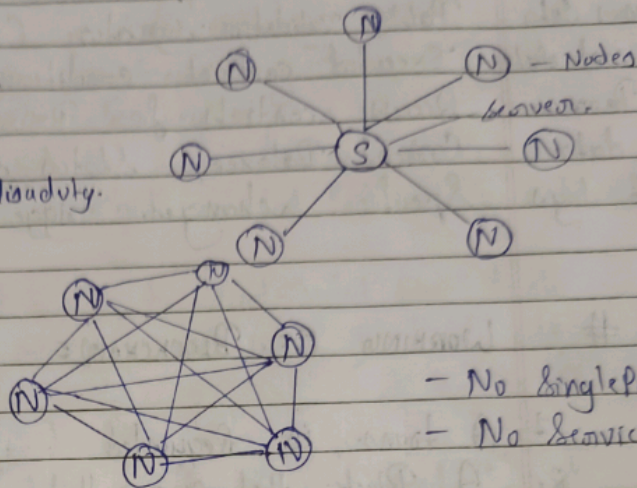


UNIT-1

BLOCKCHAIN

- Centralized Network
- Single Point failure } disadvt.
- Service Changes }
- Decentralized N/w.
- All blocks connected to each other.
- Highly Secure.

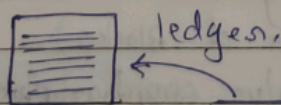


- No single point fail
- No service change

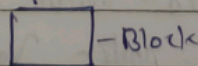
"Blockchain is a decentralized computation & ~~computation~~ information sharing platform that enables multiple authoritative domains who do not trust each other to coordinate in a rational decision making."

What is Ledger?

- Blockchain uses ledger to store transaction details
- Can be of any form/filetype.
- data stored with time. - Every ^{Block} ledger has capacity



(Record keeping system.)



- Immutable - Tamperproof.

Trans. details	← Ledger
Block Metadata	
Consensus data	
S.C. data	
Access Control	/Permissions
Event logs.	

Trans. detail -	Time, Amt, Sender receives add.
Block Metadata -	Position, unique identifier (hash) Previous Block hash
Consensus data -	PoW, Validation signature (PoS)
Smart contract data -	Executed contract conditions & outcomes
User Permissions	Access controls from Private P.C.
State data	Current Balance, Status of Account etc.
Event Logs	Specific changes triggered by protocols/contracts

WORKING OF BLOCKCHAIN

1. A trans. is Requested
2. A Block that repr. that trans. is created
3. The block is sent to Every node in N/w.
4. Nodes validate trans. ($> 50\%$ nodes).
5. Nodes receives reward from PoW.
6. A Block is added to Existing P.C. of
7. Trans. complete.

COMPONENTS OF B.C.

1. Node: A user that is part of B.C. N/w.
 full node - carry complete copy & verify trans.
 Partial node - Only essential info for quick verification
 (Header of Blocks).
 Mining nodes - Solve cryptographic puzzles (PoW)
 Validators node - Validate trans. & propose block
 (PoS)

2. Ledger - distributed database. - Public ledger.
Ensure transparency & Immutability.
3. Wallet - for storing cryptocurrency
- Public & Private key
Hot Wallet - day to day trans / online / Hacked issue.
Cold Wallet - Secure /, not connected to net / user have to purchase
4. Nonce - (Number used once) to find valid block hash
Ensures that miners must work hard to add new block.
5. Hash - (Ex. SHA-256)
Unique fixed len. cryptographic Output
Convert trans. or data into unique 64 char hexd. value.
Deterministic - Same input produces same hash
Irreversible - Cannot retrieve original data from hash.
Fixed len - Regardless of Input
6. Blocks: Each trans. grouped into Block
① Header - Metadata
② Data - Include list of confirmed trans.
③ Hash - unique identifier gen. using cryptographic hashing
7. Consensus Mechanism: PoW, PoS, PoA etc.
8. Public & Private key:

TYPES OF B.C.

① PUBLIC B.C.

- Anyone can join & initiate transaction.
- Decentralized - High transparency
- Permissionless - Security via Consensus (PoW & PoS)
- Slower trans. - Immutable
- Ex. - Bitcoin & Ethereum.

② PRIVATE BLOCKCHAIN:

- Restricted Access - approved participants can join n/w.
- Faster Transaction - due to fewer validations.
- Centralized authority. - No scalability issue.
- Controlled Governance - High Security
- Ex. Hyperledger, Corda, - Customizable rules

③ Consortium Blockchain.

