PAGE NO.
DATE

Blockchain technology notes.

* Blockchain - A blockchain is a chain of blocks which contain information.

client - Server	Peer - to - peer
① the client node request for services & server respond with services	each peer is request for services & respond services.
② provide less security than peer - to - peer	provide more security
③ It is centralized system.	It is decentralized system.
④ It is more stable	It is less ~~secur~~ stable than client - server.
⑤ Expensive to install	less expensive to install.

* Evolution of blockchain -

① Bitcoin - It is first decentralized cryptocurrency uses peer - to - peer network without the need of intermediaries.

② Litecoin - Charlie Lee designed it to improve on bitcoin technology, with shorter transaction time.

③ Ethereum - It is the currently holds the second-largest cryptocurrency after bitcoin.

④ Ripple - It is the type of cryptocurrency operates on an open-source & peer-to-peer decentralized platform that allow for a seamless transfer of money.

PAGE NO.
DATE:

⑤ NEO - It is very aggressively looking to become a major global cryptocurrency player.

* Why we need blockchain ?

→ ① In blockchain networks, operations are fully automated through software implication.
② Blockchain happens to be an open-source technology.
③ It is more secure.
④ Blockchain works in a distributed mode, in which records are stored in all nodes in the network.
⑤ Blockchain is flexible.

* characteristics of blockchain -

① Faster Settlement.
② Decentralized Technology.
③ Immutable in nature.
④ Distributed ledger.
⑤ Consensus.

* Block -

It is a data structure that stores a set of transactions that is then shared among all nodes in the network.

* structure of block -

① The blocks in blockchain contain a block header which verifies the validity of the block.
② The block height of a block is defined as the no. of blocks preceding it in the blockchain.

PAGE NO.
DATE:

③ Nonce is a random number of miner use to solve a mathmatical puzzle in the mining process.
④ Difficulty in a block is a value that measure the degree of difficulty to find a hash value
⑤ A timestamp in a block is a sequence of characters identifying when a certain event occured.
⑥ hash is a result of hash function.
⑦ the Merkle tree is known as hash tree.

* Types of Blockchain-
① public blockchain- It is a permissionless distributed ledger technology where anyone can join & do their transaction. In public blockchain, the verification of the transaction is done through agreement method such as Proof-of-Work (PoW), Proof-of-stack (PoS) & so on.
② private blockchain - A private blockchain is a restrictive or limiting permission blockchain. operative only in a closed network.
Ex: multichain & Hyperledger projects, Corda, etc.

③ Consortium blockchain- It is a semi decentralize type where more than one organization manages a blockchain network.
Ex: Energy web foundation, R3, etc.
④ Hybrid Blockchain - A hybrid blockchain is a combination of private & public block chain.
Ex: Dragonchain, XinFin's Hybrid blockchain, etc.

PAGE NO.
DATE:

* Benefits of blockchain-
① Digital freedom & decentralization.
② New-Age technology integrations.
③ Anonymity & privacy.
④ Security
⑤ Immutable data
⑥ Low transaction cost.

* Limitations of blockchain-
① Higher cost.
② scalability.
③ Immutable.
④ private keys.
⑤ Interoperability

* challenges of blockchain-
① scalability - blockchain are having trouble effectively supporting a large no. of users on the network.
② public preception - perception, blockchain holds in the eyes of people is the biggest drawback in the way of its success.
③ Security - the blockchain maintains confidentiality to protect user from hackers
④ Cost - the blockchain technology does not come free.
⑤ privacy - the Bitcoin blockchain is designed to be publicly visible.

PAGE NO.
DATE:

* Application of blockchain / Usage.

① Banking
② cloud stomge
③ voting
④ supply chain management
⑤ Cryptocurrency
⑥ Healthcare
⑦ Smart Contracts

* Types of Networks -
① public blockchain network - this type of blockchain is highly democratic & transparent because every node has equal access to data on the network
② private blockchain network - users who join the private blockchain network need permission to read write or review the blockchain
③ Consortium blockchain network - It is a type of semi-decentralized blockchain network but it is permissianed too.
④ Hybrid blockchain network - It refers to the combination of public & private blockchains

* Layered Architecture of blockchain ecosystem.

① Ecosystem that use blockchain ~~sy~~ technology consist of a set of distributed nodes where immutable transactions are replicated.

PAGE NO.
DATE

Application & presentation Layer

Consensus Layer

Network Layer

Data Layer

Hardware / Infrastructure Layer

① Hardware / Infrastructure Layer - the first layer of the blockchain is the hardware or infrastructure layer. In the blockchain the content is hosted in a server that resides in a data center.

② Data Layer - Data structures of a blockchain are represented as a linked list includes two primary elements i.e pointers & Linked list where transaction are ordered.

③ Network Layer - It is also known as the peer-to-peer (P2P) layer. It is one of that & is responsible for inter-node Communication.

④ Consensus Layer - It is the essential to the existense of blockchain platforms.

⑤ Application Layer - It is divided into two Sub Layers i.e application Layer & execution Layer.

PAGE NO.
DATE:

* cryptography - The art & science of concealing the messages to introduce secrecy of information security is recognized as cryptography.

* key - A key is usually a number or a set of numbers on which the cipher operates.
private & public keys =
(i) private key must be kept confidential & never shared.
(ii) public key, by their nature, are designed to be public & do not need to be protected.

