classmate
Date 25/06/21
Page

# UNIT:-02

## Blockchain

### Introduction:-

Blockchain is a system of recording the information in a distributed ledger which is distributed across the network in such a way that its impossible to change, hack or modify the data.

Blockchain usually contain following concepts.

1. A data store that records the changes in data. Most commonly the financial transactions but it can record any data in blockchain
2. Replication of data store across a no. of system in real-time. Broadcast blockchain such as Bitcoin, Ethereum ensure that all data is sent to all participants.
3. Peer-to-peer rather than client-server architecture. Data may be gossiped to neighbour rather than broadcast.
4. Cryptographic methods such as digital signature to prove the ownership and authenticity.

classmate
Date
Page

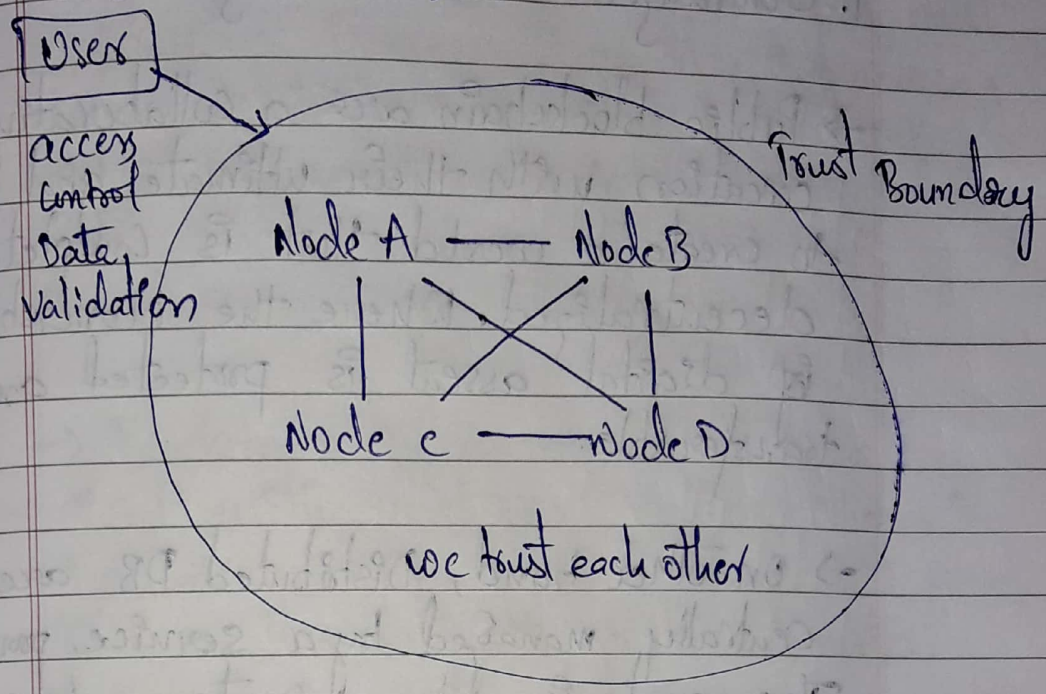
# Blockchain vs Database

→ The DB simply stores & retrieves data.
→ A Blockchain platform is more than that. It stores and retrieve data and also connects to other peers & listen for new data, validate data then stores & broadcast the new data to other networks participants to ensure that they all share same updated the data
→ It's done constantly without manual intervention.

