BT

unit-3

Page No.
Date

Block chain

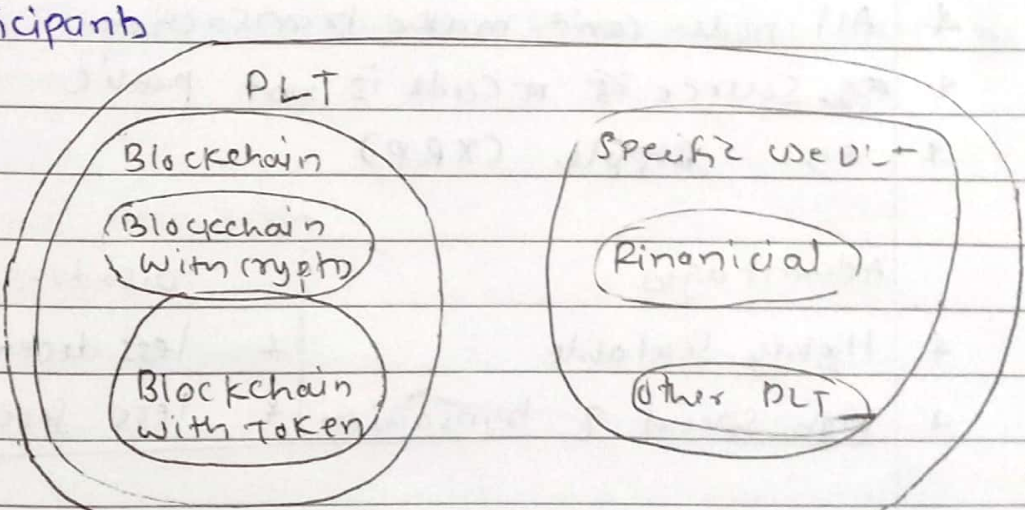
* It is a type of distributed ledger technology (DLT) that consists of growing lists of records, called block, that are Securely linked together

* Decentralized, distributed.

Distributed ledger Technology (DLT)

* Transaction are copied and stored on all the individual computer in network rather than stored on a central server.

* Shared Database with known & verified participants



Types

Public Blockchain.

* Anyone can access
* Anyone can join
* completely decentralized.

- Anyone can make transaction
- Anyone can use open source code
- Bitcoin

Advantages	Disadvantages
* transparent	* Scalability issue
* No Intermediate	* slow speed.
* Secured	* consume lot of energy

private Blockchain

- Accessibility - Single person | central Incharge
- useful for Businesses.
- permissoned
- less Decentralized
- All node can't make transaction
- ~~eg~~ Source ~~is~~ Code is not public
- eg. Ripple (XRP)

Advantages	Disadvantage
* Highly Scalable	* less decentralized
* high speed of transaction	* less secured

Consortium Blockchain

- Hybrid of both.
- multiple organisation manage it.
- permissoned
- Selected member can make transaction.

Adv.	Disadv
* Scalable	* less transparent
* efficient	* less decentralized
* access control offers.	

—xox—

- Bitcoin
- first Cryptocurrency.
- Bitcoin is peer to peer payment network that operate on a cryptographic protocol.
- currency - bitcoin.

How to use bitcoin.

open account and wallet in Service provider eg. coinbase, Bitcore, then genrate key. private key as password and public key as account ID.

How we can earn !

2 Ways.

(1) bitcoin exchange

(2) mining.

Tronsaction: Sending Money from one to another account.

Mining

When transaction happen, it broadcast to all node, then task is to find hash value for new block.

- It has some difficulty level.
- With uses nonce - a arbitrary 32 bit string

H(block + nonce).

* miner use bruteforce and try combination
* who solve it first will broadcast the block and nonce then after verified by all the node is added to blockchain and miner rewarded

* value of Bitcoin depend on demand & supply

Adv. of Bitcoin.

* fraud protection.
* No need identity of sender and receiver
* No third party.
* Direct transfer.
* easy international transaction.
* Security
* Blockchain Technology.

Dis adv. of Bitcoin.

