Camlin Page
Date / /

Blockchain Technology :-

→ Blockchain :- A blockchain is a distributed database that maintains a continuously growing list of ordered records, called blocks. These blocks are linked using cryptography. Each block contains a ~~typ~~ Cryptographic hash of the previous block, a timestamp and transaction data. A blockchain ~~is~~ is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the ~~it~~ record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of network.

→ Blockchain Explained :- Blockchain gives its name to the way it stores transaction data in blocks, linked together to form a chain. As the number of transaction grows, so does the blockchain. Blocks records and confirm the time and sequence of transactions, which are then logged into the blockchain, within a discrete network governed by rules agreed to by the network participants.

" Each block contains a hash, timestamped batches of recent valid transactions, and the hash of the previous block. The ~~pre~~ previous block hash links the blocks together and prevents any block from being altered or a block ~~being~~ being inserted between two existing blocks.

* The four key concepts behind blockchain :-

- Shared ledger :- A shared ledger is an "append-only" distributed system of record shared across a business network.

- Permissions :- Permissions ensure that transactions are secure, authenticated and verified.

- Smart Contracts :- A smart contract is "an agreement or set of rules that govern a business transaction"; it's stored on the blockchain and is executed automatically as a part of a transaction.

Consensus :- Through consensus, all parties agree to network-verified transaction. Blockchain have various ~~forms~~ consensus mechanism.

→ Peer-to-Peer Networks :- A peer to peer network is a decentralized communication model between two peers also known as nodes, which can communicate with each other without the need for a central server. Unlike the seeder / leecher model in ~~which a~~ which a seeder makes the request and a leecher fulfills the request, the P2P network model allows each party to function as both a seeder and as a leecher. This means that the network, once formed, can be used by the participants to share and store files without the help of an intermediary.

* How do peer-to-peer Networks works?
A peer-to-peer model is maintained by a distributed

networks of Computers. This means the computers don't have a server or central administrator as each node holds holds a copy of the files - acting as both a server and a client. Therefore, each node can upload files for other nodes or download files from them. These nodes use their own hard drives to store their data instead of a central server.

Since, each node has common capabilities to store, transmit and receive files, P2P networks tend to be faster and more efficient.

→ Bitcoin Mining :- Bitcoin mining is a computation-intensive process that uses complicated Computer code to generate a secure cryptographic system. The bitcoin miner is the person who solves mathematical puzzles to validate transactions. Anyone with mining hardware and Computing power can take part in this. Numerous miners take part simultaneously to solve the complex mathematical puzzles, the one who solves it first, wins bitcoin. Miners verify the transactions and then and then adds the block to the blockchain when confirmed.

Why do bitcoin needs to be mined?

Bitcoin is a digital currency where there are chances of copying, and counterfeiting, or double-spending the same coin more than once. Mining solves these problems by making the above illicit activities extremely expensive and resource intensive.

* Why mine Bitcoins?

Ans. • Mining bitcoin helps support the Bitcoin ecosystem.
• Bitcoin mining helps miners to earn rewards in form of bitcoins.
• It is the only way to release new ~~cop~~ cryptocurrencies into circulation.
• It is used to check counterfeiting and double spending.

→ Immutable ledger?

An immutable ledger is a record-keeping system that is permanent and immune to data corruption. In contrast to traditional databases, ~~where~~ where data can be modified or deleted, an immutable ledger operates on the principle that once information is recorded, it cannot be altered.

Immutability mean in the context of an immutable ledger, refers to the inability to change or ~~falsify~~ falsify recorded data. This is specifically true about transaction recorded on the blockchain, which become mostly permanent and resistant to modification.

* How it works?

Ans An immutable ledger relies on various consensus mechanism that use cryptographic techniques to make the data immutable. When a transaction is added to the ledger, it is cryptographically linked to previous ~~th~~ transaction, forming a chain of blocks, which is known Blockchain.

Each block contains a reference to the previous one, creating a continuous and tamper-proof record of all transaction. All new information that follows that freshly added block is compiled into a newly formed block that will also be added to the chain.

→ Smart Contracts :- A Smart Contract is a computer program that directly and automatically controls the transfer of digital assets between the parties by under certain conditions. A Smart contract works in the same way as a traditional contract while also automatically enforcing the contract. Smart contracts are programs that execute exactly as they are set up by creators.

* How it works?

Ans A Smart Contracts is just a digital Contract with the security coding of the blockchain.

- It has details and permission written in code that require an exact sequence of events to take place to trigger the agreement of the terms mentioned in the Smart Contract.
- It can also include the time constraints that can introduce deadlines in the contract.
- Every Smart contract has its address in the blockchain. The Contract can be interacted with by using its address presuming the contract has been broadcasted on network.

Ex :- If you send object A, Then the sum will be transferred to you.

Smart Contract	Traditional Contract
i) Legally binding only if they are in compliance with the applicable laws.	i) A legally binding agreement that is enforceable in court.
ii) Automatically executed and enforced when the terms of the contract are met.	ii) Executed and enforced through the court system.
iii) Can be validate by anyone in the blockchain network.	iii) Valid only if both parties agree and sign the contract.
iv) Records stored on a blockchain and can be viewed publicly.	iv) Records stored in paper form or digitally, not publicly available.
v) All activities all traceable on the blockchain.	v) Tracing activities is difficult as the contract is stored in paper form or digitally.
vi) Difficult to modify once deployed.	vi) Easily modified and amended with mutual consent of both parties.

→ Blockchain Hash function :- A hash function takes an input string of any length and transform it takes into a fixed length. The fixed bit length can vary depending on the hash function which is being used. The fixed length output is called a hash. This hash is also the cryptographic byproduct of a hash algorithm.

Camlin Page
Date / /

* SHA-256 :- A bitcoin's blockchain uses SHA-256 hashing algorithm.

Since the Hash function is a one-way function, there is no way to get back entire text from the generated hash. This is different from traditional cryptographic functions like encryption where you can encrypt something using the key and by using decryption, you can decrypt the message to its original form.

→ Proof of Work :- Proof of Work consensus is the mechanism of choice for the majority of cryptocurrencies currently in circulation. The algorithm is used to verify the transaction and create a new block in the blockchain.

* Purpose of POW :- The purpose of a consensus mechanism is to bring all the nodes in agreement, that is, trust one another, in an environment where the nodes don't trust each other.

- All the transaction in the new block are then validate and the new block is then added to the blockchain.

- The block will get added to the chain which has the longest block height

- Miners perform computation work in solving a complex mathematical problem to add the block to the network, hence named Proof-of-Work.

* Bitcoin's PoW System :- Bitcoin uses the Hash Cash Proof of Work System as the mining basis. The 'hard mathematical problem' can be written in an abstract way like below :

Given data A, find a number x such as that the hash of x appended to A results in a number less than B.

- The miners bundle up a group of transactions into a block and try to mine. To mine it, a hard mathematical problem has to be ~~sola~~ solved.

- This problem is called the proof of work problem which has to be solved to show that the miner has done some work in finding out the solution to the problem and hence the mined block must be valid.

- The answer to the problem needs to be a lower number than the hash of the block for it to be accepted, known as the 'target hash'.

- A miner continues testing different unique ~~word~~ values until a suitable one is produced.

- The miner who ~~mm~~ manages to solve the problem gets the bitcoin reward and adds the block to the ~~bl~~ blockchain by broadcasting that the block has been mined.

A target hash is a number that the header of a hashed block must be equal to or less than for a new block, along with the reward, to be awarded to a miner.

A lower a target is, the more difficult it is to generate a block.

→ Blockchain Wallet :-

A blockchain wallet is a cryptocurrency wallet that is used to manage cryptocurrencies like Bitcoin or ~~Ether~~ Ethereum. It helps to exchange funds easily and the transactions are more secure as they are cryptographically signed. The privacy and the identity of users are maintained and it provides all the features that are necessary for secure and safe transfer and exchange of cryptocurrencies.

