- mining is similar to PoW.
- mathematical puzzle is generated & broadcasted over the network

- miners try to figure out the puzzle.
- first node who solves the puzzle demands reward.
- diff. bet^n PoW & POA is block does not contain any transaction, they are simply templates with header information & mining reward action
- after mining PoA follows PoS protocol
- content in a block header is used for random selection for group of validators to sign up the block
- The nodes having largest no of stake validates the block.
- After the block is is signed by all validators it is added to the chain
- If it gets rejected by some of the validators, it is not added.
- The reward for adding will get distributed among validators.



★ Proof of Burn (PoB)

- implemented to avoid double spending attacks
- also called PoW without wasting energy.
- follows principle of burning of coins & getting the right for mining.
- miners get the chance of mining by burning the coins which are proportional to the no. of coins burnt.
- depending upon no. of coins burnt, miners can buy a virtual mining rig which gives the right to validate the block.
- Miners send money to unspendable address for burning.
- used by slimcoin.
- Encourages long term commitment by miners
- More sustainable & reduced power consumption
- coin burning tends to reduce the circulating supply
- coin distribution tends to be less centralized

Advantages

- No need for mining hardware
- For an avg. user, process of burning coins is not transparent
- not as fast as PoW
- not proven to work on larger scales

disadvantages

★ Byzantine Fault Tolerance (BFT)

- Byzantine General's Problem was formed in 1982 as a logical dilemma
- It illustrates how a Bz group of Byzantine generals may have a communication problem when trying to agree on their next move.
- The dilemma assumes that each general has its own army & & each group is located in different locations across the city we they need to attack.
- generals require to agree on either retreating or attacking.
- makes no difference whether they attack or retreat as long as all of them agree on a common decision
- We may consider the following requirements:

1) Each general needs to decide whether to attack or retreat
2) once decision is made it cannot be changed
3) all generals have to agree on the same decision & execute it in sync.

- generals communicate through messages which are forwarded by a courier.
- messages somehow get delayed, destroyed or lost.
- even if message is delivered successfully, one or more generals may decide to act maliciously & send a fake message to confuse other generals, leading to defeat
- applying this dilemma in context with blockchain, each general represents nodes needed to reach consensus.
- only way to accomplish consensus is by having 2f+1 honest & reliable working nodes, f = malicious/defective node.
- defective node sends attack message to 2 nodes & retreat message to 1 node
- All three nodes broadcast the message that they recieve so that non-faulty nodes recieve more no of attack messages than retreat & they decide to attack & & consensus is reached.
- BFT is able to continue operating even if some nodes act maliciously & fail.
- Used by Hyperledger Blockchain

UNIT-4

CRYPTOCURRENCY : BITCOIN & TOKEN.

★ Fiat Money

- money with no intrinsic value but made legal tender by a government order
- it is backed by tangible like silver, gold but fiat money is dependent on the creditworthiness of the government that issues it.
- it is a physical currency.
- it is not backed by a physical commodity but by the trust of its holders & authority of a government decision.
- Paper money serves as a medium of storage for purchasing power & alternative to the barter system.
- The value of fiat money depends on how a nation's economy performs.
- A country undergoing political unrest is likely to have a weaker currency & higher commodity prices.
- People can make plans & create specialized economic activities with ease because of its ability to store purchasing power.

• Advantages

- value stability.
- due to normal business cycle & recurrent recession, comodity based currencies were volatile.
- central banks have the ability to issue & hold paper money as needed, providing more influence over money supply, interest rates & liquidity.

★ Bitcoin.

- first application of blockchain.

- first cryptocurrency.
- invented in 2008.
- collection of concepts & technologies that form the basis of a digital money ecosystem.
- Units of currency called bitcoin are used to store & transmit value among participants in the bitcoin network.
- consists of P2P (Peer-to Peer) decentralized network, a public decentralized ledger (Blockchain), a set of rules for independent transaction authenticitycation & currency issuance & a mechanism for reaching global decentralization consensus.
- A valid blockchain follows the exact structure of a ~~BTC~~ typical blockchain with a P2P shared network, distributed ledger and cryptographically protected data.

• Working.

