~~ARTIFICIAL INTELLIGENCE~~

BLOCKCHAIN

Prerequisites:-
- Cryptography, Hashing
- Distributed Computing.
- Game theory.

invented by Satoshi nakamoto in 2008

Price of 1 Bitcoin = 15000 $

Smallest unit of 1 Bitcoin is 1 satoshi = ₹ 1/100

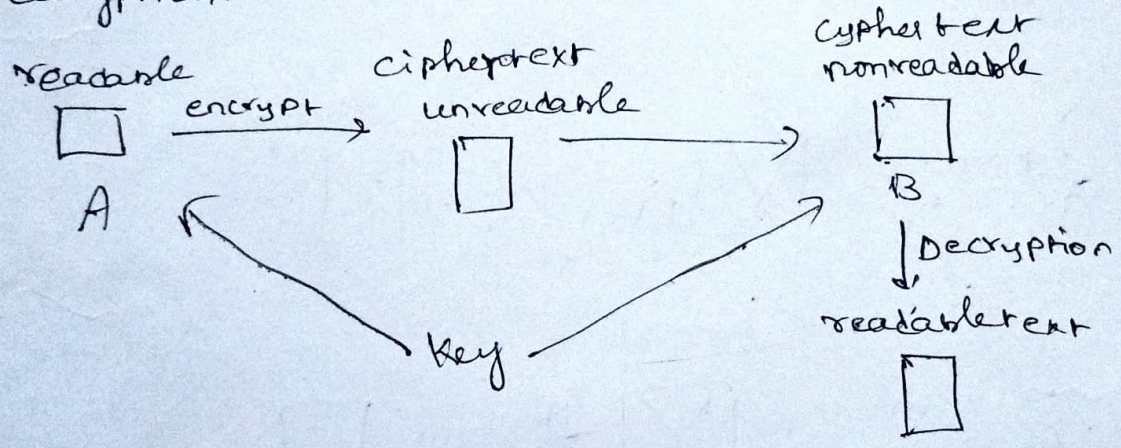
Cryptography - Blockchain
|
Peer - Peer network.

4 Concerns:-
1. Confidentiality 2. Integrity 3. non repudiation 4. authentication

Can be achieved by Cryptography

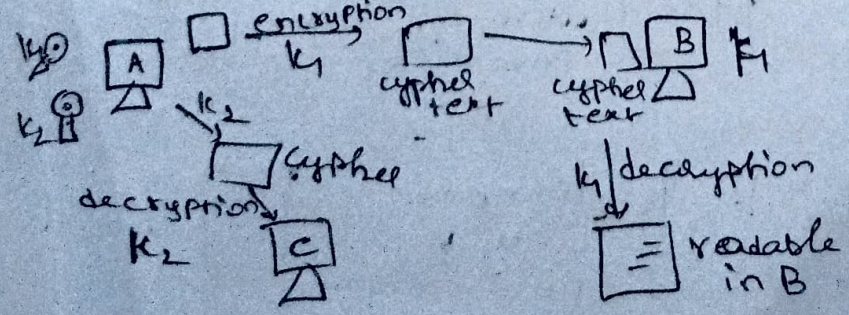
cryptography.
↓ secret writing.
- encryption
- decryption.

miners will do transactions
1 transaction reward = 12.5 bit coins.
transaction is done after solving a puzzle.



Types based on keys:-
- Symmetric key Cryptography.
- Asymmetric key cryptography.

i) Symmetric key cryptography: have symmetric key.

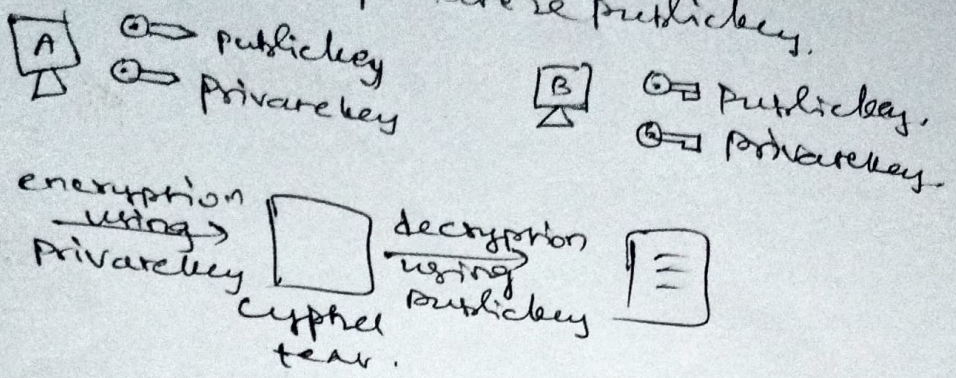


as no. of users ↑
no. of keys ↑
its diff to manage keys.

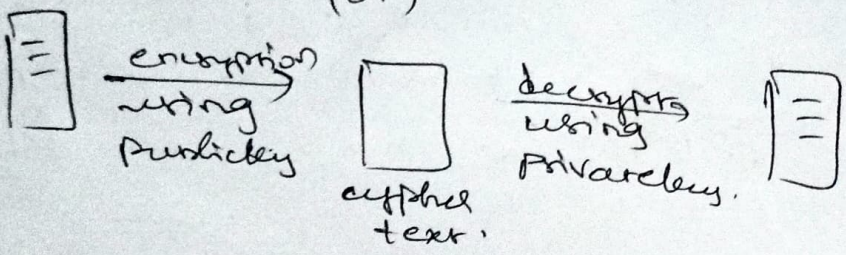
Assymetric key cryptography:-

also called publickey cryptography.

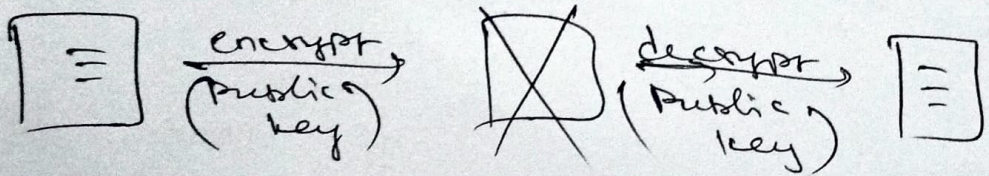
each node has own privarekey & publickey.



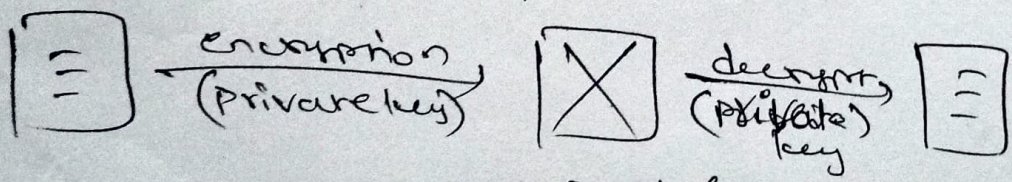
(or)



Due

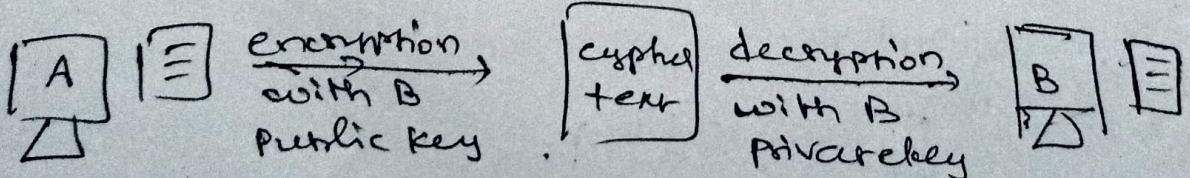


not possible

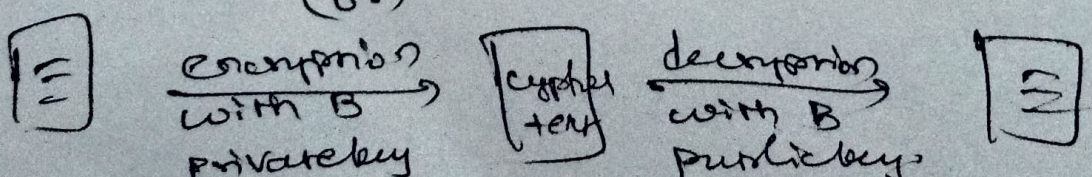


not possible

eg:-



(or)



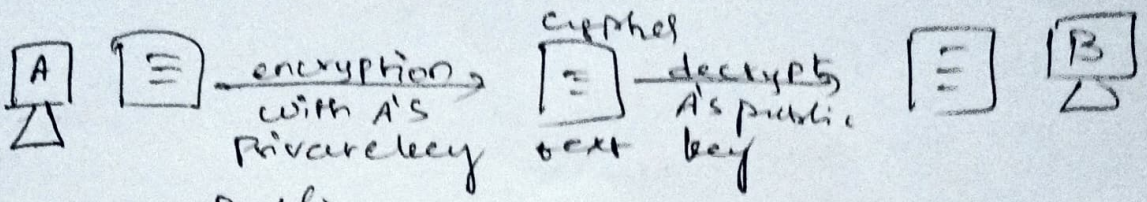
the encrypted data can be viewed by others but can be only decrypted using B's privatekey.

Digitalsignature:-

Authentication

eg:- If a message is sent from A to B, to verify that it's A we need to do digitalsignature just like signing in a letter.

case-1:- to achieve authentication:-

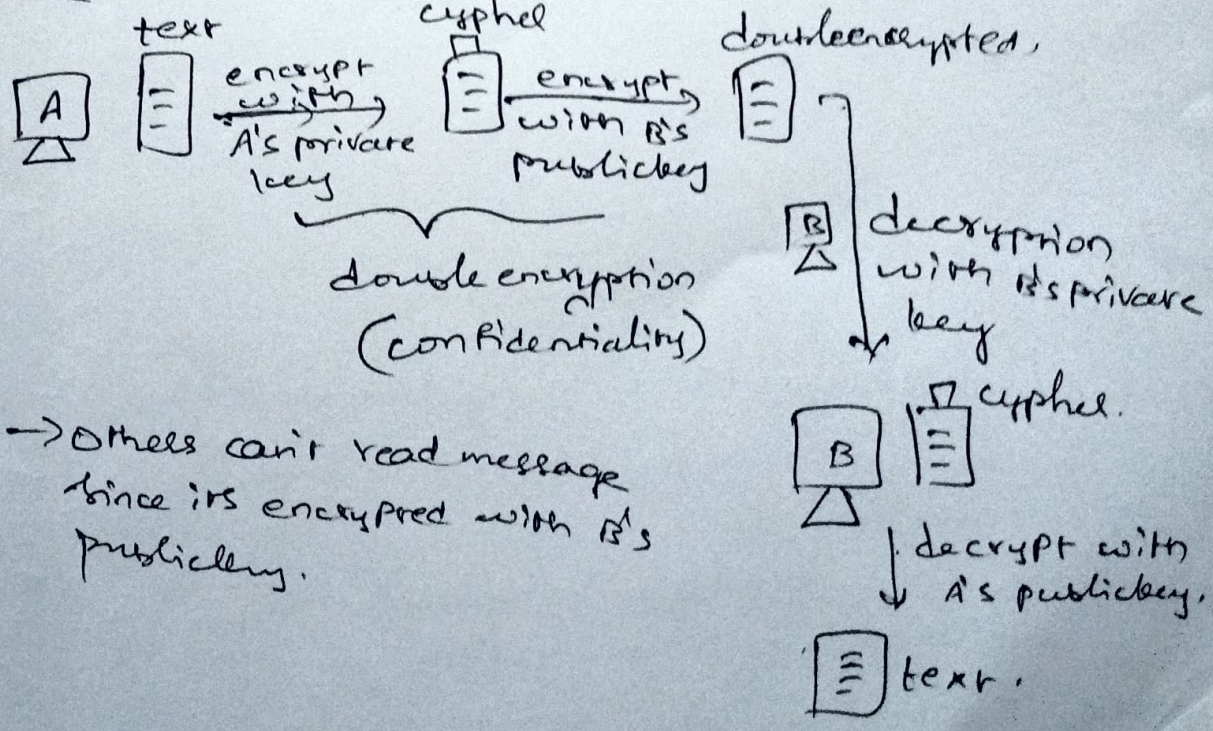


but A's ~~private~~ public key is available to every one. confidentiality is lost.

when B decrypts the message with A's publickey, its sure that the message is sent by A.

→ to achieve both confidentiality & authentication.

case-2:-



→ Others can't read message since its encrypted with B's publickey.

Node :-

2 types :-

1) Full node
2) Partial / light node.

1) Full node :-

a fullnode is computer having entire blockchain
current size of blockchain :- 188GB.
and it increases day by day.
all data stored in full node.
it verifies new data added & then stores it.

Miners :- Mined blocks.

fullnode can be miner.

full - node huge storage.
node - huge computing power.

Partial node :-

Hashing :-

Varying length input → Hash function → Fixed length output.

output length changes based on algorithm we use.