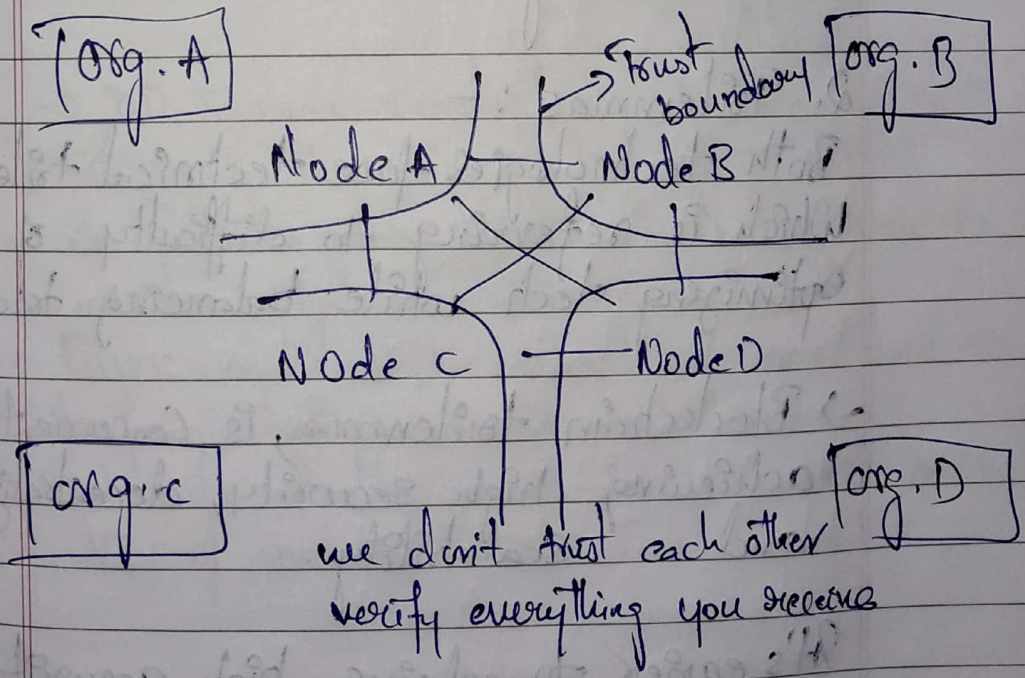
## * Advantage over Conventional distributed DB.

→ Replicated db, where data is copied in real time to multiple machines for resiliency or performance reason.
→ Shared dbs, where workload & storage are shared, to increase speed & storage.
→ With Distributed ledger or blockchain participants do not need to trust each other
→ they do not work on the assumption that the participants are honest

1. Distributed Database




2. Distributed ledger or blockchain



1. Centralized vs decentralized.

→ Public blockchain are a collaberative creation with their ultimate goal being to create a world that is completely decentralized. Where the ownership of digital asset is protected and transferable.

→ On other hand, Distributed DB are centrally managed by a service provider. The goal is to create a logical center that can provide efficient and low cost service with great scalability.

2. Trilemmas :-

Both technologies face technical trilemmas which is referring to difficulty of optimizing tech while balancing tradeoffs.

→ Blockchain trilemma, is concurrently achieving high security, decentralization and scalability.

It's easier to acheive high security & scalability by sacrificing decentralization.

→ DD (Distribute Database) managers must consider bussines support, Engineering Implementation complexities & evolving h/w equipment requirement.

3. Consensus mechanisms:-

→ Blockchain system attempts to solve BGP. with clever algos, thereby becoming BFT. In this way BCT reach Consensus even with malicious nodes.
The most commonly used Consensus mechanism are PoW/PoS & Practical BFT
BFT algorithm often have poor performance with low tolerance of 1/3 faulty nodes.

→ DD system rarely have to solve BGP since there is central point that co-ordinates the system, but do have to consider system failure.
Paxos and Raft Algorithms are used to perform better & process faster.
Tolerate faulty nodes do not exceed over 1/2 of network.

4. The Difference in value proportion.

→ The core value of BCT is not to provide rudimentary data services but to build a new ecosystem of digitalized data asset and automated trust services.

→ On other hand, the DD is to provide data storage and access services to business system. The Database is designed to provide Operational support to business products & development products with data being stored with focus on supporting analysis & retrieval.

## Blockchain through Storage technology

From the birth of Bitcoin in 2008 to emerging generation of blockchain 3.0 the fundamental storage of blockchain has not drastically changed.

The main data structures in blockchain are divided into two categories.

1. Transactions.
2. Blocks.

Transaction trigger updates to blockchain's world state. It itself contains two types of data 1) Input
2) output

Input transaction indicates source of data and transaction output indicates destination of data

Blocks stores transaction data. They are composed of Block header & Body. The Block header records imp meta data, such as hash address of previous block & creation time stamp. The body contains the transaction quantity & complete transac. data.

D.D do not use blocks & transactions.

* Advantages of Blockchain

1. Decentralization:-

Decentralization system is highly fault tolerant.

If any node crashes on Bitcoin network, it doesn't bring the entire system down. The other nodes run the network

It adds more security since the information stored on one computer must be copied to all nodes

If nodes were compromised, a hacker would need to be able to change the information on all nodes to manipulate data. This is proven to be a good safeguard.