- A public key is similar to an account number. If A wants to send some money to B using Bitcoin when A sends the public key address to B. Anyone can send Bitcoin using the pulic key.

- A private key is similar to an account password. Only the account holder knows the ~~pri~~ private key. The private key is used to send money.

→ Features :-

i) ~~Sooo~~ Secure
ii) Easy to use
iii) Low transaction fees
iv) Instant transactions.

* Why use of Blockchain Wallet :-

i) Transactions are often slow in traditional banking systems and have to pass through an intermediary, which means that there is a single central point of failure.

ii) There is an issue with keeping track of all the transactions, and ~~account~~ accounts, the data can get manipulated or even corrupted across multiple systems.

..... Blockchain wallets reduce all of these problems and hence make the transactions secure and safe for the users.

* How do Blockchain Wallets Works :-

Ans The Blockchain wallet stores the private keys and public keys for a transaction. The ~~wattet~~ wallet enables users to sell and purchase goods using Cryptocurrencies.

- When a ~~block~~ blockchain wallet is created, a public key is generated and one can share that public ~~key~~ key with anyone in order to receive funds.

- ~~Private~~ Private Keys as the ~~same~~ name suggest is a secret key that cannot be shared with anyone.

- Public keys on the other hand can be shared with anyone.

- They have a relationship similar to a lock and a key, where a lock can be opened with a correct matching key only, Similar in a transaction if a public key matches the private key only then the users can see the value of their assets.

- No matter how many people have a public key but it will only be useful when when it is paired with the right private key.

* Types of Blockchain Wallets :-

i) Hot Storage :- it refers to the type of storage that is connected to the Internet. Hot storage being connected to the internet, allows the user easy and quick access to funds. It is ~~helpfull~~ helpful in daily transaction.

a. Online Wallets
b. Desktop Wallets
c. Mobile Wallets

ii) Cold Storage :- Cold storage refers to the type of storage that is not connected to the internet. Cold storage provides a higher level of security than hot storage. It is used for long-term storage. It is not ideal for daily transaction.

a. Hardware Wallets
b. Paper Wallets

- Multi-Signature wallet :- Multi-Signature wallets are those wallets that require more than one private key to execute a transaction. The number of of private keys required depends upon the initial Configuration of that wallet. This means that it can perform transactions that require Bitcoin etc. using some wallet.

- Multi-Currency Wallet :- are those types of wallets that allow the user to store more than one crypto-currency in the same wallet. This means that it can perform transactions that require Bitcoin etc. using some wallet.

Mempool :- Mempool or memory pool refers to a backlog of pending and unconfirmed transactions in a blockchain. These unconfirmed transactions wait in the mempool to get validated and finalized in the upcoming block.

when you transact on a blockchain network, your crypto payments or transfers are not immediately confirmed. Your transaction have to validated by miners on proof-of-work blockchains and by validators on proof-of-stake blockchains, who compile pending transactions into blocks. Your transactions are only considered final once it is included in a block. Until then, your transactions will wait in a queue alongside all the other unconfirmed transactions in a place called the mempool.

Permissionless Blockchain :- It is also known as trust trustless or public blockchains, are available to everyone to participate in the blockchains process that use to validate transactions and data. These are used in the network where high transparency is required.

Characteristics :-

i. has no central authority
ii. The platform is Completely open-source.
iii. Full transparency of the transaction
iv. Heavy use of tokens.

→ Permissioned Blockchain :- These are the closed network only a set of groups are allowed to validate transactions or data in a given blockchain networks. These are used in the network where high privacy and security are required.

+ characteristics :-

i. It does not have a central authority
ii. Developed by ~~private~~ private authority
iii. Another feature is the lack of anatomy as only a limited number of users are allowed

Types ~~are~~ of Blockchain :-

i. Public Blockchain :- These ~~block~~ blockchains are completely open to following the idea of decentralization. They don't have any restrictions, anyone having a Computer and internet internet can participate in the network.

