# BLOCKCHAIN.
# ASSIGNMENT-1

1) What is mining and Explain it significance with respect to Bitcoin? How much computation power is required for it?.

Ans :- Mining is the process by which new Transactions are validated & added to the so-called Blockchain. Those nodes who are participating in mining process called miners.

So, when the new bitcoin transaction happens in the network that is broadcasted on the network. the miners listen to this Broadcasting and Engage in transaction verification. once they are verified they are added to the Block.

A peer-to-peer computer process, Blockchain mining is used to secure and verify bitcoin transactions. mining involves Blockchain miners who add Bitcoin transaction data to Bitcoin's global public ledger. of past transactions.

In the ledgers, blocks are secured by Blockchain miners and are connected to Each other forming a chain.

Bitcoin mining serves a crucial function to validate and confirm new transactions to Blockchain and to prevent double-spending by bad actors. It is also the way that new bitcoins are introduced into the system.

These Blockchain miners setup and run Specialised Blockchain mining software on their computers, which allows them to safely interact with other. when machine downloads Software joins the network & start, mining Bitcoins, It is refered as "node".

## Types of mining

Into 3 Categories

1. Individual mining
2. pool mining
3. Cloud mining

## ① Individual mining :-

When mining is done by the individual, user registration as a miner is necessary. As soon as the transaction takes place, a mathematical problem is given to all the single users in Blockchain network to solve. The first one to solve gets rewarded once solution is found, all other miners in Blockchain network will validate the decrypted value and then add it to blockchain. Thus, verifying transaction.

## ② pool mining :-

In a pool mining, a group of users work together to approve the transaction. Sometimes the complexity of the data encrypted in blocks makes it difficult for a user to decrypt the encoded data alone. So, a grp of miners work as a team to solve it. After the validation of result reward is split b/w the users.

## ③ Cloud mining :-

Cloud mining eliminates the need for Computer hardware & software. Its a hassle free method to extract BLOCKS.

But also It has its own disadvantages that operational functionality is limited with Limitations on Bitcoin Hashing.
Software upgrades are restriced and so is the Verification process

→ Average time for mining process is 10min.

→ winner of Block will go into Existing Block-chain then trancaction is confirmed.

→ once winner is decides the winner gets or provided the reward of 6.25 Bitcoins

→ Unconfirmed trancactions again goes into mempool.

→ The loo seas who are present in the process they work for validate winners.

Because if the winner may be hacker that is

why miners validate them. then Bitcoin software gives rewards.

Among validation atleast 51% of nodes if they approve, then Bitcoin software validates that miner as winner. (This is proof of work).

The Commutational power of ~~Blockchain~~ Bitcoin is estimated as 1449 kilowatt hours. of Energy to mine a single Bitcoin.

For mining Bitcoins, users are rewarded in bitcoins. this mechanism form the pivot around which Bitcoin economy revolves.

While the cost & difficulty of mining bitcoins individually continue to increase, several Cloud-based mining services have gradually Emerged.

When using bitcoins, Block chain mining is a process that verifies each stage of the transaction. The people participating are known as blockchain miners, and their primary goal is to conferm the movement of cash from one computer in the network to another through a maze of computing gear and software.

Some of the uses of Blockchain mining:

1) Validating transactions
2) Conferming transactions.
3) maintaining safe channels.

2) Explain the properties of the Blockchain and mention one property which you like the most.

Ans:- A Blockchain is a decentralized ledger that records all transactions that are visible on a public network. A Blockchain's architecture allows these transactions to be Autonomous and immature.

The Bitcoin Blockchain was created to allow a network to coordinate & reach "Consensus" on shared data. Blockchain were created to solve the problem of coordinating data with people around the world, who don't necessarily know or trust each other, but would still like to transact in some capacity.

Some of the properties of Blockchain :-

① Security

② Immutable

③ Transparency

④ Distributed.

⑤ Concensus.

⑥ DA

① Security :-

Blockchains have 2 primary security mechanisms : network structure & cryptography. In Blockchain technology, cryptography is used extensively to sign data in order to prove that a transaction was approved by owners of the funds. The decentralized structure of network eliminates any central points of failure. To compromise in an open blockchain network, a hacker would have to control a majority of nodes at same time. This makes a network attack very expensive & impractical.

Because of Blockchain is designed as a distributed ledger, many computers are connected to form as a network. As previously mentioned, this structure is refered to as a decentralized or peer-to-peer network. So If someone wants to hack the network they must hijack the entire Consensus proc The chances of this occuring are extremely low, which is a testament to security

## Transparency:

All transactions on a public blockchain, like Bitcoin, are viewable to anyone with an internet connection. Each transaction is assigned its own unique ID known as transaction hash. These Identifiers can be used to look up a public record of the transaction hash. These Identifiers can be used to look up a public record of transaction, also known as a transaction receipt. A transaction reciept includes the address involved, the amount transferred, a timestamp, transfer fees & more. All computers on the network have access to all transactions records, ensuring a high level of transparency. Because of the transparency provided many institutions, included nonprofits, can use Blockchain to instill confidence in financial practices

## Immutability :-

once a block is confirmed the data recorded to the blockchain cannot be removed or altered, Each block is stacked upon the previous block. The next block must have the preceding block's hash in order to be added to the chain. This assures that the blockchain stays in chronological order, effectively making it tamper-proof.

## Distributed:

Each computer running the blockchain's software has a copy of all the information contained in that blockchain. Information isn't processed through a central server, but is transmitted & verified by nodes in parts of network. The network functions based on set of rules that every client must follow exactly; if blocks are broadcast to the network & do not follow the validity rules the blockchain will be rejected. A block-chain's network is distributed, allowing for an egalitarian, peer-based network

that can self check

## Consensus:

Every node of the Bitcoin network contributes to consensus, the process by which the data is agreed upon and becomes the truth on the network. However certain nodes called miners play a very important role in this process. Nodes work together to verify the information being transmitted by others nodes without relying on a central BOOKkeeper. once all the messages (Transactions) are inside, there is a set of rules that dictate who may seal the envelope (block) & under what conditions.

~~The method which I~~

The property which I like the most is the transparency because. It is one of the best features of blockchain is its transparency It means that it is entirely traceable and much easier to maintain, and one of the areas where Blockchain technology shows its transparency is through Bitcoin

for cyber security sector, blockchain technology is creating new oppurtunities that haven't been envisioned before. With roots of cryptography & security, it makes sense that blockchain is introducing new ways to store information, make safe transactions, and enable trust.

Scanned with CamScanner