Vaibhav   Roll — 18IT251

①

Centralized networks.— There is a single center owner and it is single point of contact. And due to this there is a issue of single point falicure.

Decentralized networks. — extension of central networks having multiple central owner having copy of resource. This eliminate single point falicure. But, neith multiple owner acces speed is compromised.

Distributed network — it avoid centralization completly. The main idea for the distributed network lies in the concept that everyone get acces, and everyone get equal acces.

2)

Enhanced ~~techn~~ security :-

As the single point of contact is removed. it eliminate the risk of single point faliure. The logs of transaction in blockchain is also encrypted.

Distributed ledger :-

The ledger is maintained by all user in the network. This also distribute the computational power.

Consensus :-

Every blockchain runs on consensus algorithm. It is desinged in a way to help ~~make~~ the network making decission.

Tamper proof :-

Since every node have a copy of transaction manipulating a single node can't effect the overall network.

3). Network view of blockchain:

A blockchain network is a technical infrastructure that provides ledger and smart contract (chaincode) services to application. Primarily, smart contract are used to generate transaction which are subsequently distributed to every peer node in the network where they are immutably recorded on their copy of ledger. The user of application might be the end user or blockchain admin.

Structure of blockchain:-

3 core component in structure:-

1) Blocks:- A list of transaction recorded into a ledger over a given period. All blockchain record movement of their cryptocurreny as primary objective

2) Chain — A hash link that link one block to another. The hash is created from data in block.

3) Network — The network is composed of free nodes. Each nodes contain complete record of transaction that was recorded in blockchain.

4) Transaction structure -

Version No - 4B - used to specify rule to be used by miners and nodes for transaction.

I/P counter - 1B - 9B - Number of input included in transaction

List of input - variable - specifies transaction input

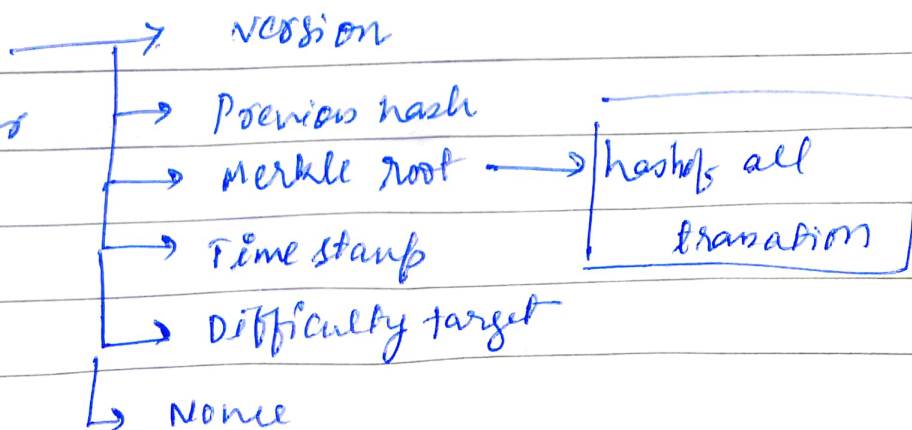Out - counter - 1B - 9B - A positive integer representing number of output.

list of output - variable - output included in transaction.

lock - time - 4B - earliest time when transaction became valid.

Block - structure.

Consist of :-
1) Block size
2) Block header ⟶ version
3) Transaction counter ⟶ Previous hash
4) Transactions ⟶ merkle root ⟶ hash of all transaction
⟶ Time stamp
⟶ Difficulty target
⟶ Nonce

5) The lifecycle follows the journey of a single transaction as it makes its way through each stages in the process of joining the blockchain. Transaction is process of sending and recieving but it is done digitally in blockchain.

Each transaction is signed by the digital signature of sender. Whenever the transaction is ~~into~~ broadcasted into the network the miners group this transaction into block and assign the hash value by finding proof of work. Now, Block is placed in blockchain.

As block gain conformation it get accepted and transaction is completed.

6) Blockchain architecture :-

a) Data layer - build the data structure and physical storage and consist of Data blocks, Markle tree, Assymetric encryption, chain.

b) Network layer - Blockchain uses distributed networks such that everyone have awes of it.

c) Physical layer - They compromises of physical devices on network which ar nodes in Blockchain and are connected as a P2P network where peers are equally privilaged

d) virtualization layer - used to allocate hardware and resource to virtual machine

e) consensus layer - This layer deal with enforcmet of network rule. It allow decentralization

f) Incentive layer — deals with distribution of rewards and motivate people to use the networks .

g) Application layer - Include capabilities that provide application on top of blockchain.

7). Smart contract are simply programs stoored on a blockchain that run when predetermin conditions are met. They typically are used to automate the execution of an agreement so that all participant can be immediatly certain of outcome without third party involument.

Smart contract permits trusted transaction and agreement to be carried out among disparse, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism