1. What is Mining and explain its significance with respect to bit coin? How much computation power is required for it?

A)

In simple terms Crypto currency mining is a process of creating new digital coins.With respect to Bitcoin, Mining is the process of verifying bitcoin transactions and storing them in a blockchain(ledger).

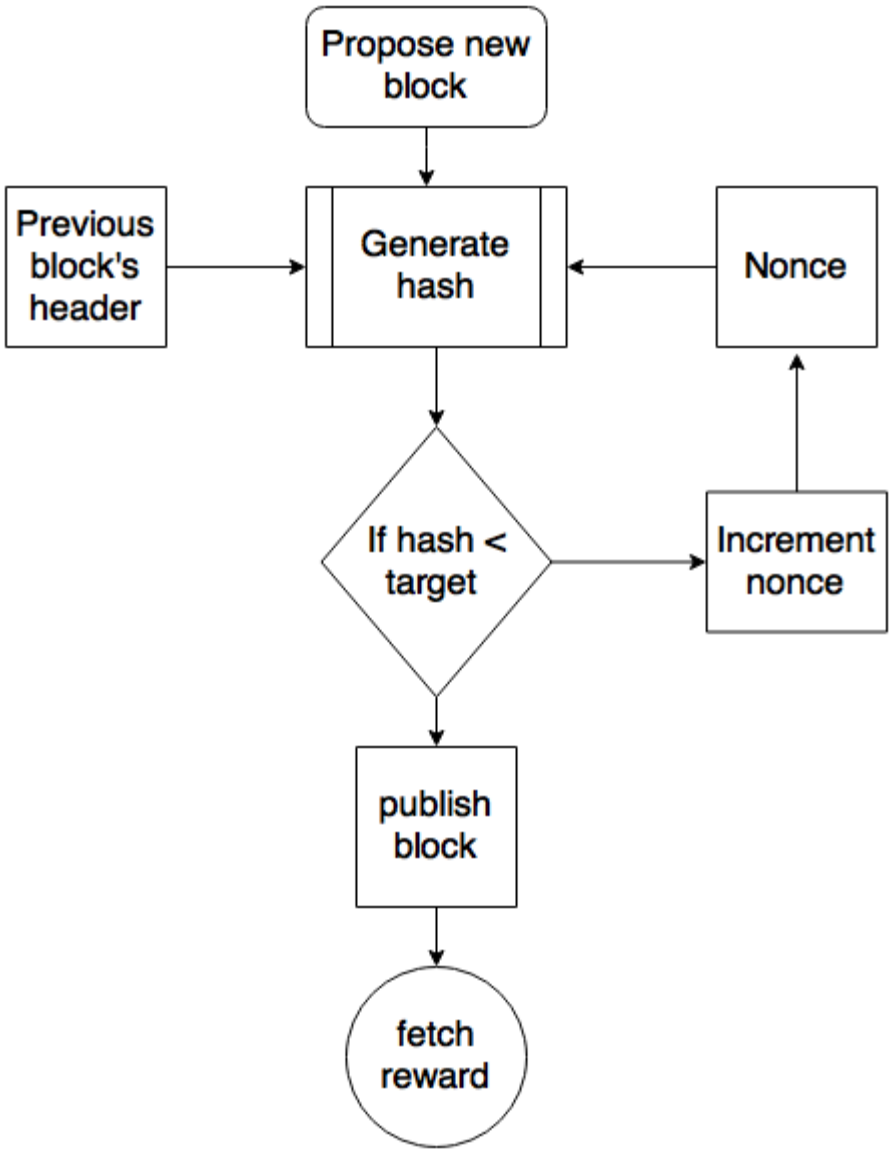
Bitcoin mining is a computation-intensive process that uses complicated computer code to generate a secure cryptographic system.

The bitcoin miner is the person who solves mathematical puzzles(also called proof of work) to validate the transaction.

Numerous miners take part simultaneously to solve the complex mathematical puzzle, the one who solves it first, wins 6.25 bitcoin as a part of the reward.

Miner verifies the transactions(after solving the puzzle) and then adds the block to the blockchain when confirmed.

Once the minor adds the block to the blockchain, bitcoins are then transferred which were associated with the transaction.



