#1 **Blockchain (Module 1)**

What is Blockchain

↓

Hashing Algorithm

↓

Immutable Ledger

↓

Distributed P2P Networks

↓

What is Mining

↓

Consensus Protocol.

#2 Why should I study Blockchain ?

⟹ Bcoz blockchain is a disruptive technology.
↓
which can change entire syste

Blockchain ⟶ Trust

#3 What is Block-chain ?

Block chain is distributed or decentralized immutable ledger which is completely transparent.

#4 Applications of Blockchain :—

(1) Product Tracking:— immutable record of a product's Jouney through its supply chain and lifecycle

(2) Smart Contract:— program which run's on Ethereu blockchain.

- A smart contract is a self-executing contract with the terms of the agreement directly written into code. These contracts run on a blockchain and automatically executes actions or enforce rules when predefined

Condition met.

(3) International wire Transfer — it involves the movement of funds from one bank or financial institution to another, typically across borders using network of financial intermediaries.

International wire transfer are used for business transactions, personal payment, remittances etc.

Ex — money transfer from one nation to other.

Sender Bank $\xrightarrow{money}$ Correspondent Bank $\xrightarrow{money}$ Receiver Bank

Centralized way — disadvatages → Huge fees
→ Time Taking.

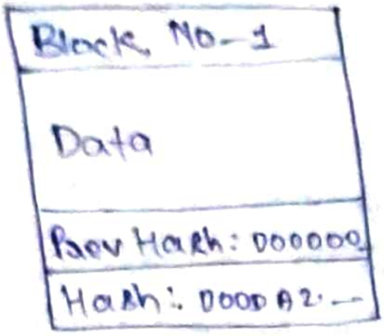
(4) Healthcare System :-

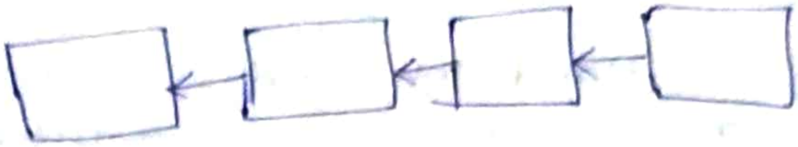
Electronic Health Records (EHRs)

(5) Legal and Notary services
(6) Gamming
(7) Agriculture
(8) Insurance
(9) Art and collectibles
(10) Food safty.
(11) Education
(12) Real Estate
(13) Voting System
(14) Finicial banking System
(15) Supply chain management.
(16) Cryptocurrienies.

#5 Hashing Algorithm

Block structure :-

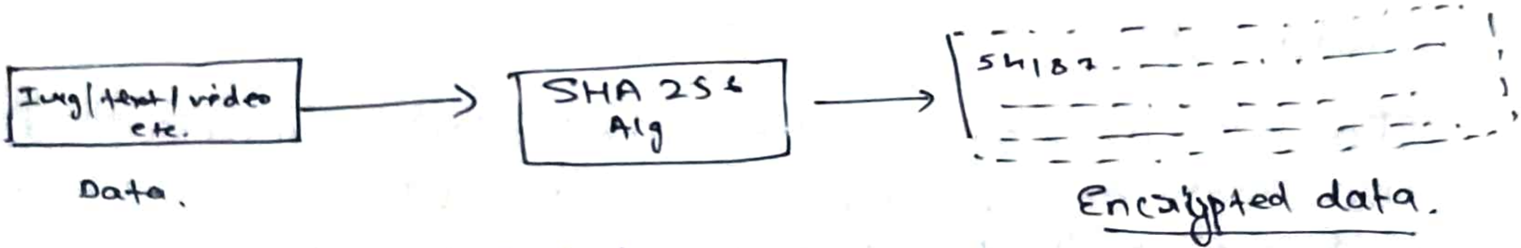




Genesis Block — First block or Black having Prev Hash value 0000— is **Genesis Block**.

Hash :- Unique Id like finger print.

Hash is genrated by SHA256 Algorithm



Encrypted data

64 hexadecimal characters. Each Character of 4 bits
64x4 = 256 bits

Fire Requirements of Hash Algorithm :-

① ONE way → Data ⟶ Encryted.
X ⟵ #.. Not possible.

② Deterministic → When we give a data in SHA256 Algo it produces single output even you give same data many time then it also produces same output.

③ Fast Computation

④ withstand Collision — resistance to producing the same hash value (collision) for two different inputs.

⑤ Avalanche Effect — It refers to the property that a small change in the input data should produce a significantly different hash value (output) making it computationally infeasible to predict the output based on minor changes in the input

#6 Immutable Ledger - refer to a record-keeping system, often based on blockchain technology, where once data is recorded, it cannot be altered, deleted or tampered with.