3. Immutability :-

A blockchain stores information that becomes immutable; it cannot be changed once block gets validated.

This is also resistant to tampering because the information is stored in distributed ledger stored on many nodes. To compromise, it has to change the information on all nodes.

3. Transparency :-

A key feature of blockchain that provides a benefit to business is transparency. Information about the transaction could not be hidden so this create more trust and adds value to the system.
Blockchain doesn't require any permission.

4. Security :-

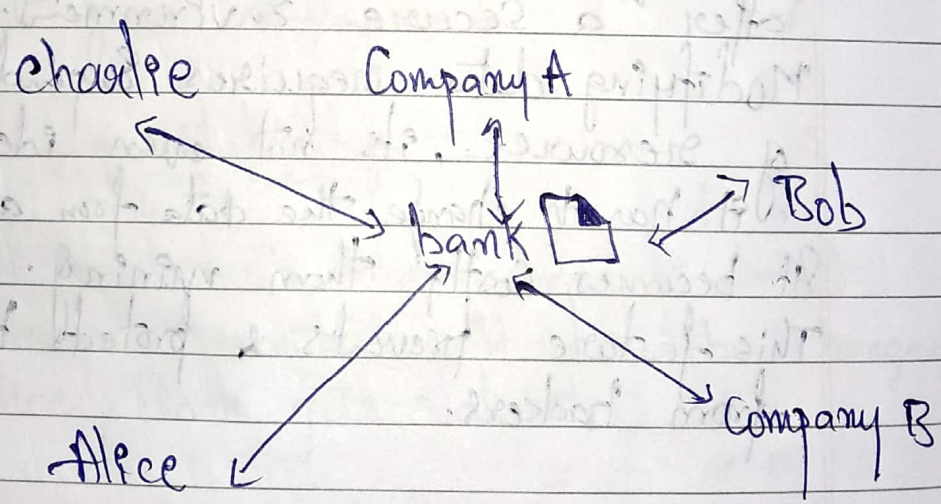
Since blockchain uses advanced Cryptographic techniques & decentralized network they offer a secure Environment.
Modifying data requires Expending plenty of resource, its not even ideal because it has to change the data from all nodes. It becomes costly than mining.
This feature prevents & protects blockchain from hackers.

* Block chain Network:-

Blockchain is a system of recording transaction (not only money) in peer to peer fashion. That means there is no intermediaries in between such as banks and brokers.

Eg:-

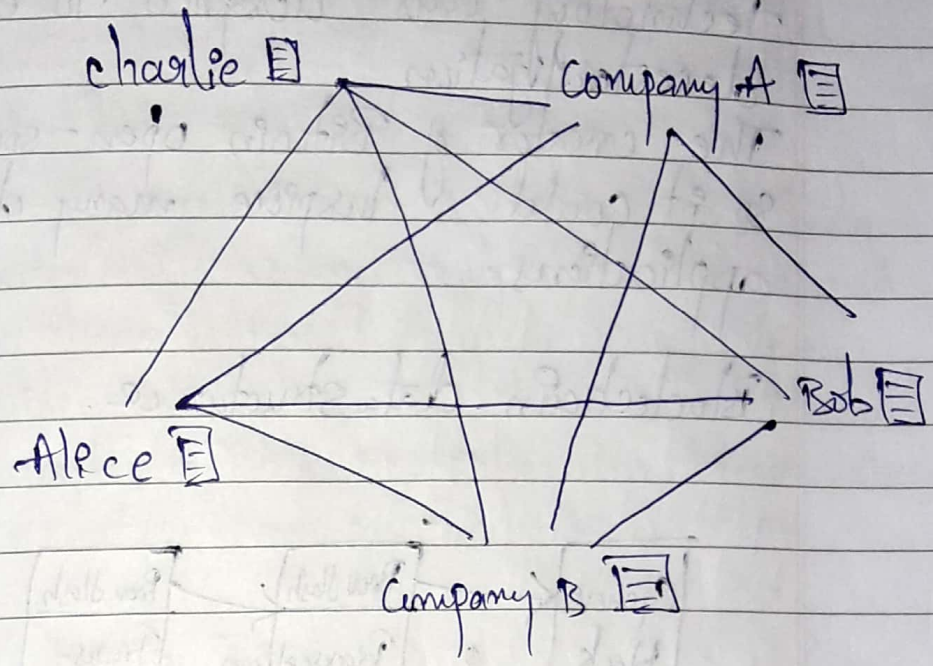
1. Stock settlement through clearing houses




Through intermediaries such as bank.