- As the name is public this Blockchain is open to the public, which means it is not owned by anyone.
- Anyone having internet and a Computer with good hardware can participate in this public blockchain.
- All the ~~comp~~ computer in the network hold the copy of other nodes or block present in the network.
- We can also perform verification of transaction or records.

ii) Private Blockchain :- These blockchain are not as decentralized as the public ~~block~~ blockchain only selected nodes can ~~participate~~ participate in the process, making it more secure than the others.

- These are not as open as a public blockchain
- They are open to some authorized users only.
- These ~~block~~ blockchains are operated in a closed network.

iii) Hybrid Blockchain :- It is mixed content of the private and ~~pub~~ public blockchain, where some part is controlled by some organisation and other nodes are not visible as a public blockchain.

- It is a Combination of both public and private ~~block~~ blockchain.
- Permission based and permission less System are used
- User access information via Smart Contracts.

iv) Consortium Blockchain :- It is a creative approach that Solves the needs of the Organization. This blockchain validates the transactions and also initiates or receives the transactions

Also known as Federated Blockchain.
This is an innovative method to solve the organisation needs.
Some part is public ~~and~~ and some part is private.

Transaction :- Peeling down a single transaction reveals several different structures in a transaction that have different Semantic meanings.

Transaction version number :- It is a version number specifying the type of transaction to the network. Through the transaction number, a node can determine the set of rules to be used to verify this particular transaction.

Output :- Transaction output consists of a ~~Cryptogr-~~ aphic lock and time.

Input :- Transaction input consists of a pointer and an unlocking key. The pointer points to the previous transaction output. The unlocking key is used to unlock the previous output the input points to.

Lock Time :- It specifies whether a transaction can be included in the blockchain right away or after some specified time.

UTXO is all those outputs that are yet to be ~~not~~ unlocked by input.

Once an output is unlocked, they are removed from the circulating supply. The new outputs take their place. Thus, the sum of the unlocked outputs will always be equal to the sum of values of the newly created outputs.

Transaction Version	→ Version Number
Input 0	→ Inputs
Input 1	
Input 2	
Output 0	→ Outputs
Output 1	
Output 2	
Lock Time	→ Time boundary for spending

~~* (b) UTXO :-~~

* UTXO :- In bitcoin, the transaction lives until it has been executed till the time another transaction is done out of that UTXO. It stands for Unspent Transaction Output.
  - It is the amount of digital currency someone has left remaining after executing a transaction.
  - when a transaction is completed, the unspent output is deposited back into the database as input ~~which~~ which can be used later for another transaction.

→ Coinbase Transaction :- All transactions ~~that~~ that take place on the cryptocurrency network are not the result of payment between ~~for~~ two people.

The first transaction that took place was in Bitcoin. It was a special transaction that formatted reward transaction for miners inside the Genesis block. Such reward transaction are specially allocated to the miner for the their work. This type of transaction is known as a Coinbase transaction.

* Structure :- A bitcoin transaction is just the data that shows the movement of bitcoins from one wallet to another. In the case of coinbase transactions, it generates new currencies that have been spent so the input remains blank in such transactions. The single blank input of a Coinbase transaction is called 'The Coinbase'.

→ Time Stamp :- The time stamp is a small data ~~stored~~ stored in each block as a unique serial and whose main function is to determine the exact moment in which the block has been mined and validated by the blockchain network.

* Used for :-
One of the main uses of timestamp is to establish the parameters of the process of mining is, this is because these timestamps allow nodes to correctly adjust the mining difficulty to be used for for each block generation period.

→ How miners pick Transactions :- Memory pool, where all the pending transactions are placed before moving them into the blockchain i.e into a valid network.

Miners can pick-up a maximum of five transaction from the Mem-Pool. It is obvious that a miner or a mining pool will choose a transaction having the highest fee reward.

→ How does Mempool work?
When a transaction is executed on a ~~block~~ blockchain, it is broadcast to the entire networks and queued in a mempool.

