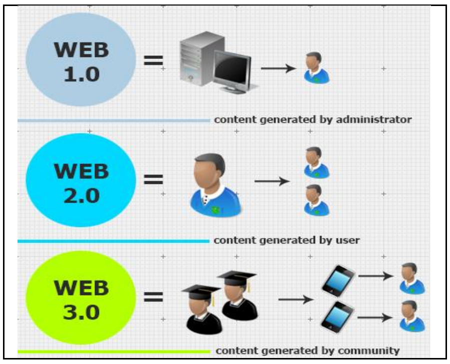
FUNDAMENTAL OF BLOCKCHAIN

WEB 1.0 V/S WEB 2.0 V/S WEB 3.0


WEB 1.0
=
content generated by administrator
WEB 2.0
=
content generated by user
WEB 3.0
=
content generated by community

- ***Web 1.0***

  1989 – 2005 (Read only)

- ***Web 2.0***

  2005 – Present (Read & Write)

- ***Web 3.0***

  Yet to come (Read, Write & Own)

What is Web 1.0?

Web 1.0 is the term used to describe the earliest form of the internet. This was the first example of the global network, while offered the potential for the future of digital communication & information sharing.

Basically, web 1.0 was a few people writing content and web pages for a large amount of people. So, people could access facts, information, and content from the source.

Example of Web 1.0:-

a) Static pages.
b) HTML forms sent via email.
c) Contact form the server's file system, rather than a relational database management system.
d) Gif buttons & graph.

What is Web 2.0?

With Web 2.0 the focus moved away from a small amount of people making a large amount of people making even more content.

So it's not just about reading, it's about contributing. Now that doesn't mean everyone's is a YouTuber, TikTok-er. Instead this can mean creating a profile on site, or leaving comments & reviews.

Basically all the users of web 2.0 has become the product. Web 2.0 or the 'Social Web', involves a number of tools & platforms where people can share their opinion, day to day, and perspective in hyper interactive day.

Example of Web 2.0 :-

a) Podcasting.
b) Social media.
c) Tagging.
d) Blogging.
e) Commenting.
f) Voting.

The main issue with web 2.0 comes from the way the traditional web 2.0 application works. A user will make a request to the server, which will then be sent to the web pages as a response. The only thing is whoever controls the data on the centralized server has access to a hall of a lot of data. The bitter trust is our data was sold to advertisers.

What is Web 3.0?

Web 3.0 is described as “read, write & own”. It is known as the future of the internet. It involves a spaces where people operate on decentralised, almost anonymous platforms. This means moving away from the big, guiding hands of tech giants like Google, Facebook & Twitter.

Web 3.0 was originally called as the Semantic web by World Wide Web. Inventor Berners Lee, and was convinces as a more autonomous, intelligent, and open internet.

Berners Lee web 3.0 was describes as a place where there is no permission is needed from a central authority to post anything. There is no central authority, and so no single point of failure.

Example of Web 3.0 :-

a) Semantic web where web tech is improved to create, share, and connect through search & analysis, based on comprehensive not keyword.

b) Artificial Intelligence & Machine learning.

c) Connectivity of multiple applications & devices, through the internet of things.

d) 3-Dimensional graphics.

e) Interactivity without need to go through a trusted intermediary.

f) Participation without the need for authorisation from the governing body.

CENTRALISED V/S DECENTRALISED V/S DISTRIBUTED

1. Centralised :-

A centralised network is built around a single, central server that handles all major management & data processing functions. Client system & users cannot directly access resources or services on different servers without first going through the centralised master servers. If the central server goes down, the entire network goes down with it. An example of a centralised network would be a small business using a single domain controller (D.C). A single central server is quick and easy to deploy because you only have to manage one configuration without load balancing.

2. Decentralised:-

A Decentralised network architecture uses multiple servers in place of a single centralised server. Each of these servers can act as an independent master slave, with the necessary workloads distributed access them for load balancing. If one server goes down, another server can take over its load to minimize network interruption.

Decentralised networks are more reliable then centralised network because these are multiple point of failure.

Decentralised network are more expensive & time consuming to display because you need to install & configure multiple servers with load balancing fail over capabilities.

3. *Distributed:-*

In a distributed network, all network services & coordination task are split evenly among many equal servers across the entire enterprise network.

A distributed network doesn’t use a single central server where all data processing, computational resources, and network management functions are shared by nodes distributed geographically & logically access the whole enterprise network. Distributed networks & extremely fault tolerant because any servers can fail independently without impacting the rest of the network at all that servers functions are automatically shared among the other available servers.

Distributed network management is more expensive because it requires network load balancing tools to provide continuously load balancing and ensure that all nodes coordination with each other for configuration and routing updates & changes to security policies.

BLOCKCHAIN

Blockchain is peer to peer decentralised distributed ledger that records transection efficiently, and in a verifiable & robust fashion.

Blockchain is a transaction where we can store the database records that is distributed, validated and maintained around the world by a network of computers.

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

A Blockchain is essentially a digital ledger of transaction that is duplicate & distributed across the entire network of computer system on the blockchain.

Each block in the chain contains a number of transactions, & each time a new transaction occurs on the blockchain, a record of that transaction is added to every participant ledger.

The decentralised database managed by multiple participants is known as distributed ledger technology (DLT).

Blockchain is a type of DLT in which transaction are recoded with an immutable cryptographic signature called as hash.

Types of Blockchain

Types of Blockchain	Public	Private	Federated
Access	Anyone	Single Organisation	Multiple selected organisation
Participants	Permission less & anonymous	Permissioned & known identities	Permissioned & known identities
Security	consensus, POW & POS	Pre-approved participants, voting basis consensus	Pre-approved participants, voting basis consensus
Transaction speed	Slow	Lighter & faster	Lighter & faster

APPLICATION OF BLOCKCHAIN TECHNOLOGY

Industries, developers & communities build blockchain application to serve a specific purpose. There are various examples of applications being built on blockchain, some of major working applications are:-

1. Humaniq:- A fintech start-up which connects unbanked people with global economy.
2. Augur:- A peer-to-peer oracle and predication market place.
3. Ether roll:- Etherium powered trust less betting platform.
4. Cryptokitties:- Blockchain based game centred around breedable, collection & digital assets.
5. Golem :- Etherium start-up aimed at decentralizing cpu processing.

APPLICATION SCENARIO OF BLOCKCHAIN TECHNOLOGY

1. ***Financial Market:-*** It is an integral part of blockchain innovation research. For example, blockchain can create a secure and reliable peer-to-peer financial market. Noise has developed a method that combines peer-to-peer algorithms & MPC (Multi Party Computing) protocol to make a p-to-b (peer-to-business) financial MPC market.

2. ***Data Analysis & Data Management:-*** Blockchain contain usual technical compensation over large data application. In data organisation, blockchain & has spread & safe skin allow it to amass significant data and make sure that it is a data source.

   Based on data analysis, blockchain operations allow for general convenience for extensive data analysis. For example, Obtaining customers transaction methods can analyses the business behaviour of potential partners.

3. ***Identification:-*** Blockchain safety, security & reliability using in the meadow of identification. The blockchain feature uses to remove the requirement for trust third parties and verify and protect the individuality in secret and verified method. It feels like routine control of individual information.
4. ***Ownership Management:-*** Blockchain knowledge is helpful in owner organisation, property possession, & legal investments. It uses to defend the authenticity of verification in sequence by storing time & personal keys when storing & legally investing in copyright information.

5. ***Logistic chain:-*** In normal mode manufactures customer products have to go through many intermediate connections & it is challenging to trade abroad. At the same time, the market is full of counterfeit and monotonous products. As different companies store information about the supply chain, the information does not change, and the lack of transparency leads to an expensive logistic procedure.

COMPONENTS OF BLOCKCHAIN TECHNOLOGY

1. ***Cryptography:-*** Use of verity of cryptographic techniques including cryptographic one-way, hash function, Merkle tree & public key infrastructure (private public key pairs).