But,

peer-to-peer trading Blockchain.



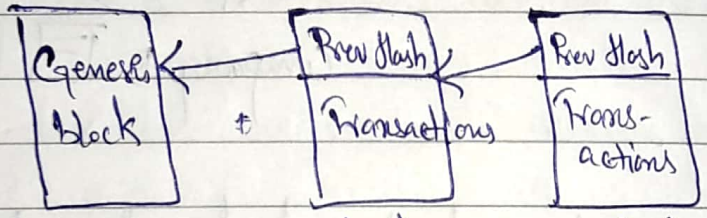

It is shared, decentralized and open ledger of transactions. The ledger database is append-only db and cannot be modified or altered. That means every entry is a permanent Entry.

There is no need for trusted third party to secure and settle the transaction

It is an another layer on top of internet and can coexists with other Internet technologies.

Just like TCP/IP was designed to achieve an Open system. Blockchain technology was designed to enable true decentralization.
The creator of Bitcoin open-sourced it so it could inspire many decentralized applications.

Blockchain data structure.




Everynode on the blockchain network has an identical copy of transactions.

Every node contains block header which stores hash of prev block so that no one can alter any transaction in prev block. The body parts consists of list of validated transactions and some more details.

So given the latest block, it's feasible to access the prev block in blockchain

classmate
Date
Page

# Different types of Blockchain Types:-

There are four major different types.

1. Public Blockchain
It is permissionless distributed ledger technology where anyone can join & do transactions. Any one can access public blockchain if they have internet
Examples:- Bitcoin, Ethereum, litecoin, NEO
Use Cases:- Voting, Fundraising.

2. Private Blockchain
Private Blockchain can be best defined as blockchain that works in a restrictive Environment i.e closed network. It is permissioned blockchain under the control of an entity.
Eg:- Multichain, Hyperledger fabric, Corda
Use-cases: Supply chain, asset ownership, Internal voting

3. Consortium Blockchain or federated.
It is a creative approach to solving the need of organization where there is need of both public & private blockchain. In this some aspects of organization are made public and some private.
Eg:- Macro Polo, Energy web foundation, IBM food trust.

Usecases :- Banking, Research, Food tracking.

4. Hybrid Blockchain :-
It sounds like federated blockchain but it is not, however there can be some similarities between them.
It is defined as a combination of a private & public blockchain. It have use case in organization that neither wants to deploy private blockchain nor public & simply wants to deploy best of both worlds.
Eg :- Dragonchain, Xinfin's hybrid bc
Usecase :- Real-estate, retail, high regulated markets.

* Blockchain Mining :-

The term Blockchain Mining is used to describe the process of adding records to bitcoin blockchain.
The process of Blockchain mining is performed by a community of people around the world called Blockchain miners.

Miners are special type of node that compete in game of creating new blocks & are recorded in terms of bitcoin.

Anyone can apply to become a Blockchain miner. These Blockchain miners install & run a special Blockchain mining software that enables their computer to communicate securely from one another.

Once Computer installs the software, joins the network and begins mining bitcoins, it becomes what is called as nodes.

Together all these nodes communicate with one another and process transaction to add new blocks to the blockchain which is commonly known as bitcoin network.

This bitcoin network runs throughout the day. It processes equivalent to millions of dollars in bitcoin transactions and has never been hacked or experienced a down time since its launch in 2009.

## Types of Bitcoin Mining:-

- Mining process under taken divided into 3 categories.

1. Individual Mining: When mining is done by an individual, user registeration as a miner is neccessary. As soon as a transaction takes place, a mathematical problem is given to all the users

in blockchain network to solve. The first one to solve gets rewarded. Once solution is found, all other miners will validate the decrypted value and adds it to blockchain.

2. Pool mining:-
In this, a group of users work together the approve the transaction. Sometimes complexity of the data encrypted makes it difficult for a user to decrypt data alone. So group of miners works as a team to solve. After validation reward is then split b/w all users

3 Cloud mining:-
It eliminates the need of computer h/w or s/w. Its a hassle-free method to extract blocks. With cloud mining, handling all machinery, order timing, or selling profits are no longer worry

There are two ways to mine bitcoin

1. Mining Bitcoins on cloud
2. Mining Bitcoins on your own

1. Mining Bitcoin on cloud:-

→ Obtain a bitcoin wallet:- Bitcoins are stored in digital wallets in an encrypted manner. This keeps bitcoin safe.