Each blockchain node has its own mempool with transactions that may or may not differ from the transactions in a mempool of ~~another~~ another node. A node maybe configured in a way to receive transactions at different times, while some nodes may use lower-end hardware which can ~~limit~~ limit the amount of transactions it can store in its mempool.

A miner or validator has the discretion to choose and pick which transactions to prioritize when creating a block.

→ Orphaned Blocks :- In Blockchain terms, an orphan blocks are blocks mined simultaneously as another ~~block~~ block but not accepted by the blockchain. Most of the time, this is because there are not enough blocks generated from that block for the network to recognize it as the longest fork. The Bitcoin ~~blockchain~~ blockchain discards orphan blocks; however, other blockchains may use them for different purposes.
An orphane block is a block that has been solved within the blockchain network but was not accepted by the networks.

There can be two miners who solve valid blocks simultaneously. The network uses both blocks until one chain has more verified blocks. Then, the blocks in the shorter chain are orphaned.

Orphan blocks are a regular occurrence in a distributed blockchain such as Bitcoin.

Proof of Stake :- As understable from name it is a cryptocurrency consensus mechanism for processing transaction and creating new blocks in a blockchain. A consensus mechanism is a method for validating entries into a distributed database and keeping the database secure. In case of cryptocurrency, the database is called a blockchain - so consensus mechanism secures the blockchain.

Under POS validators are chosen based on the number of staked coins they have.

Proof of Stake was created as an alternative to POW, the original ~~coren~~ consensus mechanism used to validate transactions and open new blocks.

POS mechanisms require validators to hold and stake tokens for privilege of earning transaction fees.

The ~~block~~ next block writer on the blockchain is selected at random, with higher odds being assigned to nodes with larger stake positions.

POS changes the way blocks are verified using the machines of coin owners, so there doesn't need to be as much

Computational work done. The miner offer their coins as collateral - staking - for the chance to validate blocks and earn rewards.

→ DeFi :- Decentralized finance is an umbrella term for financial services on public blockchains, primarily Ethereum. With Defi you can do most of the things that banks support - earn interest - but it's faster and doesn't require paperwork or a third party.

* importance of DeFi :- DeFi takes the basic premise of Bitcoin - digital money - and expands on it, creating an entire digital alternative to Wall Street, but without all the associated costs. This has the potential to create more open, free and fair financial markets that are accessible to anyone with an internet connection.

→ NFT :- Non-fungible tokens, which are generally created using the same programming used for cryptocurrencies. In simple terms these cryptocurrencies graphic assets are based on blockchain technology. They cannot be exchanged or traded equivalently like other Cryptographic assets. like Bitcoin and Ethereum. The term NFT clearly represents it can neither be replaced nor interchanged because it has unique properties. Physical currency and Cryptocurrency are fungible. fungible, which means that they can be traded or exchanged for one another.

* How it works :-

- The majority of NFTs resides on the Ethereum Cryptocurrency

cy's blockchain, a distributed public ledger that records transactions.

- NFT are individual tokens with data valuable information stored in them.

- Because they hold a value primarily set by the market and demand, they can be bought and sold just like other physical types of art.

- NFT unique data makes it easy to verify and validate their ownership and the transfer of tokens between owners.

→ Ethereum :- It is blockchain network that introduced a built in Turing Complete progeramming language that can be used for creating various decentralized applications also called Dapps. The Ethereum network is fueled by its own Cryptocurrency called 'ether'.

- Ethereum network is currently famous for allowing the implementating of Smart contracts. Smart Contracts can be thought of 'Cryptographic bank lockers' which contain certain values.

* Features of Ethereum :-

i) Smart Contracts :-

ii) Ethereum Virtual machine :- It is designed to operate a runtime enviornment for compiling and deploying Ethereum based Smart Contracts.

iii) Ether :- Ether is the cryptocurrency of the Ethereum network. It is the only acceptable form of payment for transaction fees on the Ethereum network.

iv) Dapps :- Dapp has its backend code running on a decentralized peer-to-peer network. It can have a frontend and user interface written in any language to make calls and query data from its backend. They operate on Ethereum and perform the same function irrespective of the environment in which they get executed.

v) DAOs :- It is a decentralized organization that works in a democratic and decentralized fashion. DAO relies on smart contracts for decision-making or decentralised voting systems within the organization.