→ If we use certain algorithm & give input we'll get same hash value for same input.
→ If we have small change in input there will be change in hash value.
→ we can't get actual input from hash value

hashing isn't encryption. once we get hash value, we can't get the data back.

we'll be looking lot of data in hashing. it converts GB data into bits. ~~we'll never~~

we'll never get same hash value for different inputs. If that happens its called collision.

different algorithms are available:

i) MD (versions - MD2, MD3 ... MD6)
message digest

ii) SHA (secured hash algorithm) built by NSA (national security agency)
(SHA 0, 1, 2, 3)

SHA 2 → SHA 256 } Popular.
↳ SHA 512 }

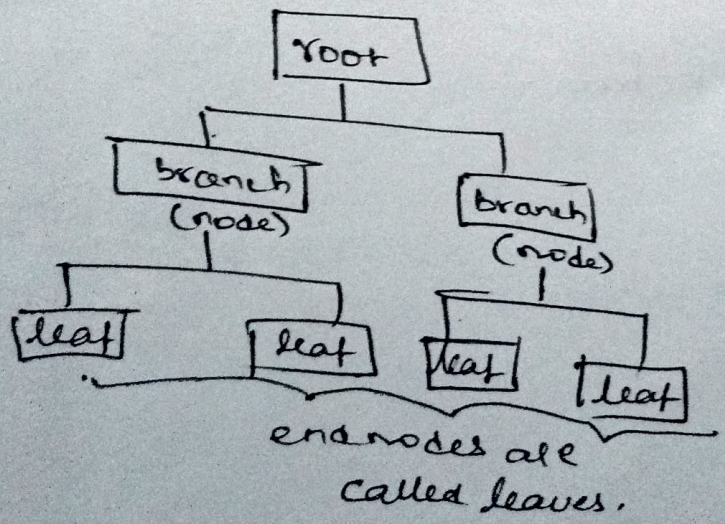
↓
256, 512 represents output bit values

Merkle tree:-

In a block chain, we have many blocks, each block is connected by a hash value.

when we want to find hash of block. it is easier to find combined hash of all blocks rather than extracting hash value of each block.

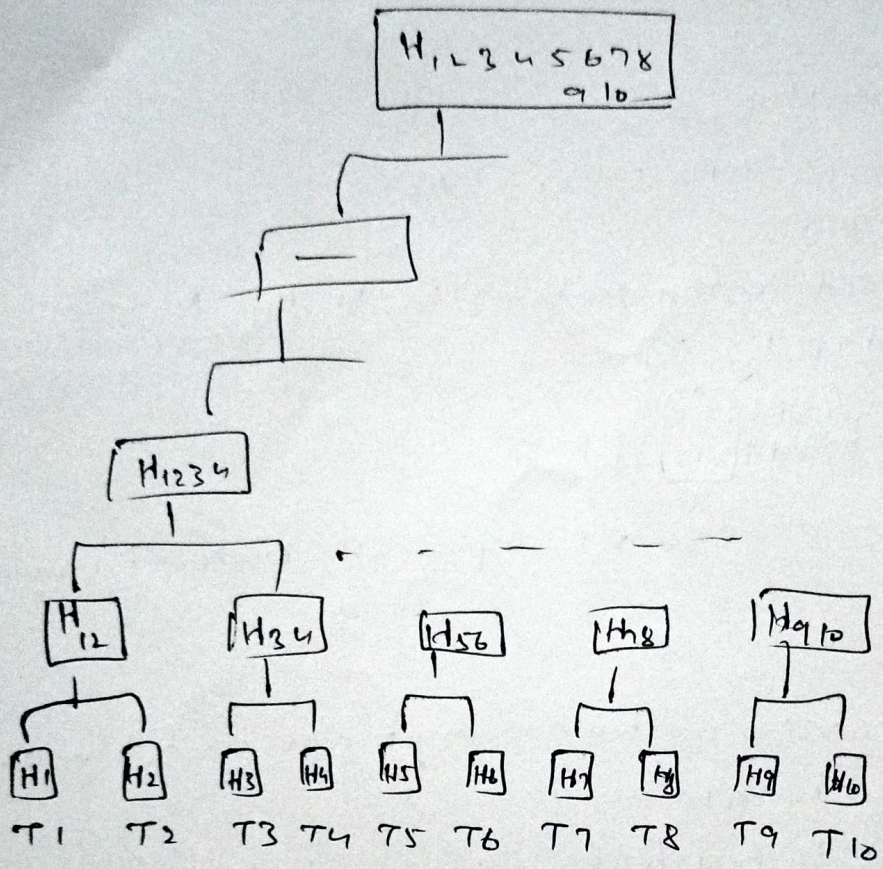
Then we use Merkle tree.



block

10 transactions.