1) not easy to understand common man.
2) popular in Black market and criminals.
3) volatile price
4) No refund if payment done

Ethereum.

* open source Blockchain platform, anyone develop and deploy DAPP.
* private, public & main Ethereum network
* no need to create a new network
* It provide platform

* account → EOA
  → smart contract
* DAPP front end - Bootstrap, etc
  Back end Smartcontract - Solidity
* whipser, swarm,
* computing platform.
* Turing complete.

Hyperledger.

* By Linux foundation.
* provide neutral, open source platform for Business transaction.

→ enterprise blockchain
→ consortium Blockchain.
→ enterprise need privacy and speed balance.
→ It host many enterprise project.
→ Collaborative effort.

framework

1. Hyperledger fabric
develop blockchain app, product or Solution.
private, Scalable
Smart Contract → Chaincode. (Business logic)

2. Sawtooth:
- Both private and public, (POET)

3 Indy, 4. Burrow 5. Cello, 6. Grid.

IOTA

* Open source, decentralized, highly Scalable Distributed ledger Technology (DLT)

* IOT solution.

* IOTA used DAG (Directed alyclic graph)

* IOTA protocol, Tangle offer functiondity similar to blockchain.

In DAG Nodes or vertices are gadget or computer and edge are communication b/w them.

features.

(1) IOTA is Scalable.
(2) Feeless
(3) Flexible, public + private.
(4) Quantum proof security
(5) No miner in IOTA Nework.

verification is done by node itself. and uses validation algorithm. But first node has to verify any two random transaction.

R3 corda.

- private Blockchain.

-> aim to build financial system where companies can participate to bring transaction directly into business using Smart Contract.

-> Enterprise Blockchain

features.

(1) open source - Built on JVM.
(2) Data privacy
(3) large Community ↑.
(4) Scalability.

Defi - Decentralised finance.

* Corda uses Notory as unique consensus Service

CorDapps. - Corda Distributed app.

Consensus in Blockchain.

- It is procedure through which all nodes come to a common agreement.
- It guarantee that a state, value, or piece of information is correct and agreed by most nodes.

-> Some are best in speed, Secure, Some are in public some are in private.

+ Collaboration of all nodes.
+ Cooperative work by all nodes.
+ equal rights to all nods.
* All node will participant in voting.

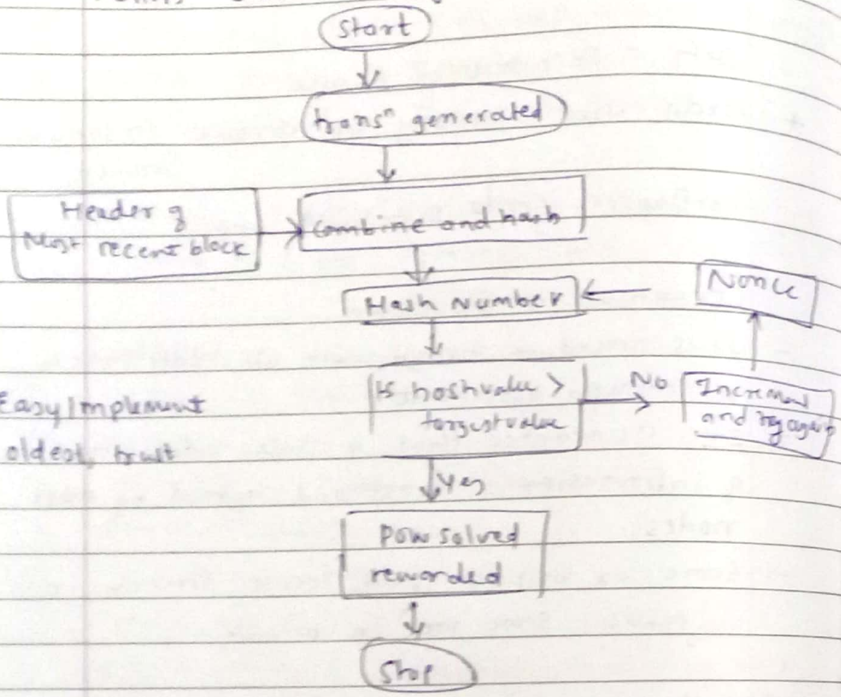
Objective of Consensus Mechanism

(1) fair & equitable
(2) unified agreement
(3) It reward or punish to node
(4) Prevent double Spending

(5) fault Tolerant.