→ Secure the wallet :- Since there is no ownership on bitcoins, anyone who gain access to your wallet can use it without any restrictions. So enable two-factor authentication and store wallet on the computer that does not have internet access or external device.

→ Choose a cloud mining service provider:- They allows user to rent processing or hashing power to mine bitcoins remotely. Eg:- Genesis Mining & HashFlare.

→ Choose a cloud mining package:- To choose a package, you will need to decide on how much you are willing to pay and keep an eye of hashing power the package will offer.

→ Pick a mining pool:- This is the best shot you can get to earn bitcoin easily. There are many mining pools which charge

2% of total earning. Over here, you will have to create workers which are basically subaccounts that can be used to track your contributions to pool.

→ Put your earnings in your own secure wallet.

Whenever you witness an ROI, simply withdraw your earning & put them in your secure wallet..

*2. Mining Bitcoin on your own

1. Purchase Custom mining hardware:- You have to purchase ASIC miner to mine bitcoin. While purchasing consider its hashing power & pricing policies.

2. Purchase a power supply:- Blockchain miners consume a lot of power so get a dependable power supply compatible with ASIC.

3. obtain a bitcoin wallet:- // same as cloud (refer)

4. Secure the wallet:-
// same as mining in cloud. (refer)

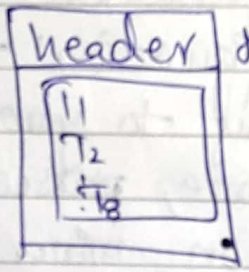
5. Picking a mining pool:-
// same as mining in cloud. (refer)

then:
→ Connect the power supply to ASIC Miner
→ Connect ASIC to router
→ Boot up your ASIC miner
→ Enter router IP address in web browser
→ Find connected device in router miner page
→ Find your ASIC miner and click on it to display device information
→ copy paste your ASIC miner IP address in web browser
→ login to ASIC miner with default credentials username & password as Root & Root
→ Select 'Miner Configuration' to setup miner according to your preferences
→ Enter URL, username, password for your mining pool on miner configuration page of ASIC miner
→ click save & Apply to save for future
→ Start mining & check profitability at regular intervals
→ Put your earnings in secure wallet:
// same as mining in cloud (refer).

# * Merkle Patricia tree

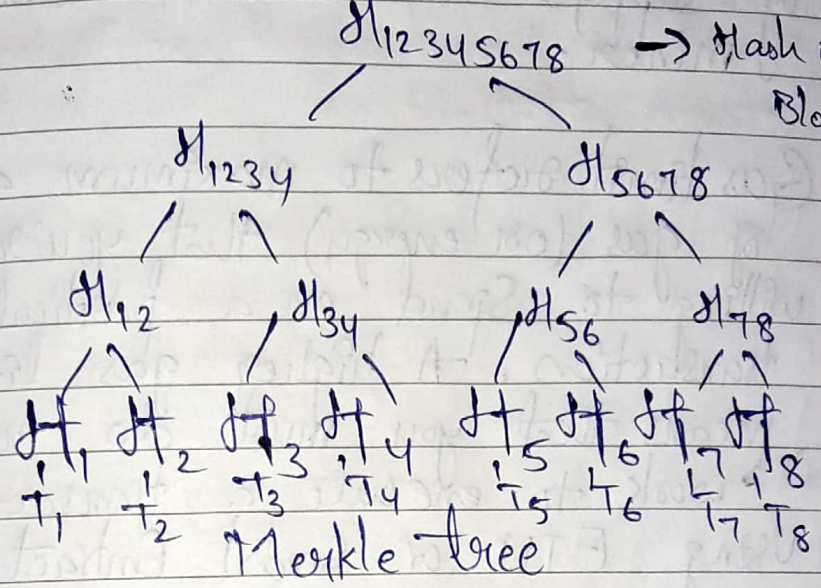
A Merkle tree is a data structure that is used in Computer Science applications. In bitcoin and other cryptocurrency, merkle tree serves to encode blockchain data more efficiently & securely.