2. ***Peer-to-peer Network:-*** Network for peer discovery and data sharing in a peer-to-peer fashion.

3. ***Validity Rule:-*** Common set of the network (i.e. what transaction are considered valid, how the ledger gets updated, etc).

4. ***Ledger:-*** List transactions bundled together in cryptographically linked blacks.

5. ***Consensus Mechanism:*** - Algorithm that determine the ordering of transaction in an adversairal environment (i.e. assuming not every participant is honest).

HASHING ALGORITHM

1. ***Cryptographically secured hashing algorithm:-*** Hash is just like a fingerprint. Fingerprint will be unique for everyone. Hash is one way encryption & it cannot be decrypt.

- ***What is Encryption?***
  Converting the plain text (readable text) into cipher text (unreadable text) is known as encryption.

- ***What is Decryption?***
  Converting the cipher text into plain text is known as decryption.

- ***What is Cryptography?***
  The process of encryption & decryption is known as cryptography.

2. ***SHA-256 hash algorithm:-*** Secure hash algorithm 256 is nothing but the 256 hexadecimal values. This SHA-256 hash algorithm is going to convert any random (one word, two word or multiple words a group of sentence also) text is going to convert into a fixed length of 256 hexadecimal value.

- ***What is an algorithm?***

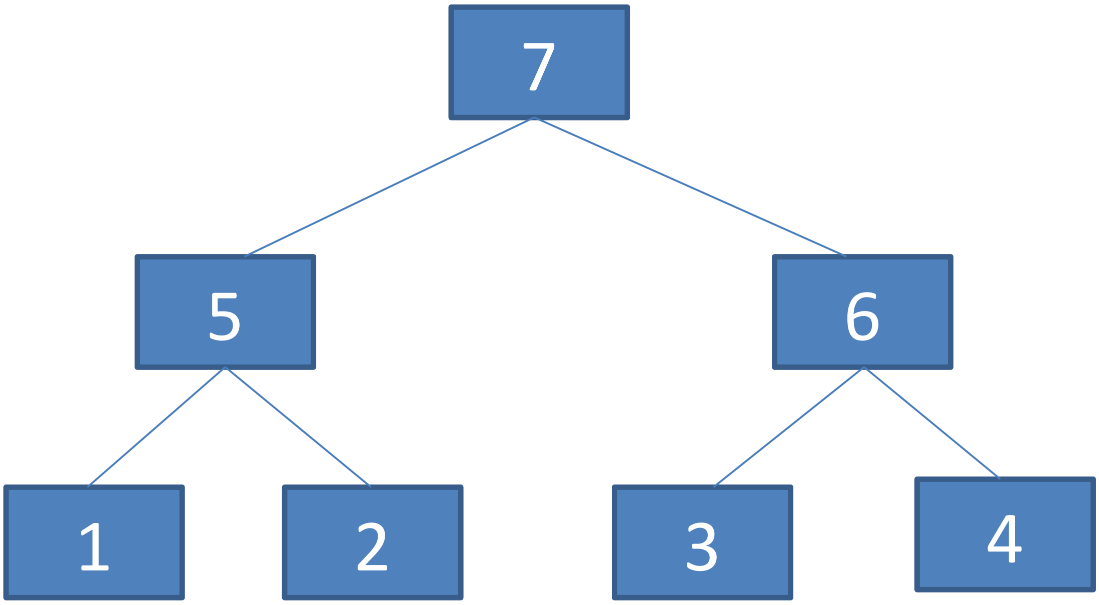
  It is a finite number of steps written to accomplish some specific fast.
  i.e. (Adding of two numbers :-
  Step 1 - Take 2 variables 'num1' & 'num2'.
  Step 2- Initialise the variable 'num1=2, num2=3'.
  Step 3- Take a new variable called 'sum'.
  Step 4- Assign 'sum= num1 + num2'.
  Step 5- Print the value of 'sum'.

3. ***Merkle tree:-*** The way it comes to blockchain we have a lot of blocks & then these blocks will be connected with the help of hash values. Every block will have transactions. Now this can be one transaction of thousands

of transaction & than we want to find the hash value of the block. So in the case we need to find the hash of each transactions or we need to find one hash for all the transaction. For finding the hashes of all the transaction we have to store all the hashes. It is very difficult to store all the hashes of all the transaction because it is not like that one block will have only one transaction some blocks may contain thousands of transaction. But we don’t want all the hashes in the block header. We want only one hash for one block. We have merkle tree concept. Merkle tree will have again leaves like left leaf & right leaf.

For example in one block you have 4 transactions we need to start calculating the hash of each transaction. So we will get 4 hashes for 4 transactions.

In a block each transaction has its own hash and by combining those hashes according to concept of merkle tree we will get a single overall hash of that single block.



We need to compile that hash of 1&2, 3&4 Then we will get hash of hash 5 & hash 6. Finally we need to combine the 2 hash into one hash i.e. hash 7.

For even number of transaction we can find this root has easily what of we have odd numbers of transaction. Then simply duplicate the last transaction to make it even & start finding root hash.

- ***Shared immutable distributed ledger :-***
    - Every node maintains a local copy of the global datasheet.
    - The system ensures consisting among the local copies.
    - The local copy of every node is identical.
    - The local copies are always updated based on the global information.

- ***What is peer-to-peer network?***
    - In a peer-to-peer network, there is no central governing authority.
    - All nodes in peer-to-peer distributed network are equal to each other.
    - Anyone connected to the network is free to share & download any file share by other users in the network.
    - Peer-to-peer systems are classified as unstructured, structured & hybrid p-to-p network.

BLOCKCHAIN V/S CRYPTO CURRENCY

A blockchain is decentralised ledger of all transaction across a peer-to-peer network, whereas crypto currency is a medium of exchange, created & stored electronically in the blockchain.

Basis of comparison	Blockchain	Crypto currency
Nature	A technology that records transaction.	The tools used in the visual exchange
Use	Record transaction	Make payments, investments, storage of wealth.
Value	Have no monitory value	Have monitory value
Mobility	Can't be transferred	Can be transferred

FUNGIBLE & NON-FUNGIBLE TOKENS

- ***Fungible Tokens***
  - These tokens are easily interchangeable although there is no additional value associated with interchanging fungible tokens.
  - Value transfer depends on the number of tokens in an ownership of a person.
  - Fungible tokens can be divided into smaller parts & the smaller parts can help in paying off the large source.

- ***Non-fungible Tokens***
  - These tokens are not interchangeable as each of them represents unique assets.
  - The value of the unique asset represented by NFT is helpful in their value transfer.
  - NFT’s are not divisible & have their value use a whole entity.
  - Non Fungible tokens leverage the ERC-721 stands.

DAPP

- DApps are Decentralised Apps. They are like normal apps, and offer similar functions but the key difference is they are run of peer-to-peer network such as blockchain.

- That means no one person or identity has control of the network. There are other key features such as :
  a) It must be open-source & operate on its own without anyone entity controlling it.
  b) Its data & records must be public.
  c) It's must use a cryptographic token to help keep the network secure.

MINING

It is a process of validate of adding transaction records to the blockchain network & confirm the same to the rest of the network.

Mining is intentionally designed to be resource intensive and difficult so that the number of blocks found each day by miner remains steady and spam attacks could be controlled.

Miner serves as two purpose:

1) To verify the legitimacy of transaction, or avoid the so called double spending problem.
2) To create new digital currencies by rewarding miners for performing the pervious task.

Mining could be done using different models or mechanisms. Proof of work was the original model that bit coin blockchain had introduced to all of us.

WHAT IS PROOF OF WORK?

If we don't have a proof of work mechanism in mining process. In one minute thousands if not millions of blocks easily could be added to the blockchain network. In order to minimize this, so that there is no spam add a block is properly validate with adequate time, a mining mechanism called as proof of work is added to the system. Individual blocks must contain a proof of work to be considered as valid. This proof of work is verified by others bitcoin nodes each time when they receive a block.