- Public + Private B.C. - Customizable Rules.
- Anyone can participate & initiate trans. But some chosen nodes only can verify the trans. & validate
- Ex. Maersk, IBM food trust.
- No scalability issue - Highly secure - Efficient.
- Less Anonymous. as compared to above types.

SATOSHI NAKAMOTO (Bitcoin Inventor)

Block Connection:

$H_0 \leftarrow \text{Block-1}$
 $\text{Hash}(0) = H_1 \leftarrow \text{Block-2}$
 $\text{Hash}(1) = H_2 \leftarrow \text{Block-3}$
 $\text{Hash}(2) = H_3 \leftarrow \text{Block-4}$

$\boxed{\text{PoW} + \text{data}} \leftrightarrow \boxed{\text{PBH} + \text{data}} \leftrightarrow \boxed{\text{PBH} + \text{data}}$

Public B.C.

Open to Everyone
Fully decentralized
Slow trans.
Transparency fully
PoW, PoS
Energy Intensive

Ex. Crypto, Smart contract
Network congestion (less secure)

Private B.C.

Restricted users
Partially or centralized
fast trans.
Limited transparency
Varies Based on usage
Energy Extensive

- Supply chain Mgmt.
- More controlled risk of centralization (highly secure)

Public Key Cryptography:

Public key (shared openly)
Private key (kept secret by owner)

Working -

- ① Encryption / Decryption (Confidentiality)
Sender encrypts message using recipient's Public key
Only recipient's Private key can decrypt message.
- ② Digital Signature (Authenticity & Integrity).
Sender signs message using their private key
Anyone can verify message using sender's Public key.

Use in B.C.

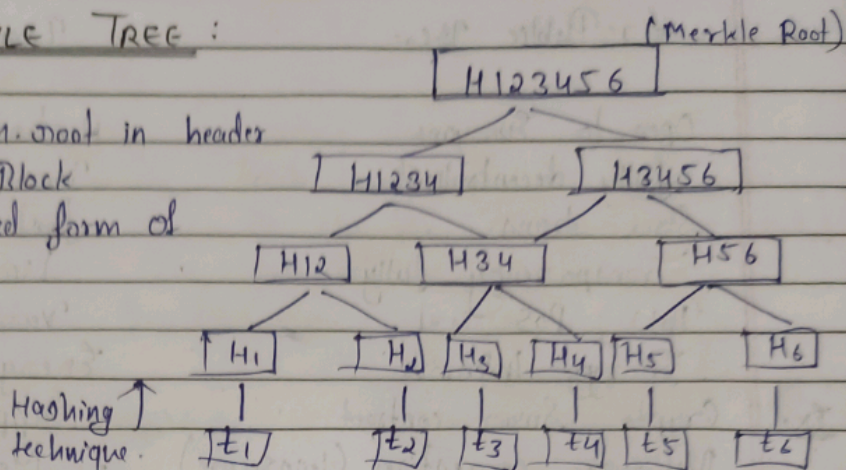
- Wallet add. derived from Pubk key
- Nodes verify sign. using - " -
- Signed trans. with Priv. key to validate trans.

Why?

- Security
- Global Interoperability
- Ed. of digital identity.

MERKLE TREE :

- Store M. root in header of a Block
- Encrypted form of trans.



Block IN B.C. :

- Any change in 1 Block break chain
- digital contains stores List of trans.
- linked to block before.
- Create an unbreakable chain

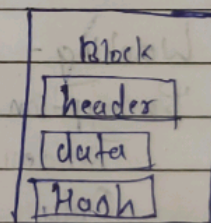
① Block header

Prev. Block hash

Timestamp

Nonce - Merkle Root

Difficulty Target



2. Block body : List of valid trans. added to B.C.

includes : Crypto trans.

Smart contracts

no. of trans. limited by size of Block.

②. Hash : Unique identifier created using technique

PERMISSIONED B.C. (PRIVATE B.C.)

- Key char:
- Controlled access
 - Defined Roles
 - Auditable & Secure
 - Faster trans.
 - Customizable Consensus (RAFT, PBFT, PoA)
- Known & traceable Participants.
 - Where used?
 - Enterprises level Appl.
 - Consortium of trusted parties
 - Regulated industries (Finance, Insurance).
- Ex. Hyperledger Fabric
R3 Corda - Quorum.
- (Why choose Permissioned over Private?).

DISTRIBUTED CONSENSUS :

- It is a type of Agreement (Voting or Validation)
- Helps in validating trans.
- Promotes Security & Trustworthiness.

"A process by which a decentralized n/w. of computers agrees on a single, unified version of truth." Without relying on central authority.

- PoW - PoS - PBFT, - RAFT & PAXOS
- Security
- Transparency
- Fault tolerance

#. CRYPTOGRAPHY

Why? Secure, transparent & Trustworthy.

- Foundation of B.C.
- Science of Securing Infor. through mathematical techniques.
- Data Integrity
- Public / Private key
- Digital Signatures
- Hash fn (SHA-256)
- Asymmetric Encryption (RSA, ECC)
- Merkle tree.

#. CRYPTO CURRENCY:

- Digital or Virtual currency.
- Operates on decentralized B.C. Ntw.
- No govt. Control
- Peer to Peer
- Immutable
- Use B.C. for task automation
- Borderless

Ex. → Bitcoin, Ethereum, Solana (BTC, ETH, SOL)

- Uses:
- Cross Border Pay
 - Investment asset
 - NFT - Buying & trading digital Assets
 - Decentralized finance (Borrowing, lending without Banks)

Working:

- User has wallet
- Trans. Initiation by signing digitally
- Verification by nodes using consensus.
- Trans. done Added to B.C.

#. HASH FUNCTION:

- One Way Cryptographic Algorithm
- takes input (message) & return fixed size hexd. string.

Properties:

- Fast Computation
- Deterministic
- Avalanche Effect (small change large effect).
- Irreversible
- Collision Resistance.

Hash Pointer:

- Special type of data structure in B.C.
- Stores pointer to some info. & also hash of that information.
- Every Block contain hash Pointer to Prev. one.
- Helps creating chain of Block (Hence B.C.)
- Change in Prev. Block can leads to change in all subsequent next blocks

Digital Signatures: (Eqv. to handwritten signature.)

1. Hashing Message
2. Encrypt hash with Priv. Key.
3. Sending data + Signature
4. Verifying sign. (using Public key of sender)

- Authentication
- Integrity - Non repudiation (sdr can't deny trans.)

UNIT-3

PERMISSIONED BLOCKCHAIN Applications

- Banking - Inter Bank Settlement
KYC - Trade Finance
- Supply Chain Mgmt. - Goods tracking
Automated Audits
Vendor Coordination
- Healthcare - Record keeping
- drug traceability - Consent Mgmt.
- Govt. Sector - digital Identity - Voting Systems
Land Registration
- Education - Digital Certificates
- Cross Institution collaboration.
- Insurance - claim Processing
- Reinsurance Coordination
- Manufacturing & Industrial (IIOT)
 - Real time Quality Control
 - Asset Lifecycle Management.

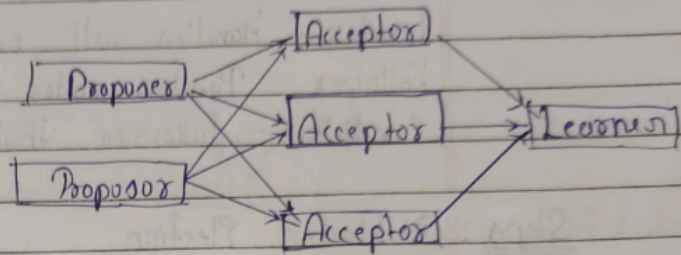
DESIGN ISSUES OF PERMISSIONED B.C.

- Identity & Access Mgmt.
- Consensus Protocol design (PBFT, RAFT, PoA)
- Privacy & data confidentiality.

- Governance & Policy control
- Scalability & Performance (complexity)
- Smart Contract Mgmt.
- Ledger Architecture
- Resilience & Fault tolerance

Paxos

- Consensus Algorithm



Proposer - Wanted to change

Acceptor - votes for Proposer's change (Accept or reject)

- Proposer Broadcast vote counts.

What if Acceptor / Proposer fails?

Proposer
 Acceptor → Propose Phase [No vote considers] Propose phase
 → Accept phase. [N/2+1 shouldn't fail] Accept phase.

Proposer → P.F.: Not considered the Proposer

Wait if only one proposer is there & chose new

A.F.: Unanimously accept or reject decision.

Unable to Broadcast votes so no win/lose.