Proof of work (PoW)

→ first consesus algorithm, Bitcoin.
when transaction occur it Broadcast to all nodes then.
Miners start mining



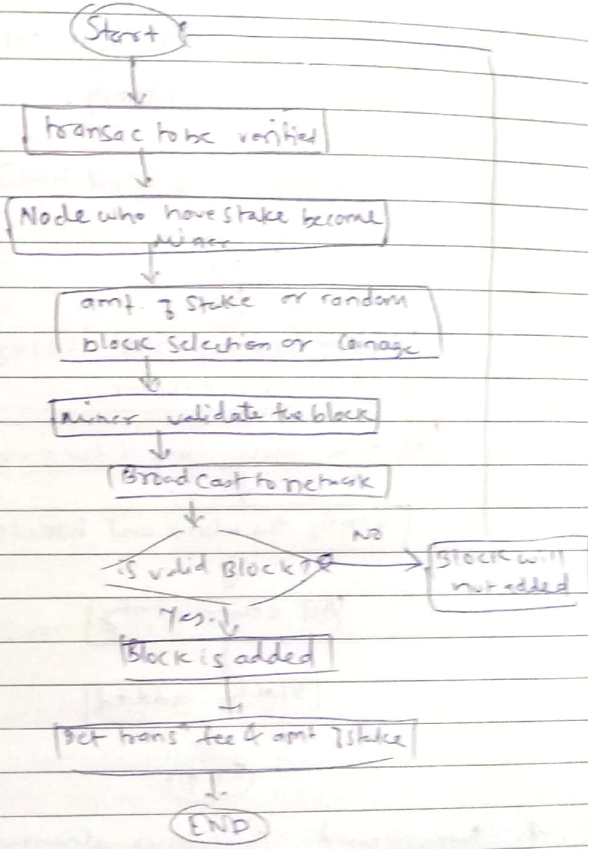
#Easy Implement
* oldest, trust

After problem solved, the nonce is broadcast to all nodes then, verified by network. and added to the network.

* Consume lot of energy and resources.
* 51% of chance of network attack
* required hardware cost

(PoS) Proof of stake.

* validators. and no mining competition
* validator is chosen based on stake (amt of money deposited).
* max State will get Chance first



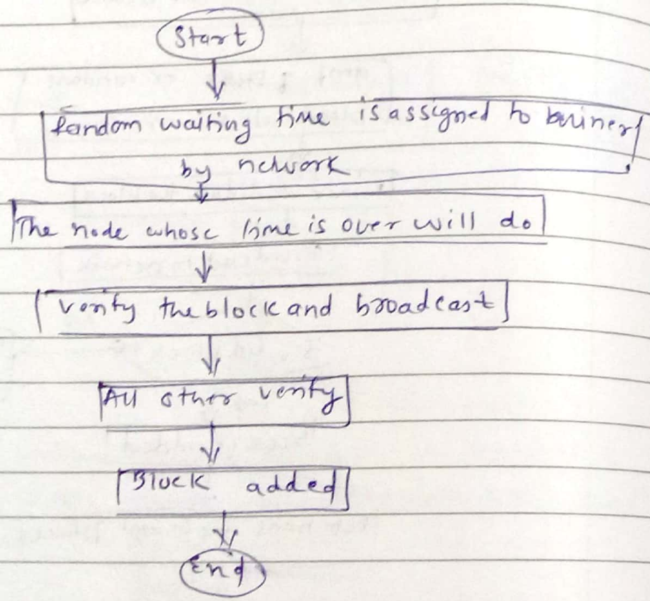
Coin age based selection. - No of day coin held by Miner
Randomized Block Selection - chosen with Combinatio
of 'lowest hash value' and highest stake.