* How does it work :-

Ethereum implements an execution environment called Ethereum Virtual Machine.

- When a transaction triggers a smart contract all the nodes of ~~the~~ the nodes of the network will execute every instruction.
- All the nodes will run the EVM as part of the block verification, ~~whe~~ where the nodes will go through the transactions listed in the block and runs the code as triggered by the transaction in EVM.
- All the nodes on the network must perform the same calculations for keeping their ledger in sync.
- Every transaction must include :-

i) Gas limit

ii) Transaction fee that the sender is willing to pay for the transaction.

- If the total amount of gas needed to process the transaction is less than or equal to the gas limit then the transaction will be processed and if the total amount of gas needed is more than the gas

limit then the transaction will not be processed the ~~fe~~ fees are still lost.

Thus it is safe to send transaction with the gas limit ~~abo~~ above the estimate to increase the chances of getting it processed.

→ Bitcoin Cash :- Bitcoin Cash is a Cryptocurrency, created from a hard fork from the Bitcoin blockchain in ~~2017~~ 2017. A hard fork is when a blockchain splits, with no compatibili between the two forks. This is a radical change to a network protocol that makes previously invalid blocks and transactio valid, or vice versa. A hard fork requires all nodes or users to upgrade to the latest version of the protocol software.

Bitcoin Cash is designed to be used as a cheap payment system, much in the way Bitcoin was designed to be ~~orign~~ originally. Transaction fees are generally less than $0.1, and transaction ~~conf~~ Confirmation times are significantly less than Bitcoin's generally within seconds.

→ Tether :- Tether aims to provide a "safe" digital asset that maintains a stable valuation. The goal is that Tether should always maintain the same value as its peg. It is stable coin pegged to the U.S. dollar and backed "100%" by Tether's reserve

→ Decentralized ~~App~~ Apps :- are digital applications or programs that are based on blockchain and fundamentally different from other normal applications. Unlike normal ~~appl~~ applications that run on centralized servers that belong ~~to~~ to the company which owns them, dApps run on a decentralized peer-to-peer network that is based on ~~Bl~~ Blockchain.

* How do ~~DApp~~ dApps work?

A dApp has a backend code on a decentralized peer-to-peer network. It can also have a frontend code and a user interface that can be written in any language just as it is done for normal applications. The frontend can be hosted on on any decentralized server like IPFS. dApps work in a manner similar to normal applications except for the few differences that are discussed below:

- Decentralized
- Deterministic
- Turing Complete: dApps can perform any action given the req. res.
- Isolated

* EVM :- Ethereum Virtual Machine is designed as the runtime environment for Smart Contracts in Ethereum. It is ~~sandboxed~~ Sandboxed and isolated from or other parts of System. This means that any operation on EVM should not affect your data or programs in any ways, no matter how many times you call a particular function on it.

- An EVM is the runtime environment that executes Ethereum Smart Contracts.
- Ethereum contains its own Turing-complete scripting language called Solidity and with this comes a need to execute this code.

* Working :- EVM is a program which executes scripts used to implement certain operations usually in Ethereum blockchain. EVM makes the process of creating new tokens on Ethereum Blockchain. Here, Script means a set of instruction or an algorithm which tells the computer what it needs to do in order for something

to work properly.
In Ethereum there is something called a Smart contract. These contracts have some computer code which facilitates the exchange of money and information.
These contracts are predefined by the creator of the Small Contract, in order to ensure that a certain outcome will happen on either what happens or doesn't happen.
Ethereum Virtual Machine provides Turing Complete environment for execution of Scripts and Smart Contracts. This means that anything that can be implemented with a Computer can be run on EVM.