- Safety
- Fault Tolerance
- Liveness

Used → MS. Azure

Google Chubby (distrib. lock Manager)
 OpenReplica & Consul

RAFT

- distributed consensus Algorithm
- Ensures exple n/w. nodes agree on a sequence of actions

Leader - Handles all node Entries from client & coordinate

Follower - Passive nodes that replicates Entries & respond

Candidate - followers that try to become leader.

Steps: ① Leader Election

(Election & voting)

② Log Replication

leader receive trans. (log Entry) from client

- Appends entry to own log & send Append Entries to followers

- Once A majority acknowledges, the Entry is applied to the state machine on all node

③ Safety & Consistency

- follows reject Entries that not matching to log
- Even after crashes, nodes can recover status from committed logs.

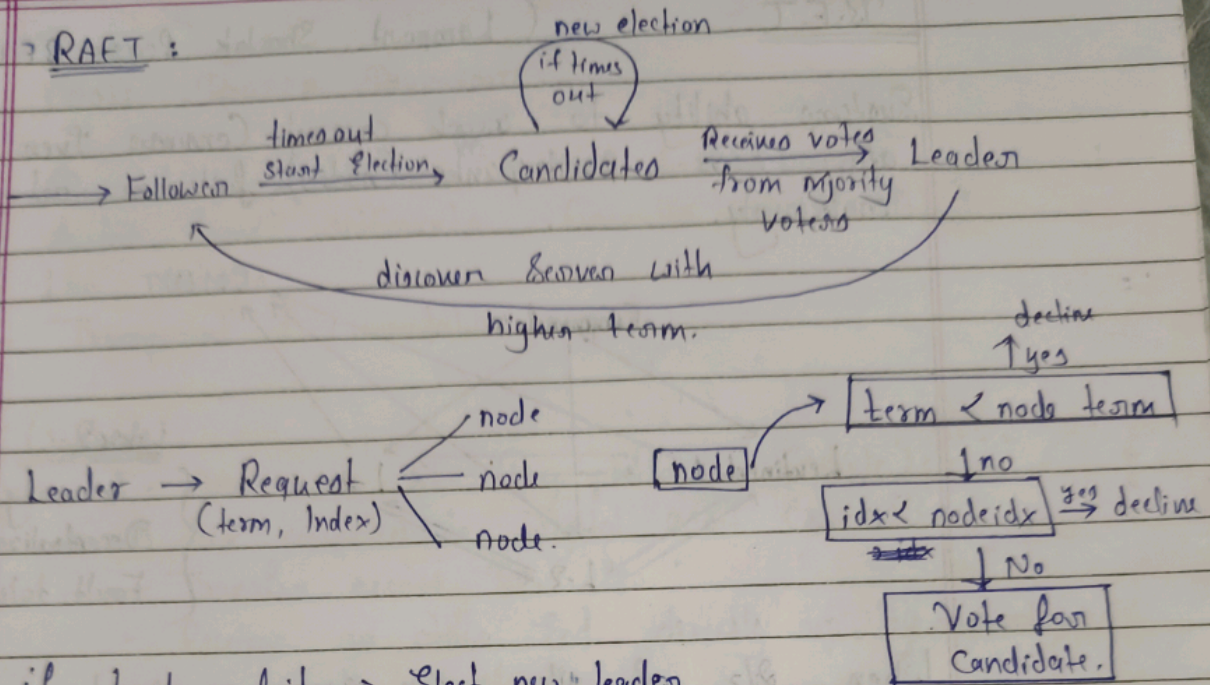
Why?

- Simple debugging & Implementation
- Low latency
- Deterministic Behaviour.

Appl.

- Hyperledger fabric

RAFT :



1. if Leader fail $\rightarrow$ Elect new leader
2. if follower fail $\rightarrow$ 50% followers should active otherwise no issue.