Bitcoin uses the hashcash proof of work function. If this hashcash function the following things happen: -

1) First transactions are bundled together into what we call a block.
2) Miners verify that transactions within each block are legitimate.
3) To do so miners should solve a mathematical puzzle known as proof of work problem.
4) A reward is given to the first miner who solves each block problem.
5) Verified transactions are stored in the public blockchain.

CONSENSUS WITH PROOF OF WORK

As soon as a new transaction is added it’s broadcast to all nodes & the mining nodes start working to solve the proof of work puzzle. Who whoever finish it first broadcast it to others. Nodes accept the block only if all transactions in it are valid & not already spent.

The transaction is confirmed and added to the blockchain only if a minimum percentage of all nodes accept it.

For bitcoin blockchain, originally the percentage was 51% matching the democratic voting models in the world.

However soon it was observed that more than 51% of computing power in bitcoin network lies with handful miners today.

Hence people soon tried to increase this consensus percentage from 51% to higher rates. Ripple blockchain framework today uses 80% of consensus model.

USAGE OF PUBLIC & PRIVATE KEYS IN BLOCKCHAIN?

Blockchain is a public network & any transaction that happens on the network should not be visible to all.

In order to do so we use public and private keys.

Private keys is a secret key kept by the user only to self.

The public key is derived from private key & are known to the world.

Any data that is encrypted by one of the keys can be decrypt by the other.

WHAT IS CRYPTO WALLET?

A crypto currency wallet digitally stores a user's public & private keys and programmatic-ally helps in sending & receiving digital currency.

FORK IN BLOCKCHAIN

Crypto currency like bitcoin & ether are powered by decartelised, open source software called a blockchain. A fork happens whenever a community makes a change to the blockchains protocol or basic set of rules.

TYPES OF FORK IN BLOCKCHAIN

There are 2 types of fork in blockchain:-

1) Soft fork

Think of a soft fork as a software upgrade for the blockchain. As long as it's adopted by all users, it becomes a currencies new set of standard.

Soft fork have been used to bring new features or functions, typically at the programming level to both bitcoin & Ethereum because the end result is a single blockchain, the changes are backward compatible with the pre-fork blocks.

2) Hard fork

A hard fork happens when the code changes so much the new version is no longer backward compatible with earlier blocks.

In this scenario, the blockchain splits in 2:-

a) The original blockchain & new version that follows the new set of rules.

b) This creates an entirely new crypto currency is the source of many well-known coins.

WHY DO FORKS OCCUR?

Just like all software needs upgrades, blockchain are updated for verity of reasons.

a) To add functionality

b) To address security risk.

c) To resolve a disagreement with the community about the crypto currency direction.

HOW BLOCKCHAIN WORKS

- ***Steps involved before transaction completes in the blockchain network:***

1) If someone request transaction in a blockchain network.
2) The request transaction is broadcast to a p-to-p network consisting of computers known as nodes.
3) The network of nodes validates the transaction & the user's status using known algorithms.
4) A verified transaction can involve crypto currency, contracts, records, or other information.

- ***Steps involved after transaction is completed in a blockchain network:***

  1) The transaction is completed after successful verification.
  2) The new block is then added to the exiting blockchain, in a way that I permanent and unalterable.
  3) One verified, the transaction is combined with other transaction to create a new block of data for the ledger.

TYPES OF NODES IN BLOCKCHAIN

1) Archival full Nodes

   It stores the entire blockchain ledger, which includes all transaction from the beginning to the present, lots of memory is required.

2) Pruned full Nodes

   It holds the most recent blockchain transaction up to its set memory limit.

3) Light Nodes

   It store only block headers. It sticks with essential data.

4) Master Nodes

   It validates transaction & maintain a record of the blockchain, but can’t add blocks to the blockchain.

5) Mining Nodes

   It participants in crypto mining process.

6) Authority Nodes

   It is used by organisation in charge of blockchain where nodes must pass through a vetting process.