In bitcoin blockchain, a block of transactions run through an algorithm to generate a hash. Bitcoin's software does not run the entire block of transactions at once. Instead each transaction is hashed, then each pair of transaction is concatenated & hashed together until we achieved one hash for entire block.




Assume
There are 8 transactions
$T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8$

Hash is calculated going from the leaf nodes.




Merkle tree

The merkle tree is useful because it allows user to verify specific transactions without downloading the whole blockchain.

* Gas and Gas limit:-

Gas refers to fee or pricing value required to succesfully conduct a transaction or execute a contract on ethereum blockchain platform. Priced in small fractions of cryptocurrency ether (ETH).

Gas is used to allocate resource of EVM (Ethereum virtual machine) so that decentralized applications like smart contract can self-execute.

The exact price of gas is determined by supply & demand b/w network's miner.

Gas limit refers to maximum amount of gas (or energy) that you're willing to spend on a particular transaction. A higher gas limit means that you must do more work to execute a transaction using ETH or Smart Contract

If gas limit is too low, then miners can choose to ignore such transactions. price of gas fluctuate with supply and demand for processing power.

* Transaction fee :- Blockchain fee.

The blockchain fee is a cryptocurrency transaction fee that is charged to users when performing crypto transactions. The fee is collected in order to process the transaction on the network.

You need to pay the blockchain fee to ensure your cryptocurrency transfers arrive in a timely manner.

The blockchain fee is one of the tool used to speed up crypto transactions, which are often slow due to high congestion on blockchain network.

The lower the blockchain fee the lower your transaction priority on the network.

## * Block Reward

Bitcoin block reward refers to the new bitcoins that are awarded by blockchain network to eligible cryptocurrency miners for each block they mine successfully.

At inception, each bitcoin block reward was worth 50 BTC. The block reward is halved after discovery of every 210,000 blocks, which takes around four years to complete. As of feb 2019 one block reward was worth 12.5 BTC.

Working on the principle of standard cryptocurrency economy with declining bitcoins awarded as block reward, fewer new bitcoins will be available

Over time that will keep bitcoin price high. After 64 iterations of halving the block reward, it will eventually becomes zero.

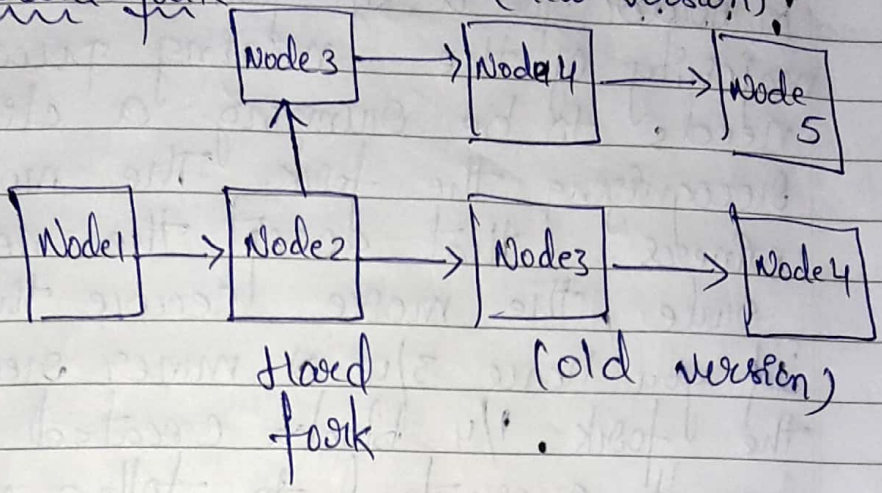
* Hard fork

It is a radical change to a network's protocol that makes previously invalid blocks & transactions valid or vice versa. A hard fork requires all nodes or user to upgrade to the latest version of protocol software

A hard fork is when nodes of newest version of a blockchain no longer accept the older version of blockchain, which creates a permanent divergences from the previous version of blockchain.

Adding a new rule to the code essentially creates a fork in blockchain. One path follows the new upgraded blockchain the other continues to old path, after some time they will realize & upgrade to latest version.