BYZANTINE FAULT TOLERANCE

1. PROBLEM ? (Byzantine General Problem).

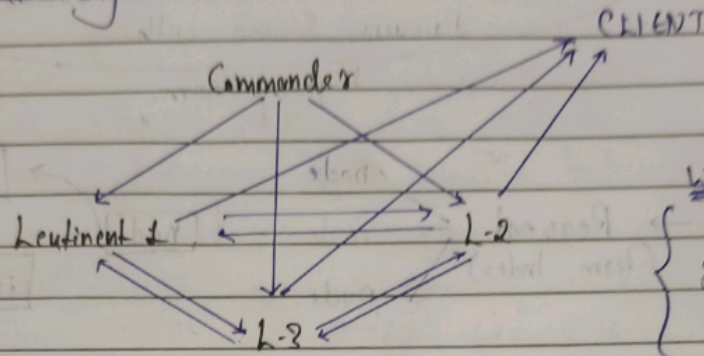
"How multiple parties agree on a action even after some of them are unreliable, malicious or sending false information"

- Imagine several generals surrounding a city
 - Must agree on unified plan - Attack / retreat
 - But - Each genl communicates via Messenger.
 - Some general may be traitors
 - Message can be intercepted, changed or delayed.
- "How the loyal generals reach consensus?"

B.F.T.

(Lamport Shostak Pease BFT.)

System's ability to reach correct consensus even after some participants (nodes) fail or act maliciously.

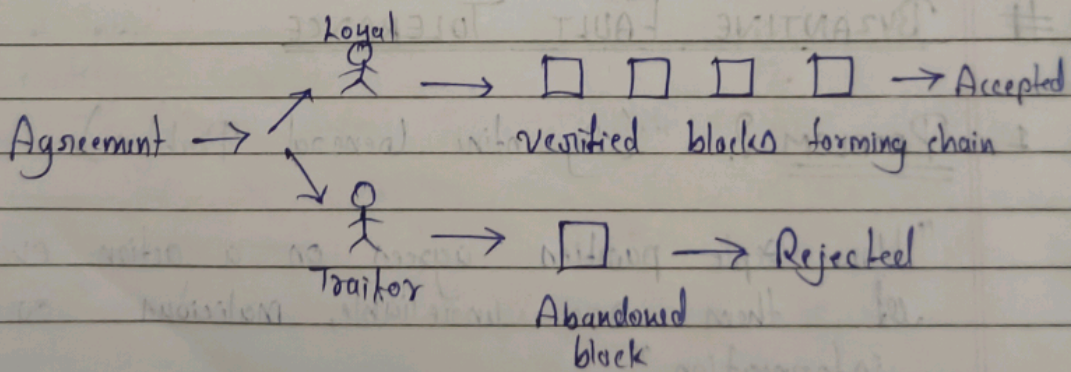


Why?

- Security
- Decentralization
- Fault tolerance

- When 2/3 of N/w. can agree on reach a consensus and the system still continues to operate properly, it is said to have BFT.

- In order to create decentralized N/w. the BFT essential



UNIT-4

CROSS BORDER PAYMENTS

- Peer-to-peer transfer without intermediaries
- Faster trans. settlements (minutes inst of days)
- Low Charges
- Transparent & immutable records.

Working:

- One uses bk. Pay platform (Ripple) etc.
- INR converted to digital asset (XRP/USDC)
- Transfer across B.C. N/w.
- Receives on other end directly or by converting.

Ex. RippleNet, Stellar, JP Morgan's JPM coin

Challenges → Wallet mgmt.

- Regulatory Compliance (AML/KYC)
- Currency volatility (if not using stable coins)

KNOW YOUR CUSTOMER KYC :

KYC is process by which inst. verify id of their clients

Working:

- A user completes kyc with org. A
- Verified data is encrypted & stored in Permissioned B.C.
- Institution B can access this data (with user permission) and skip redundant verification.
- Creates single source of Truth for Redundant data.

KYC Appl. → Banking / finance - Telecom (sim card)
Insurance - Healthcare
Fintech & Crypto exchange

Advts:

- Data immutability
- Time saving
- User Control
- Faster onboarding
- Single source of trust
- Cost Efficiency
- Fraud Reduction

Privacy & Security:

- Zero knowledge Proof
 - Allows verification without actual revealing ^{actual} data
- Smart Contracts: Automate access control & compliance
- Decentralized identities - Let users own & manage ^{check} their digital identity.

Challenges:

- ① Interoperability - diff. institutions use incompatible systems
- ② Data Privacy laws - Should follow govt. protocols
Indraj DPDP act
- ③ Regulatory uncertainty - Varies across jurisdiction.

#. BLOCKCHAIN IN FOOD SECURITY:

Food Security Means that all people at all times have physical, social & economic access to sufficient food & nutritious & safe food.

Four Pillars:

- Availability - is food Produced & supplied
- Accessibility - Can people afford & obtain it.
- Utilization - is food safe & nutritious
- Stability - Are these conditions consistent over time.