EVM ensures that all transactions and Smart contracts made on the Ethereum blockchain are executed in correct and expected manner as desired by the Smart contract code. It serves as a platform for applications to be executed on.

* Uncles :- These are small pieces of Smart contracts or data stored on the blockchain. This is a useful feature because it allows for you to store metadata about your program.

→ Ethereum Gas :- Ethereum gas is the fees that a user must pay to conduct a transaction on the Ethereum blockchain. In technical terms, gas refers to 'the amount of computational effort' required to make execute operation on a blockchain network.

Imagine blockchain as a chain of hard drives. Each hard drives has a limited amount of space to save transaction data. Users transacting on blockchain are

actually paying gas fees so that their transaction information is uploaded to a block. Gas fees are critical to a blockchain's security. Part of gas fees on Ethereum is paid to block validators - nodes that verify transactions and create new blocks - for performing honest work.

* How does Gas relate to Performance of EVM?
- Gas is a measure of computational power. It determines how much time each transaction and contract takes to execute.
- Because there is so much code already in the system, it uses a limited amount of Gas to run all of this code. It sets the default gas limit to 250,000 gas units.

→ DAO stands for Decentralised Autonomous Organization. The concept of a DAO was first proposed by BitShare. It is a whole organization that is automated. It stores rules and processes in code. DAOs are often stateless and distributed over millions of computers. No single government could decide to take it down.

Smart Contract Creation → Funding → Deployment

→ Hard Fork :- A bitcoin hard fork is a protocol change that creates a new set of rules for the computers that make up the blockchain network. If a hard fork is implemented without the complete agreement of the other network participants, it can cause the Cryptocurrency network to split into two.

A protocol change that does not reject the pre-existing rule set. A hard fork requires all network participants to upgrade to the new rule set and reject the old rules, while a soft fork will continue to accept transactions created by the old rule set.

* Reasons :-
  - Correcting Security risk
  - adding functionality
  - Reverse transaction.

→ Soft fork :- A soft fork is a change to the software protocol where only previously valid transaction blocks are made invalid. Because old nodes will recognize the new blocks as valid, a soft fork is backward-compatible. This kind of fork requires only a majority of the miners upgrading to enforce the new rules, as opposed to hard fork that requires all nodes to upgrade and agree on the new version.

→ Initial Coin Offering :- ICO

A company seeking to raise money to create a new coin, app, or service can launch an ICO as a way to raise funds.

- ICO are a popular way to raise funds for products and services usually related to cryptocurrency.
- ICO are similar to initial public offering, but coins issued in an ICO also can have utility for a software service or product.

* How can ICO works :-

Static supply and static price :- A company can set a specific funding goal or limit, which means that each token sold in ICO has a preset price, and the total token

supply is fixed.

- Static supply and dynamic price : An Ico can have a static supply of tokens and a dynamic funding goal - this means that the amount of funds received in the Ico determines the overall price per token.
- Dynamic supply and static price : Some Ico have a dynamic token supply but a static price, meaning that the amount of funding received determines the supply.

→ Coin :- Coins are Cryptocurrency ~~to~~ belonging to a blockchain. They are independent of other chains and can cannot be used on other chains in their native form.

* Characteristics :-

i) Decentralization :- Coins are not controlled by any central ~~author~~ authority or intermediary.

ii) Security :- Coins are protected by Cryptography and encryption.

iii) Scarcity :- Most coins have a limited supply that is predetermined by their algorithm. This creates a deflationary effect that increases its value over time.

* Coins :-

i) Native Coins :- These are coins that run on their own blockchain and serve as the main currency of the the network.

ii) Forked Coins :- These are coins that are derived from an existing blockchain by ~~split~~ splitting or branching off from it. ex- BCH

iii) Wrapped Coins :- These are coins that represents another asset on a different blockchain. They allow users to access cross-chain functionality and liquidity. Ex- WBTC

iv) Stable coins :- ~~These~~ These are coins that are pegged to the value of another asset, such as fiat currency or gold. They aim to provide price stability and reduce volatility. Ex- USD Coin.