* Hard fork



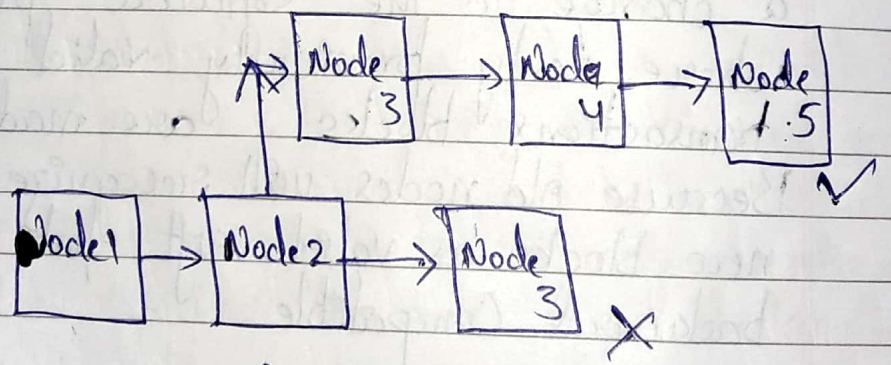

* Soft fork:-

In blockchain technology, a soft fork is a change to the software protocol where only previously valid transactions blocks are made invalid. Because old nodes will recognize the new blocks as valid. soft fork is backward Compatible

A soft fork can also occur at times due to a temporary divergence in the blockchain when miners using non-upgraded node violate a new consensus rules their nodes don't know about.

In order for a soft fork to work, a majority of the mining power needs to be running a client recognizing the fork. The more miners that accept the new rule, the more secure the network. If you have 3/4 of miner recognizing the fork. 1/4 blocks created aren't guaranteed to follow new rules, these are ignored by new nodes.

Soft fork have been used on bitcoin and ethereum blockchain




## * Private & Public Blockchain

### → Public Blockchain

Public blockchain are open network that allows anyone to participate in the network. It is permissionless. In this type of blockchain anyone can join the

network and can read, write and participate within blockchain.
It is decentralized and does not have single entity which controls the network. Data on public blockchain are secure as it is not possible to modify or alter data once they have been validated on Blockchain.

Features:-

1. High Security:- It is secure due to mining (51%).
2. Open Environment:- open to all
3. Anonymous nature:- everyone is anonymous
4. No regulations:- no limit how to use
5. Full transparency:- ledger is available at any time to all participants & everyone participate in consensus
6. True Decentralization:- No centralized entity. Nodes are responsible for updating ledger and promotes fairness using Consensus Algorithm.
7. Full User Empowerment:- Users are empowered as no central authority to look at everymore
8. Immutable:- once written can't be changed
9. Distributed:- No centralization. All nodes participate in validation of transaction.

# Private Blockchain:-

It is managed by a network administrator and participants need to consent to join the network. It is permissioned There will be one or more entities controlling over the network. In this the entities participating in the transaction have knowledge about the transaction whereas others will not able to access i.e Transactions are private

## Features:-

1. Full privacy:-
   focus on privacy concern.
   There are more centralized
2. High Efficiency & Faster Transaction:-
   When you distribute the nodes locally but also less nodes to participate, the performance is faster
3. Better Scalability:-
   Being able to add nodes & services on demand can provide a great advantage to its Enterprise.

# Differences b/w Public & Private Blockchain

| S.No | Basic of Comparision | Public | Private |
|---|---|---|---|
| 1. | Access | Anyl can read, write & participate in blockchain It is permissionless | Read & write is done upon invitation. It is permissioned |
| 2. | Network Actors | Don't know each other | know each other |
| 3. | Decentralized vs centralized | Decentralized | more Centralized |
| 4. | Order of magnitude | order of magnitude is lesser than Private Blockchain as it is lighter & provides transaction throughput | The order of magnitude is more |
| 5. | Native Token | Yes | not neccesary |
| 6. | Speed | slow | fast |
| 7. | Transaction/sec | lesser | more |
| 8. | Security | More secure due to decentralization Due to more no. of nodes its Impossible to attack the System | less secure. It is more prone to hacks, frisks & data breaches. |

| | | | |
|---|---|---|---|
| 9 | Energy Consumption | more energy Consumption | less energy Consumption |
| 10 | Consensus Algorithm | Proof of work, Proof of stake, proof of burn, proof of Space | Proof of Elapsed time Raft Istanbul BFT |
| 11 | Examples | Bitcoin, Ethereum, monero, zcash, Dcash, litecoin | R3, B3i Corda |