Steps:

① Data Entry at Source:

farmers or producers upload data (eg. harvest date, pesticide use)

2. Supply chain Tracking:

Each mid handler (transporter, retailer, processor) logs their action, location, storage condition, temp.

3. Immutable ledgers:

All Entries are time-stamped & cannot be altered ensuring data integrity.

4. Consumer Access

End users can scan QR to view the product's full journey

- Traceability
 - Food Safety
 - Supply chain Efficiency
 - Certification
 - Consumer trust
- Ex. - IBM food trust
- Nestle + Rainforest Alliance.

Mortgage Over B.C.

→ Traditional Mg. Process

- Paper heavy
- Time Consuming
- Prone to Error & Fraud
- Involves multiple intermediaries (Bank, notaries etc.)

→ Working:

- Application → Borrower submits digital doc. via a b/c platform
- Verification → Smart contract validates Kyc, credit score, property titles
- Approval → Lenders review verified data & issue loan terms
- Contract Sign → Borrower sign digitally, the agreement is recorded.
- Disbursement → Funds released via smart contracts
- Servicing → Payments, Interests & defaults tracked transparently.

→ Advts: Speed - Security - Automation
Transparency - Processing cost - Auto Monitor
- Auditability

→ Tech. Involved - Smart Contract - Oracles
- digital identity (feed offchain data)
- Tokenization (Credit score)
- property values

BLOCKCHAIN ENABLED TRADE:

- Smart Contract Initiation -

A dgtl trade Agreement is created on B.C.

2. Doc. Upload:

Bill of lading, invoice, Certificate of origin & insurance are uploaded and timestamped.

3. Shipment Tracking:
Real-time location & condition
4. Customs clearance.
Authorities access verified doc. instantly.
5. Payment Execution:
Once delivered, &c. auto-release payment via tokenized currency or stablecoin.

Advts: Transparency - Security - Trust
Speed - Cost Efficiency

Ex. We trade
TradeLens (By IBM)

Tech. Involved → Hyperledger fabric/corda
IoT integration
Digital Signatures
Stable Coins.

IDENTITY ON B.C.

- System for managing digital identities using B.C.
- User can create own & control their identity.
- Without trusting any central authority

1. Id creation → User create & store on digital wallet
2. Verification → By trusted institutions.
3. Storage → Stored off-chain
4. Selective disclosure → User can share only necessary data without revealing full doc.
5. ~~Val~~ Validation - Relying Parties verify credentials using B.C.

UNIT-2

POW

[Satoshi Nakamoto (2008)]

- Find Nonce by trial & error Basis.
- Consensus Algo. to validate trans. & add block.
- Requires participants (called miners) to solve C.M. Problem
- Work $\rightarrow$ computational Efforts. Ex. Bitcoin, Litecoin, Dogecoin (Doge)

Working.

- ① Trans. Pool - Trans. Broadcasted
- ② Block formation - Miners group trans into a block
- ③ Puzzle Solving - solve puzzle, find nonce, verify hash below diff level
- ④ Proof Submission - first miner to solve it broadcast a solution
- ⑤ Verification - other nodes verify solution quickly
- ⑥ Block Addition - If valid block is added
- ⑦ Reward. - Miner is rewarded (Bitcoin)

- Security - PoW is track record.
- Decentralization - Tamper resistant
- Centralization Risk - Energy consumption.
- Limited trans Per Second (scalability)

POS (Proof of Stake) Ex. Ethereum, Cardano

- Validators are chosen to create new blocks & verify transactions based on the amt. of currency they "stake" (lock up)
- PoS relies on Economic Commitment
- Energy Efficient - Decentralized Access
- Scalable - Security via incentives.

Working of PoS

- Staking - Users lock a certain amt. of crypto in n/w.
- Validator selection: Select validators - often randomly but weighted by stake size & sometimes coin age.
- Block Proposal - The chosen validator proposes next block
- Validation - Other validators confirm the block's validity
- Reward & Penalty - If valid, validator earn trans. fees / reward
if not, The validator's stake may be slashed

- Wealth centralization
- Long Range attacks.

(PoW vs PoS)

Proof of Elapsed Time - PoET

- Each node request a random wait-time
- All nodes sleep for their assigned time
- The node with shortest wait time wakes up first & wins right to propose next block
- N/w. verified that the node actually waited the correct time using cryptographic proof from TEE.