- user can start working with bitcoin by creating a bitcoin wallet.
- Coinbase & Bitcore can be used to create a wallet.
- A public key & private key is required to create an account.
- ~~private~~ Public key is visible to anyone.
- private key is visible & known to the user only.
- If a person loses private key, he loses his money & access to account.

• Buy bitcoin.

- easiest way to own bitcoin is to buy bitcoin from bitcoin exchange.
- variety of online bitcoin exchanges available which exchange bitcoin for normal money.
- people can use normal currency to exchange it for bitcoin & move it to their wallet.
- another method is bitcoin mining.

• Transaction.

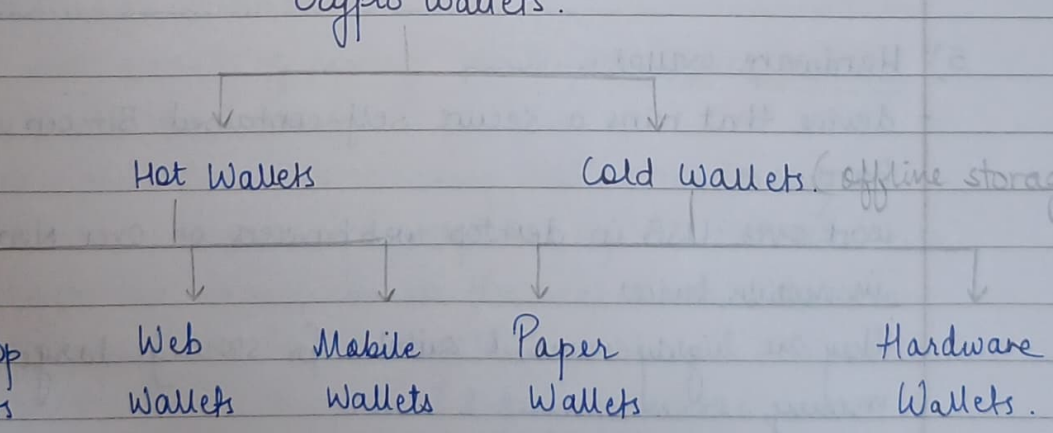
- Sending bitcoins from one account to another.
- usually done through a wallet.
- wallet app provides interface where we input recepient's account

id & amount we want to transfer.
- once we make a transaction, miners will validate it & add it to the blockchain ledger if it is legitimate.
- Bitcoin transactions are free.
- transaction is validated in 10 mins.
- if we want to speed it up, transaction fee has to be paid.

. Bitcoin mining
- one of the most important part of Bitcoin.
- process by which transactions are verified & added to the blockchain.
- requires dedicated mining hardware
- not all nodes are engaged in mining.
- Nodes that participate in the mining process are called miners.
- when new transaction occurs in the network, it is broadcasted via P2P & miners listen to these & engage in transaction verification
- once transactions are verified they are added to the block.

★ Wallets.

- Bitcoin wallets are used to interface with bitcoin system, just like web browser is used to interact with HTTP.
- there are many bitcoin wallets & implementations & brands.



1) Desktop Wallet.
- popular because of features, autonomy & control.
- first type of bitcoin wallet
- use of general-purpose OS such as windows & Mac OS has certain security disadvantages.

2) Mobile Wallet
- most common type
- working with smartphone OS such as Android & Apple iOS.
- designed to be simple & easy to use but are also full-featured mobile wallets for power users.

3) Web Wallet
- accessed from web-browser
- user's wallet is stored on a server owned by third-party.
- similar to webmail that relies on third party servers.
- services work with client-side code running in user's browser putting control of Bitcoin key in the user's hands.

4) Paper Wallet.
- keys to control Bitcoin can be printed for long time storage.
- offer simple & highly secure way to store bitcoins for long term.

5) Hardware wallet.
- device that runs a secure self-contained Bitcoin wallet on dedicated hardware
- work over USB in desktop web browsers or over Near Field Comm (NFC) in mobile devices.
- They are highly secure & suitable for storing large amount of money.

Full-node client.

- client that can store full history of Bitcoin transactions.
- manage a user's wallet
- initiate transactions directly on Bitcoin network.
- handles all aspects of protocol
- can validate the entire blockchain & each transaction independently.