* Token :- Token sits on top of an existing blockchain and ~~depen~~ depend on it for their operation. A token can represent various thing, such as utility, governance right. Tokens are usually "pre-mined", meaning developers use a smart contracts to issue new tokens and distribute them to users.

* Characteristics :-

i) Utility :- Tokens are necessary to use the decentralized application they are built for. Users can use tokens to pay for fees, perform action etc.

ii) Governance :- Token can give users a voice in the decision making process of the blockchain. Users can use tokens to vote on proposals, changes or upgrade.

iii) Interoperability :- Token can enable cross chain communication and Compatibility.

* ~~Fot~~ Token :-

i) Utility tokens :- They provide access to a service or function on the blockchain or dApps.

ii) Governance token :- They give users a say in the governance of the blockchain or dApps.

iii) Security Tokens :- They represents a share of ownership or a claim on an asset or income stream.

iv) Non-fungible Tokens :- They represents as unique and indivisible digital items, such as art and collectibles. They are not interchangeable and have varying values.

→ Wrapped Tokens :- Wrapped tokens are assets that allow the value of a native asset from one blockchain to transfer to another blockchain. One ~~native~~ of the best known wrapped tokens is Wrapped Bitcoin.

→ ~~Air~~ Airdrop :- A Cryptocurrency airdrop is a marketing strategy that involves sending coins or tokens to wallet addresses. Small amount of new virtual currency are sent to the wallets of active member of the blockchain community for free or in return for a small service. The ultimate goal of a crypto airdrop is to promote awareness and circulation of a new token or coin.

→ Crypto Faucet :- A Crypto Faucet lets users earn small crypto reward by Completing Simple tasks. The metaphor is based on how even one drop of water from a leaky faucet could eventually fill up a cup. There are various kinds of Cryptofaucets, including bitcoin, Ethereum.

→ Litecoin :- is a cryptocurrency created from a ~~fork~~

fork in the Bitcoin blockchain in 2011. It was initially designed to address the developer's concern that bitcoin was becoming too centrally controlled, and to make it more difficult for large-scale mining firms to gain the upper hand in mining. While eventually unsuccessful in preventing enterprise miner from taking over the lion's share of litecoin mining, the cryptocurrency has rewarked itself into a minable coin and a peer-to-peer payment system.

* Governance Token :- are Cryptocurrencies that allows holders to participate in on-chain governance for a Crypto project. Usually, each governance token a person holds equates to one vote on upcoming proposals, but there are other methodologies. People with governance tokens can use them to accept or reject changes to dApp or blockchain during scheduled voting periods. Many dApps also allow people to use their governance tokens to create initiatives and put them up for a vote.

* The main feature that Separates governance tokens from other Cryptocurrencies is that they come with voting rights.
  - Deciding on a crypto project's treasury allocation.
  - Increasing or decreasing the interest rates on Crypto lending sites.
  - Adjusting Crypto rewards for liquidity providers.

→ Consensus Mechanism :- A consensus mechanism is a program used in in blockchain systems to achieve distributed agreement about the ledger state. Generally, it is imp implemented in a network with many processes and users. Cryptocurrencies, blockchain, distributed ledger benefit from their use because the consensus mechanism replaces much slower human verifiers and auditing. For instance, the Bitcoin blockchain uses a mechanism called Proof-of-Work, which requires computational power to solve an encrypted puzzle, called the hash. After hash is solved by one miner, Bitcoin's POW requires that every node on the network verifies the data that has been changed by checking.

- The data structure
- The block header hash
- The block timestamp
- The first transaction
- The block size

→ Proof of stake :-

i) Block creators called Validators
ii) Participants must own coins or tokens to become a validators.
iii) Energy Efficient
iv) Security through community control
v) Validators receive transactions fees as rewards.

Proof of works :-

i) Block creators are called miners.
ii) Participants must buy equipment and energy to become a miner.

iii) Not energy efficient.
iv) Robust security due to expensive ~~upfront upfront~~ upfront requirement.
v) Miners receive block rewards.