- Low Energy
- Fairness
- Security
- Cost Efficiency
- Scalability

Appl. - Hyperledger & Bluetooth
- Supply chain
- Digital identity

Intel SGX (Side Guard Extensions)
TEE (Trusted Execution Env.)

- H/w. dependency
- Risk of Centralization
- Not suitable for Public B/c.

PROOF OF BURN (PoB).

- Permanently destroying a portion of their Cryptocurrency.
 - Burning Coins
 - Proof generation
 - Mining Rights
 - Block creation.
- Steps.
- Energy Eff.
 - Fairness
 - Decentralization
 - Waste of Resources
 - Wealth centralization
 - Irreversibility
 - Limited adoption
- Alternative to PoW.

CRYPTOCURRENCY WALLETS

Hot Wallets

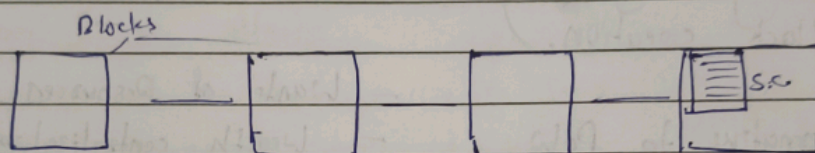
- Desktop w.
- Mobile w.
- Online w. (cloud)

Cold Wallets

- H/w. wallets
- Paper wallets

SMART CONTRACTS :

- Condition Oriented Program
- Written in Prog. Language.
- Remove Middleware/Intermediaries
- All nodes have copy of contract
- Any one block in b/c has S.C.
- Less chances of fraud.
- Automate System process
- S.C. cannot be altered
- No commission
- Fast
- distributed.
- Infor. to all.



Blockchain

Activating S.C. $\rightarrow$ Time
Situation.

- Pbk. broadcasting
- Provide Private key to sender (Trans-initiator) & Pbk to other nodes
- Sender generate message & Encrypt using Pbk.
- Message S.C. is Executed & they can send S.C.

Types

Smart Legal Contracts. (100% rule follow).

Decentralized Application (DApp) (App. Enabled ledger)

Distributed Autonomous Transaction (DAO)
(Financial Transaction), (Human Intermediary)

BTC

- 1 MB
- 21 million Coin
- Most Popular
- Tokens not availbl
- Avg Block time - 10 min
- SHA 256
- 2009
- Cryptocurrency

ETH

- unlimited
- Unlim.
- 2nd Most Popular
- Available tokens
- 14-15 sec
- KECCAK-256
- 2015
- Crypt + N/w. S/w.

Token # Gas (is a type of token used in Eth)
Gas = Ethereum
Gas → 0.01 Ether

- fixed cost
- charge on transaction

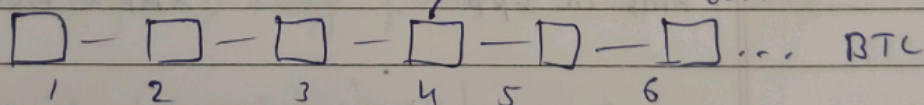
Altcoin Alternatcoin generated due to forking Process

P to P

Altcoin

Btcwin (Caché)
(BCH)

Forking



CORDA

Permissioned distributed ledger Platform

- Regulated financial services
- P-P - Notary services
- CordApps - Smart contracts (Kotlin / Java)
- No global trans. Broadcast

Ripple. (2012) Ripple Labs

BC. Based Payment Protocol

RippleNet (NW. of Banks)

XRP ledger (cryptocurrency) decentralized open source BC.
XRP (cryptocurrency)

B-A → RippleNet → B-B
(USD) (Euros)

↓ ↑
Ripple gateway → Validator node → Ripple gateway
Fiat to XRP (XRP to Fiat)

Protocol level APIs

Hyperledger Fabric
Modular, Permissioned B.C. for Enterprise.
B.C. Framework Implementation

1 Membership Service Provider
Manages Identity & access control
Issues digital certificates using (CAs)

2. Peer Nodes:
Maintain ledgers & execute B.C. (called chaincode)
Endorsing Peers
Committing Peers
Anchor Peers facilitate cross org. communication

3 Ledger
Consist of B.C.: Immutable trans. logs
World state: current state of assets

4 Chaincode: Smart contracts
Business logic written.
Executed by endorsing peers to simulate trans.

5 Ordering Service (consensus layer)
Order trans. into blocks
- Ensures total order across n/w.

6. Channels: Private subsets within n/w.
Allow confidential transactions.