Light weight client

- also known as Simple Payment Verification (SPV)
- connects to a Bitcoin full node to access Bitcoin transaction info, but stores user wallets locally.
- creates transactions & independently verifies them.
- interacts directly with Bitcoin network without any intermediary.

* Bitcoin Transaction lifecycle.

Lets assume Rob wants to send 0.3 BTC to Laura.

Steps:

a) Steps at Rob's end.

1) Rob opens his bitcoin wallet
2) He scans Laura's address
3) Fills in reqd. amount of money, info. & fees & click on send.

b) Processes by bitcoin network

1) Wallet signs the transaction using Rob's private key.
2) Transaction is propogated & validated by the network node
3) Miners include the transaction in the next block to be mined.
4) Miner who solves the PoW propogates new block to the network
5) The network verifies the result & propogates the block.

* Cryptocurrency.

- digital asset which can be circulated without the need of any central authority.
- cryptocurrencies are created using cryptographic technology to allow people to buy, sell or trade securely.
- digital / virtual currency that works on cryptographic principles.
- they have no physical existence
- they are intangible.
- they exist only as sets of programming code.
- it offers greater security & ease of use than existing currencies.
- go hand in hand with blockchain.
- for cryptocurrencies, ledger tracks the cryptocurrencies generated & traded on the network
- every person on the blockchain has a unique ID.
- cryptocurrencies are associated with these IDs.
- users can manage their accounts through apps called wallets.
- through wallets, anyone can conduct transactions with anyone on the network.
- both sender & receiver must have an account.
- transactions are verified by peers & added to the blockchain ledger.
- Pros

1) No restriction on payments
2) Maintainance of anonymity
3) Use of complex algorithm
4) Speed of Exchange
5) No third party involvement
6) Free / Less transaction fee
7) No inflation

- Cons

1) lack of awareness
2) use of complex technique
3) Highly volatile in nature
4) not accepted everywhere
5) victim of scam & theft
6) No reverse payment & recovery
7) Black market
8) Scaling issue
9) May not be exchanged with fiat currency

Types of Cryptocurrency.

Cryptocurrency.

- Bitcoin
- Altcoin
  - Derived from Bitcoins
  - Derived from original blockchain
- Token.
  - → Payment Tokens
  - → Exchange Tokens
  - → Utility Token
  - → Security Token
  - → NFT

Security Tokens
A "security" is a tradable financial asset.

Equity Tokens
form of security tokens that allow holders to have some ownership rights.

Asset-backed tokens
Tokenization of assets makes them tradable

- Instead of trading asset itself, you trade the token.
- similar to paper money.

Utility Tokens.
- Security tokens are traded with the expectation to get direct profit from it.
- Utility tokens are traded to get some utility.

Non-Fungible Tokens.
- If we buy collectibles such as art, comics, stamps or baseball cards, it matters which one we have.
- This property is especially attractive for computer games, where players already pay a lot for rare items within the game.
- Putting those on blockchain gives player more control over the asset.

Stable coins
Digital representation of fiat currencies.
1) fiat-collateralized - crypto backed by fiat currency
Eg- Tether, Gemini Dollar.
2) Crypto-collateralized - crypto backed by crypto.
Eg - DAI
3) Non-collateralized - stablecoins rely on smart contract to buy/sell the stablecoin to keep the price constant.

Dogecoin
open source, peer-to-peer digital currency favoured by Shiba Inus worldwide.

IOTA.
- IOTA stands for Internet Of Things Angles.
- Open source distributed ledger & cryptocurrency designed for IoT.

- It uses acyclic directed graph to store transactions on the ledger
- does not use miners to validate transactions, nodes that issue new transactions to the network must approve two previous transactions.
- transactions can be issued for free, facilitating micro transactions.
- reaches consensus through co-ordinator node, operated by IOTA foundation.
- network is centralized.

★ ALTCOIN.

- digital currency.
- alternative of bitcoin.
- when compared to Bitcoin, many differences are noticed.
- Litecoin aims to process a block every 2.5 ~~sec~~ minutes rather than every 20 mins, allowing it to confirm transactions faster than Bitcoin.
- Ethereum has smart contracts to run decentralized applications on the blockchain.

