BLOCKCHAIN

- Hash Cryptography

  It will create a unique id like a fingerprint for a person.

  SHA256 is 64 character hash algorithm

  main contents of any hash algorithm are

  - One way - we can get a hash id for a thing but we can't get anything from a hash id.
  - Deterministic - Unique for unique text or unique document
  - Fast computation
  - The avalanche effect - it had to change for everything even for a change of one simple character
  - Must Withstand collisions - It has to withstand collisions

- Immutable Ledger

  Ledger means a note where we note details of house owners or transactions

  Immutable ledger means we cannot change data in blockchain if we change one we have to change all the blocks next to it

- Distributed peer 2 peer network

  This will help if someone hacked and changed the data in a block or accidentally happened

  The blockchain will be distributed among so many computers and if a random changes data in a block the remaining systems will alert the hacked system this follows the majority rule so if we want to hack a blockchain we have to change data in half of the systems which the blockchain is distributed.

- How mining works

  There will be a few things in a block in the blockchain

  - Block number - Number of the block which is fixed
  - Data - Which is not to be changed
  - prev hash - hash of the previous block fixed
  - the hash of the block - if all the fields are fixed we cannot control the hash
  - Nonce - this will help to change the hash without changing data or previous hash or block number

  Miners fix a target and try putting different nonce if they get a hash less than the target they can add a block

  Miners will take data and prev hash and block number and will keep on trying nonce

  (How will they get prev hash, How will they know the block number)

- Byzantine Fault Tolerance

  This is an algorithm to find what is the correct thing to do even if there are traitors in a group.

  Image representation

  The result will be the more number of same orders one got

  The constraint is the count of traitors had to be less than 34% of the total networks.

- Consensus Protocol

  This protocol will find solutions for the following challenges.

  What if anyone wants to add a block at the end of the chain?

  what if two people got the same nonce almost at the same time? which one to record first? what about the splitting of blockchains?

  - Power of Work
    - If anyone wants to add a block at last it will pass through certain tests called consensus protocol
    - When two people added blocks in the gap of 1 second the block which came first will be linked by more number of systems. so when a new block is added and the acceptance rate is more than 50% the new block and the old block which gave 50% will be added in place of the block which came 1 second late.
  - Power of Stake