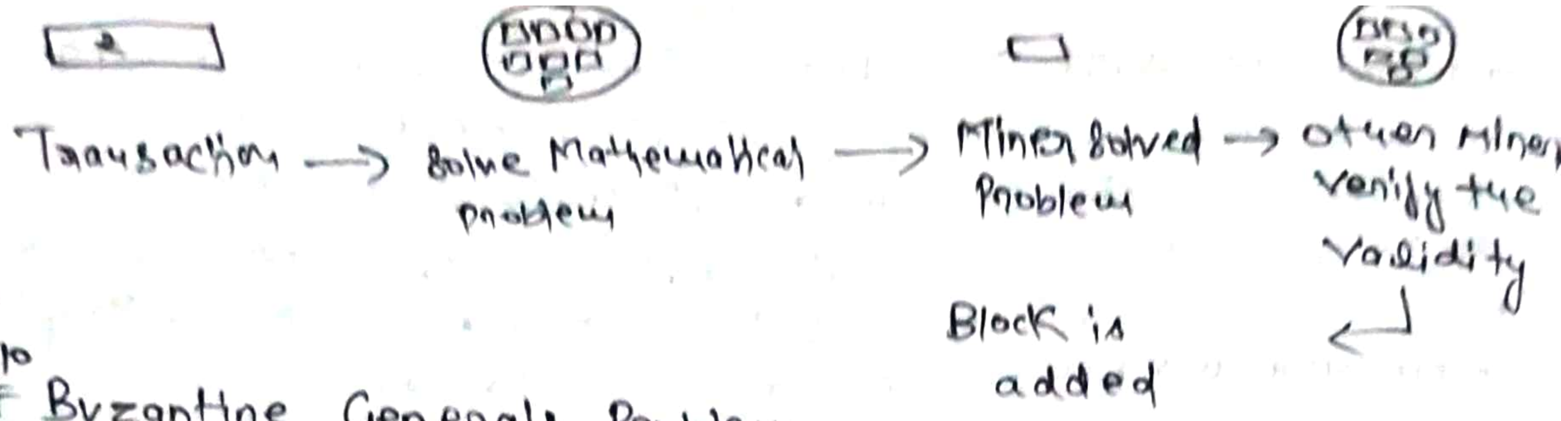
#7 What is P2P Network ?.

In P2P network, participants (nodes) communicate directly with each other without the need for intermediaries such as centralized server or authorities.

#8 Distributed P2P network

Ex- BitTorrent, Blockchain Networks, (CDNs) → Content delivery Networks, (DApps). Decentralized Application.

#9 Blockchain Mining :— Block chain mining is the process by which new transactions are added to a blockchain and new blocks are created and confirmed on the network. This process is fundamental to security and functioning of blockchain networks, particularly those that use Proof of work (PoW) or similar consensus.



#10 **Byzantine Generals Problem**

In the blockchain network, multiple nodes (computers) participate in a decentralized system to validate transactions and add them to the blockchain ~~edge~~ ledger. These nodes are akin to the Byzantine generals in the problem because they need to reach a consensus on the state of blockchain, even when some of them may be dishonest or faulty. The problem becomes particularly important in the context of cryptocurrencies like Bitcoin. where financial transactions are at stake.

#11 **Consensus Protocol** → 2 type and many more.

(I) Prevent Attacks
(II) Competing chain Problem

(I) Proof of Work (PoW)
(II) Proof of stake (PoS)

Prevent Attack

(I) **Proof of Work** :- In Proof of Work, miners compete to solve complex cryptographic puzzles. The first miner to solve the puzzle get the ~~stde~~ right to add a new block of transaction to blockchain. other nodes in the network must then validate the block. The process of solving these puzzle is energy-intensive and requires significant computational power.

(11) Proof of Stack — Pos assign the right to create new blocks and validate transactions based on the amout of cryptocurrency a participant is willing to 'stake' as collateral. Essentially, the more cryptocurrency you have and are willing to lock up the more likely you are to be chosen as a validator.

#12.

Competing block chain problem

A situation where multiple valid blockchain branches or chains emerge due to disagreements among nodes in the network about which transaction should be included in blockchain. This problem is also referred to as a "fork" in the blockchain.

Solve using Consensus Resolution : —

Note :—

- The Consensus Protocol of Blockchain is much better than the Byzantine fault Tolerance as consensus protocol only need as 51% majority while Byzant fault Tolerance need approximately 66%.
- All the transaction in the orphan block will be dropped and the miner that hed mined the blocked will not get any reward.
- So that's why wait for the 6 confirmations before assuming payment to be successful.