- new coin is not generated in pos.
- Miner can get penalty also

Adu. (1) Energy - efficient
(2) security - 51% attack

disadu. (1) large stake will get chance
(2) New technology.

POET (proof of Elapsed time).

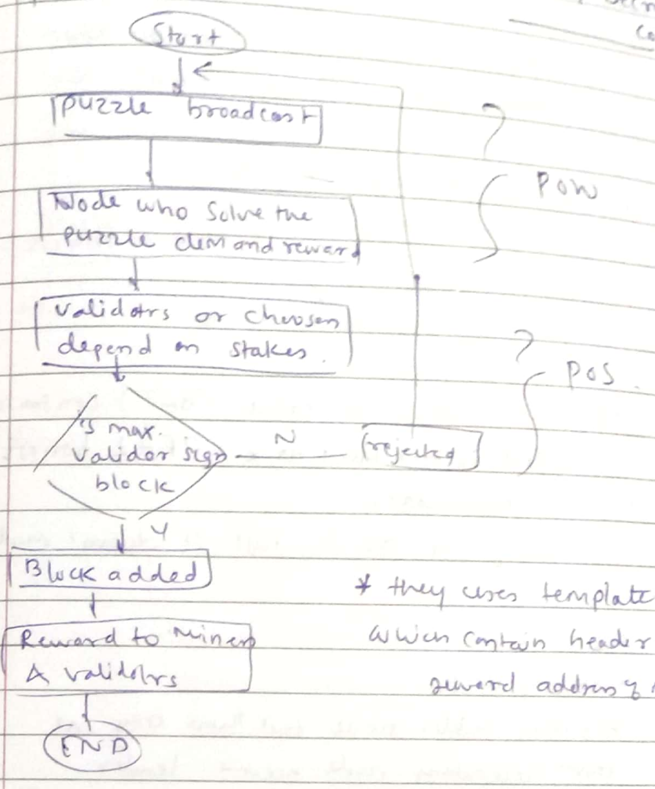

Start
random waiting time is assigned to miner by network
The node whose time is over will do
verify the block and broadcast
All other verify
Block added
End

- Permissioned Consensus algorithm.
- lottery System is used.
- Energy efficient
- Processor can sleep in waiting time

proof of Activity (PoA)

PoW + PoS.

eg Espers, Decred coin


Start
puzzle broadcast
Node who solve the puzzle claim and reward
validators are choosen depend on stakes.
is max. validator sign block
N
rejected
Y
Block added
Reward to miners & validators
END
PoW
PoS.

* they uses template which contain header and reward address of miner

Proof of Burn (PoB)

* The miner get chance of winning by burning coin.

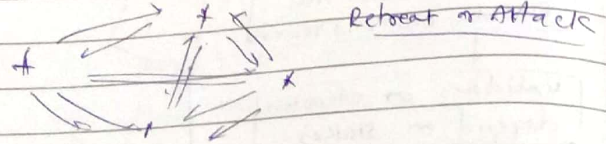
Adv. (i) little power consumption
(ii) used for long term termination.

Disadv (i) required wealthy participant
(ii) Slower Mechanism.

BFT (Byzantine fault toleronce).

* It is diffcult to reach a consensus when Some nodes are dishonest or fail.

Byzantine General's problem



Byzantine fault toleronce (BFT) consensus.

-> distributed system must have 2f+1 honest

-> used in hyperledger.

-> If out of 4 one is fail it doesn't matter.

PBFT.

- Variant of BFT.

-> ~~wo~~when ledder node fail then any one from secondary node become leader.

-> Max. 1/3rd of the node may be malicious

Working

(1) trans^n. broadcast, leader selected based on Round Robin.

(2) leader prepares block proposal and brodcast to the network and the state alters to preprepare state.

3. The backup node receive it and verify. if they agree request then broadcast to network

4. node chang state to prepared state After getting Same result from 2m+1

5. Block added.

Adv. (1) Energy Efficier

(2) low reward variance.

disadv. (1) work when small no of nodes.