	Fungible Tokens	Non-fungible Tokens.
1)	Fungible tokens are assets which are interchangeable & can be exchanged with another asset of similar kind.	NFTs are unique assets that are not interchangeable & cannot be exchanged with another NFT of same kind.
2)	divisible assets, item can be broken down as long as value	non-divisible assets & represents a whole entity.
3)	Uniform & do not have a unique value proposition like NFTs.	NFTs have a unique value proposition.
4)	Use ~~ERC20~~ ERC20 to represent on the Ethereum Blockchain	Use ERC720 to represent.

	IPO	ICO	STO.
1)	Initial Public Offering	Initial coin Offering	Security Token Offering
2)	Shares	Utility tokens	Tokens baked by real-life assets.
3)	Strict Regulations imposed by governments.	No regulatory framework or legal protocol is reqd.	Regulated via KYC verifications.
4)	Startup forfeit control & ownership in the company.	Not backed by anything predisposed to scams.	Investors rights such as voting & revenue distribu...
5)	Expensive process that can take up to 6 mnths	Complete anonimity for investors via Blockchain.	Transparent fundraising sol^n
6)	Centralized	Decentralized	Centralized + Decentralized

* CDBC VS Cryptocurrency.

	Digital Currency	Cryptocurrency.
1)	Centralized	Decentrallized
2)	Requires verification	Partial anonymity
3)	Not Transparent	Transparent
4)	Regulated by central banks	No regulatory authority to control cryptocurrency
5)	Robust laws for trans. in all states	Only a few states have stringent laws for crypto transactions.

★ Metamask

- web browser add-on that allows anyone to run Dapps without running a full Ethereum node.
- A node installation of Ethereum takes up a lot of disk space.
- tool that removes the hectic installation overload.
- Initially, it was available only on google chrome, now it is available on Firefox & other web browsers as well.
- can be added to Google Chrome from Chrome web store or metamask.io website.
- Metamask extension provides a user interface for interacting with the blockchain.
- Users can connect to the main Ethereum network & or create their own private network to run Dapps on the blockchain.
- Usually, to interact with Ethereum Dapps, we need web3.js installed on your system.
- But Metamask injects web3.js into each ~~acce~~ page to access the Ethereum blockchain itself.
- eliminates overhead installing of web3.js on your computer.
- Users can create ~~app~~ accounts, access Ethereum Dapps, deploy their own Dapps.
- each user has a vault account.
- the vault stores, secures & a controls access to tokens, passwords, certificates, API keys etc.
- vault → second level of encryption for user's account.
- Metamask provides a group of 12 words called "wallet seeds" during installation.
- They are user's credentials & should be kept in a secure location
- Users can also create passwords for their accounts.
- Wallet seed or password is reqd. to log into metamask.

★ Coinbase

- allows users to buy, sell, transfer and store digital currencies securely online.
- Its goal is to build a financial system that is open to the world which helps to convert digital currencies into & out of their local currencies.
- ~~used for~~ buying & selling digital currency is easy
- Sending or recieving digital currency bet^n online crypto balances, friends or merchants on Coinbase is free.
- security & backups are maintained by Coinbase itself.
- offers primary balance service, an exchange & merchant tools within one simple interface.
- Some of the major currencies supported by Coinbase:

1) Bitcoin
2) Ethereum
3) Ethereum2
4) Tether
5) USD Coin
6) BNB
7) Binance USD
8) XRP
9) Cardano
10) Solana.

★ Binance

- Binance is Binary Finance
- It is a crypto exchange platform
- matching engine can sustain 1,400,000 orders per second
- Features:

1) Spot trading
2) Margin trading
3) Futures
4) Anonymous instant exchange.
5) Decentralized exchange

- Supports trading of :

1) BTC
2) ETH
3) LTC
4) NEO
5) BNB

- Device coverage :

1) Web-based trading client
2) Android native client
3) iOS native client
4) Mobile HTML5 client
5) PC native client
6) Rest API

- Binance has created two cryptocurrencies : Binance coin (BNB) & Binance USD (BUSD).
- BNB chain deploys "Proof of Staked Authority", a hybrid of PoS & PoA.
- BNB has 3rd highest market capitalication of any cryptocurrency.
- Allows its users to pay fees for BNB exchanges.