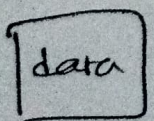
10 Hash values - H.



Suppose, if we have odd no. of nodes;
at the end we'll repeat the transaction.
at last we'll get hash of merkelroot.

Architecture of blockchain:-

its a simple database.



block

Public blockchain
eg: bit coin

data:-
from
to
money info } saved in block

to differentiate each block to form blockchain, we use block header. contains:

- every block needs specified time. (time stamp)
- block version.
- Merkeroot.
- difficulty target
- Nonce
- previous hash. (every block has hash of prev. block)

to verify the block we use POW (Proof of work) algorithm.

advantages:-

- immutability.

if we manipulate the data hash value is changed, we can know where there's change.

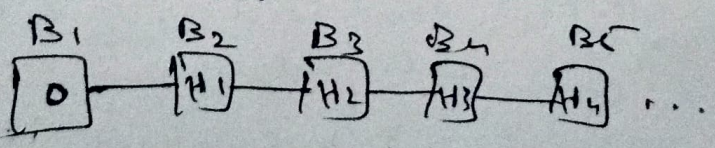
every time we need to change the block/ add a new block it should be validated first then we use POW to make it secured.

- it takes atleast 10min to add a block.
- blockchain is stored on multiple machines. so to add new data it has to be verified by everyone.
- then we have concept of consensus algorithm where we make the blockchain secured.

To change block:

- need super computers
- 50% majority in blockchain network is.

Suppose 5th block has 4th block's hash value so on. but 1st block's has value ... its zero. so 1st block is called 'Genesis block'



Genesis block.

1st block is created by the inventor of blockchain

- Satoshi nakamoto.

Types of block chain:-

majorly for cryptocurrency.

Public blockchain:

- open
- anyone can be part of it.

Private blockchain:

- specially for single company.

Federated block chain:

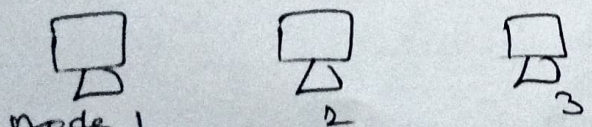
- group of people / companies.
- anyone can't be added, they're added by head of the block chain.
- permissive blockchain
- permission less blockchain.

∵ we use POW, public block chain is slow.

—x—

Consensus:- in blockchain

- block chain is distributed ledger.



all nodes will contain the exact copies of the blockchain.

Suppose, if a new block is to be added, if one of the node is malicious, then whole chain may be corrupted, that is where we use the consensus algorithm to make secured

diff. types of consensus algorithms.

POW

POS (Proof of stake)

- we should spend huge computing power on POW so its not needed in case of POS

(POET) - Proof of elapsed time (by Intel)

POD - " " deposit (enters blockchain after inserting an amount)

POC - " " capacity (consumes hard drive space)

Proof Of Work :- (POW)

its a consensus algorithm used in Bitcoin.

Ethereum in Blockchain :- (inventor - Vitalik Buterin)

ethereum	Bitcoin
building apps/websites which runs on decentralized network	Peer to peer electronic cash system for cryptocurrency.

EVM - ethereum Virtual machine.

to run any app/software. we need this virtual machine for decentralized apps. (or Dapps)

its an app building platform.

Ether - crypto currency in ethereum.

We use 'solidity' language to build apps on ethereum.

Smart Contract - Ethereum

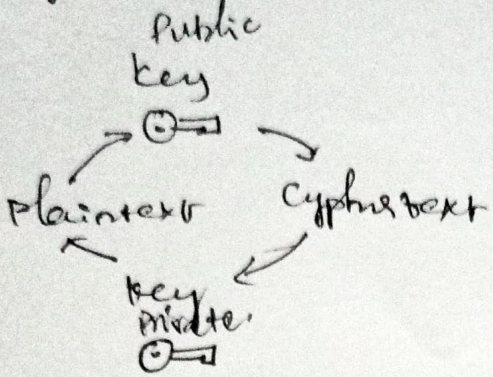
Hyperledger in Blockchain:-

its not a blockchain / cryptocurrency.
its a project.

Cryptography:-

- It is the practice and study of techniques for secure communication in the presence of 3rd parties called adversaries

- working:-



- encryption
- Signature
- Key derivation
- Hashing