Nonce –

There is 2 important topics in mining 1.nonce 2.Hash

Nonce stands for “Number used only once”. As we know the miner has to calculate the hash which should be below the target hash assigned to him.

Hash value obtained for a particular nonce value.

Why Do Bitcoin Needs To Be Mined?

Bitcoin is a digital currency where there are chances of copying, double-spending the same coin more than once. Mining solves these problems.

Why Mine Bitcoins?

There are several pros of mining a bitcoin:

- Mining bitcoin helps support the Bitcoin ecosystem.
- Bitcoin mining helps miners to earn rewards in form of bitcoins.
- It is the only way to release new cryptocurrencies into circulation.

Requirements to Mine Bitcoin

more computing power is required to mine bitcoin.

When there is more computing power working together to mine for bitcoins, the difficulty level of mining increases. Therefore, in order to mine bitcoins, the user must possess-

- Specialized mining hardware is called “application-specific integrated circuits,” or ASICs.
- A Bitcoin mining software to join the Blockchain network.
- Powerful GPU (graphics processing unit).
- **computation power**
- Bitcoin transaction takes **1,449 kWh** to complete.
-

2. Explain the properties of the block chain and mention one property which you like the most.

Properties of Block chain

1) Mining
2) Consensus protocol
3) Hash cryptography
4) Distributed p2p network
5) Immutable
6) Decentralized

These are the main properties

Mining

In simple terms Crypto currency mining is a process of creating new digital coins. Mining involves finding of nonce (number only once used) to generate hash.
In mining miner verify the bit coin transaction to prevent double spending of digital coin.
Through the mining process miners get the rewards like bitcoin. At present miners receives 6.25 BTC as reward. The reward automatically set by the bitcoin software.
After the completion of mining procedure block will be created and this block is get into the block chain.

Hash

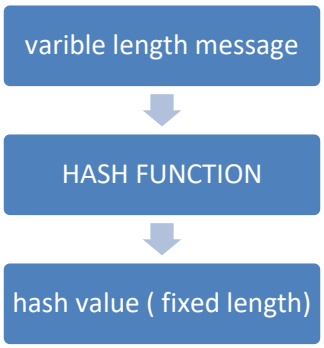
A hash function is a mathematical function that takes an input string of any length and converts it to a fixed-length output string. The fixed-length output is known as the hash value.

Properties of hash

.

- **Deterministic:** A hash function must be deterministic, which means that for any given input a hash function must always give the same result.
- **Avalanche Effect:** This means for a small change in the input, the output will change significantly.
- **Puzzle Friendliness:** This means even if one gets to know the first 200 bytes, one cannot guess or determine the next 56 bytes.
- **Fixed-length Mapping:** For any input of fixed length, the hash function will always generate the output of the same length.
- **Collision resistant:**

- **Pre image resistance:**



Distributed Ledger

All network participants have a copy of the ledger for complete transparency. A public ledger will provide complete information about all the participants on the network and transactions

A ledger is a system containing all the records of a input and output of a process. A distributed ledger is a data structure which is spread across different computing devices. DLT (Distributed Ledger Technology) is the technology that distributes records across all the users.

Consensus

Consensus is a process of ensuring that all the different users in a block chain come to an agreement regarding the current state of blockchain. There are several consensus mechanisms that are used by different block chains to achieve consensus. For example, Bitcoin uses Proof-of-Work while Ethereum is moving from Proof-of-Work to Proof-of-Stake algorithm.

Decentralized

The blockchain network is decentralized which means that there is no central governing authority that will responsible for all the decisions. Rather a group of nodes makes and maintain the network. Each and every node in the blockchain network has the same copy of the ledger. Decentralization property offers many advantages in the blockchain network

Immutable

Immutability means that the blockchain is a permanent and unalterable network. Blockchain technology functions through a collection of nodes.

- Every node in the network has a copy of the digital ledger. To add a transaction every node checks the validity of the transaction and if the majority of the nodes think that it is a valid transaction then it is added to the network. This means that without the approval of a majority of nodes no one can add any transaction blocks to the ledger.
- Any validated records are irreversible and cannot be changed. This means that any user on the network won't be able to edit, change or delete it

I like this property very much why because this prevent tampering of data. Due to this property data will be more secure, can't change the data.

THANNK YOU