7) Staking Nodes

   It locks up crypto currency funds as collateral. It is used to confirm transaction.

8) Lightening Nodes

It creates a separate network for user to connect to off the blockchain enabling off-chain transactions. Useful for congested networks.

CONSENSUS MECHANISM

A consensus mechanism is a fault-tolerant mechanism that is use in computer & blockchain system to achieve the necessary agreement on a single data value or a single state of the network among distributed process or multi-agent systems, such as with crypto currencies.

It is useful in record-keeping, among other things. On the Bitcoin Blockchain, for instance, the consensus mechanism is known as proof of work (POW), which requires the excretion of computational power in order to solve a difficult but arbitrary puzzle in order to keep all nodes in the network honest.

BLOCKCHAIN CONSENSUS MECHANISM

There are different kinds of consensus mechanism algorithm, each of which works on different principles.

➢ *Proof of work*

PoW represents Proof of Work.

It was first introduce in 1993 by Dwork & Naor & reinstate by Satoshi Nakamoto in the bitcoin record in 2008.

PoW selects a miner for producing the next block.

The objective behind PoW is to find a solution for a difficult mathematic puzzle.

The miner who initially solves the problem gets to mine the next block.

This algorithm is used by bitcoin and requires much computational power for finding the solution to the puzzle.

➢ *Proof of Stake*

PoS represented Proof of Stake.

PoS was first introduced in 2011 as low-cost, low-energy consuming alternative to PoW.

In PoS, miners don’t require expensive hardware for solving a tricky puzzle instead the miners lock up their coins as a stake and authenticate the block by placing a bet.

Once a new block is added all the validators get rewarded equal to their bets and increase the state accordingly.

Ethereum uses this kind of algorithm for mining.

➢ *Delegated Proof of Stake*

DPoS stands for assigned Proof-of-Stake.

It was first introduced by Daniel Larimer.

In DPoS, delegates vote for their special validators to achieve a consensus for a new block and the selected validators are responsible for maintaining the network and validating the transaction.

In return, the validator receives rewarded with transaction fees for the work.

This consensus algorithm is used by EOS, Bitshares, Tezos, Steem, etc, for validating transaction in the block.

➢ *Proof of Burn*

PoB represents Proof of Burn.

As the name suggests, in POB validators ‘burn’ coins by sending them to an address where they are not fixable.

It’s on miners to burn the native currency or any of the currency of their choice.

More the coins a miner burns, the higher is the chances of his selection to mine the next block.

Though PoB wastes resources, PoB is the best alternative of POW.

The only coin which uses Proof-of-Burn is Slimcoin, it uses a mix of PoS, PoW, & PoB.

➢ *Proof of Capacity*

PoC represents Proof of Capacity.

In Proof of Capacity algorithms, instead of burning coins or investing in high-cost hardware resources, validators are supposed to fill in their hard drive space.

The more hard drive space validators allocate, the better are the validators chance of getting selected for mining the next block for earning for block award.

➢ *Proof of Elapsed Time*

PoET represents Proof of Elapsed Time.

PoET is one of the fairest consensus algorithms which choose the next block using fair means only.

It is widely used in permissioned Blockchain networks.

In this algorithm, every validator on the network gets a fair chance to create their own block.

All the nodes do so by waiting for random amount of time, adding a proof of their wait in block.

The created blocks are broadcast to network for others consideration.

The winner is the validator which has least timer value in the proof part.

The block from the winning validator nodes gets appended to the Blockchain.

There are additional checks in the algorithm to stop nodes from always winning the election, stop nodes from generating a lowest timer value.

➢ *Byzantine Fault Tolerance*

The Byzantine general problem is a game theory problem, which describes the difficulty of the decentralised parties have in arriving at consensus without relying on a trust central party.

Byzantine Fault Tolerance is a feature of a distributed network to reach consensus (agreement on the same value) even where some of respond with incorrect information. The objective of BFT mechanism is to safeguard against the system failures by implying collective decision making (both correct & faulty nodes) which aims to reduce to influence of the faculty nodes.