* Hashing - Hashing is a cryptographic technique which simply converts a data of any size into a fixed size output.

* Digital Signature - Digital Signature is a perticuler type of electronic signature that encrypts the signed document.

* Smart Contracts - It is a self executing contracts containing the terms & condition of an agreement among associate.

Applications - Insurance, Transportations, Employment Contract.

PAGE NO.
DATE:

* Block chain Use Cases -

① Blockchain in Capital Markets.
② Blockchain in Energy & sustainability.
③ Blockchain in financial services.
④ Blockchain in Government & the public sector.
⑤ Blockchain in Insurance.
⑥ Blockchain in Real Estate.

* properties of Cryptographic hashing -

① It is impossible to find two input texts that produces the same hash value.
② It is easy to Generate hash value.
③ It is impossible to generate original text from the hash value.
④ Commitment.

* Types of Cryptographic Hash function -

① Secure Hashing algorithm (SHA-2 & SHA-3)
② RACE Integrity Primitive Evaluation Message Digest (RIPEMD)
③ Message Digest Algorithm 5 (MD5)
④ BLAKE 2.

PAGE NO.
DATE:

* process of SHA-256-

Input message

SHA-256

SHA-256 Preprocessing

Padding the message

Persing the message

Initialize hash values

SHA-256 Hash Computation

message schedule functions

Working Variables Computition

Interations

256-Bit Hash

① the SHA-256 starts by converting the message to a binary number & get Length l.
② the objective of this padding is to prepare the message before the hash computation begins.
③ the padding ensures that the padded message is a multiple of 512 bits.

* Immutable Ledger-

Blockchain is a decentralized, distributed & immutable ledger technology that operates over a peer-to-peer network. Immutability is defined as the ability of a blockchain ledger to remain unchanged.

PAGE NO.
DATE:

* Distributed P2P Network-

① The blockchain records transaction in the form of an immutable Layer.
② Peer-to-peer (P2P) network is a decentralized network consists of a group of devices that collectively store & share files where each node acts as an individual peer.
③ The peer-to-peer architecture of blockchain allows all cryptocurrencies to be transferred worldwide.

pros & cons of P2P-

ⓐ As blockchain is a decentralized System of peer-to peer network, it is highly available due to decentralization.
ⓑ P2P networks offer greater security compared to traditional client-server systems.
ⓒ These networks are virtually immune to the Denial-of-services (DoS) attacks.

* Nonce-

① Nonce stands for "Number used only once" i.e Nonce refers to a number or value that can only be used once.
② Nonce is a 32-bit random number which can be used one time.
③ Nonce is often used on Cryptographic hash functions & authentication protocols.
④ The 'nonce' ~~is~~ in a Bitcoin block is a 32-bit field whose value is adjusted by miners

Proof of Work	Proof of stake
① The probability of mining a block is determined by how much computational work is done by miner.	The probability of validating a new block is determined by how large of a stake a person holds.
② compete to solve difficult puzzles using their computer process power	There is no competition as a block creater or is chosen by an algorithm based on user stake.
③ Less energy efficient & less costly.	have more cost & energy efficient.
④ Initial investment to buy hardware.	Initial investment to buy stake & build reputation.

* Ethereum Network -

① It is the hottest cryptocurrency in the blockchain at present.

② Cryptocurrency is the word that's used to describe decentralized digitized currencies.

③ Ethereum is relatively new cryptocurrency & was invented in 2013.

④ Ethereum is a technology that is home to digital money, global payments & applications.

⑤ Ethereum is a blockchain platform with its own cryptocurrency called Ether (ETH) & Solidity is its own programming language.

⑥ Ethereum works as an open software platform functioning.

PAGE NO.
DATE:

* Ethereum virtual machine (EVM) -
① EVM stands for Ethereum Virtual Machine.
② the purpose of EVM is to serve as a runtime environment for smart contracts build on Ethereum.
③ EVM is the core engine that runs the Ethereum platform.
④ the EVM can be considered a Turing Complete virtual machine, which means it can perform any logical step of a computational function.
⑤ Virtual machines are essentially creating a level of abstraction between the executing code & the executing machine

* DApps
① DApps is an abbreviation for decentralized application.
② DApp has its backend code running on a decentralized peer-to-peer (P2P) network such as the Ethereum blockchain network.
③ A DApp is an application build on a decentralized network that combines a smart contract & a frontend user interface.
④ Advantages -
(a) Zero Downtime
(b) Privacy
(c) Resistance to Censorship
(d) Complete Data Integrity.
(e) Trustless Computation

PAGE NO.
DATE:

* Decentralized Autonomous Organization (DAO)-

① The DAO stands for Decentralized Autonomous Organization.
② As the name implies, it is an organisation which is both autonomous & decentralized.
③ A DAO is the most complex form of a smart contract.
④ A DAO is also a computer program that runs on top of a blockchain & embedded within it are governance & business logic rules.

Hard fork	Soft fork
① It refers to making significant changes to the blockchain, splitting into older & newer version.	It is making software changes to the original blockchain.
② It does not support backward compatibility.	It is backward Compatible
③ Speed & security are high	Speed & security are Low.
④ Ex. Bitcoin Cash	Ex. Segwit.