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

Bitcoin Mining:

- Bitcoin mining is the process by which new bitcoins are entered into circulation. It is also the way the network confirms new transactions and is a critical component of the block chain ledger's maintenance and development.
- "Mining" is performed using sophisticated hardware that solves an extremely complex computational math problem. The first computer to find the solution to the problem receives the next block of bitcoins and the process begins again.
- Cryptocurrency mining is painstaking, costly, and only sporadically rewarding. Nonetheless, mining has a magnetic appeal for many investors who are interested in cryptocurrency because of the fact that miners receive rewards for their work with crypto tokens.
- This may be because entrepreneurial types see mining as pennies from heaven, like California gold prospectors in 1849.
- The bitcoin reward that miners receive is an incentive that motivates people to assist in the primary purpose of mining to legitimize and monitor Bitcoin transactions, ensuring their validity.
- Bitcoin is a "decentralized" cryptocurrency, or one that does not rely on any central authority like a central bank or government to oversee its regulation.
- Because bitcoin is not overseen or regulated by a central authority, bitcoin miners confirm and verify transactions by solving complex mathematical cryptography calculations, which ultimately are included in a block to the block chain.
- Miners receive the latest batch of transaction data, which is then run through a cryptographic algorithm. A hash, or string of numbers and letters that does not reveal any transaction data, is generated and

used for validity. The hash is designed this way to help ensure that its corresponding block has not been tampered with. If even one number is different or out of place, the corresponding data generates a different hash. The previous block's hash is included within the next block so that, if something has been changed in the previous block, the generated hash then changes. The hash must also be below a specified target set by the hash algorithm. If the generated hash is too big, it is generated again until it is below its specified target.

- The hashing process is designed to make solving transaction-related algorithms more challenging over time. This means solving these algorithms also requires more and more computing resources.

- To reward bitcoin miners, a certain number of bitcoin are issued to them in exchange for doing the work. Bitcoin mining, therefore, accomplishes three tasks. It verifies bitcoin transactions, creates a way to issue more currency and incentivizes more bitcoin mining.

- The current processing power needed for bitcoin mining today means access to powerful computers and large amounts of electricity are a must. Bitcoin mining could originally be done by individuals on single computers. However, because the difficulty level of solving transaction-related algorithms grows over time, individual computers are highly unlikely to be able to mine bitcoin. Instead, most bitcoin miners use application-specific integrated circuits (ASICs) and other methods to mine for bitcoin.

- The mining reward amount changes by half every four years.

- It takes an estimated **1,449 kilowatt hours** (kWh) of energy to mine a single bitcoin. That's the same amount of energy an average U.S. household consumes in approximately 13 years.

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

A blockchain is a chain of blocks that contains information. Most people think that Blockchain is Bitcoin and vice-versa. But it's not the case. In fact, Bitcoin is a digital currency or cryptocurrency that works on Blockchain Technology. Blockchain was invented by Satoshi Nakamoto. As the name suggests, Each block consists of a number of transactions, and each transaction is recorded in the form of a Hash. Hash is a unique address assigned to each block during its creation and any further modification in the block will lead to a change in its hash.

1. 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.

2. Distributed

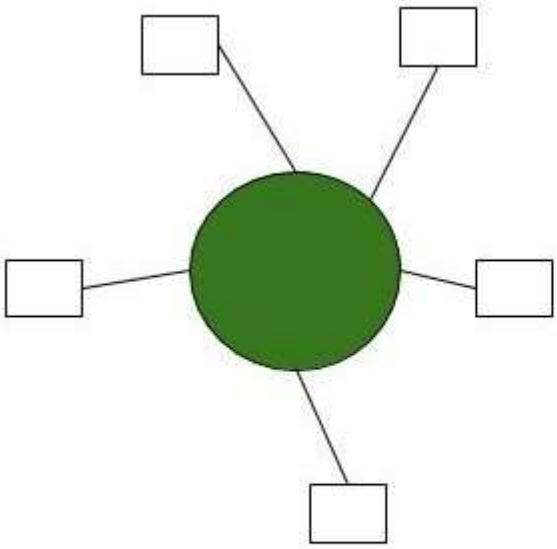
All network participants have a copy of the ledger for complete transparency. A public ledger will provide complete information about all the participants on the network and transactions. The distributed computational power across the computers ensures a better outcome. Distributed ledger is one of the important features of blockchains due to many reasons like:

- In distributed ledger tracking what's happening in the ledger is easy as changes propagate really fast in a distributed ledger.
- Every node on the blockchain network must maintain the ledger and participate in the validation.
- Any change in the ledger will be updated in seconds or minutes and due to no involvement of intermediaries in the blockchain, the validation for the change will be done quickly.
- If a user wants to add a new block then other participating nodes have to verify the transaction. For a new block to be added to the blockchain network it must be approved by a majority of the nodes on the network.
- In a blockchain network, no node will get any sort of special treatment or favors from the network. Everyone will have to follow the standard procedure to add a new block to the network.

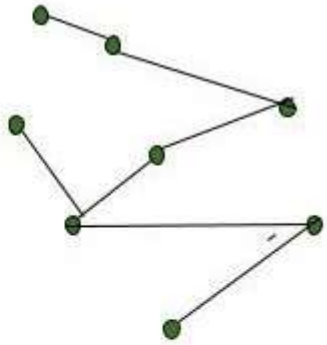
3. Decentralized

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:

- As a blockchain network does not depend on human calculations it is fully organized and fault-tolerant.
- The blockchain network is less prone to failure due to the decentralized nature of the network. Attacking the system is more expensive for the hackers hence it is less likely to fail.
- There is no third-party involved hence no added risk in the system.
- The decentralized nature of blockchain facilitates creating a transparent profile for every participant on the network. Thus, every change is traceable, and more concreate.
- Users now have control over their properties and they don't have to rely on third-party to maintain and manage their assets.



Centralised Network



Decentralised network

4. Secure

All the records in the blockchain are individually encrypted. Using encryption adds another layer of security to the entire process on the blockchain network. Since there is no central authority, it does not mean that one can simply add, update or delete data on the network. Every information on the blockchain is hashed cryptographically which means that every piece of data has a unique identity on the network. All the blocks contain a unique hash of their own and the hash of the previous block. Due to this property, the blocks are cryptographically linked with each other. Any attempt to modify the data means to change all the hash IDs which is quite impossible.

5. Consensus

Every blockchain has a consensus to help the network to make quick and unbiased decisions. Consensus is a decision-making algorithm for the group of nodes active on the network to reach an agreement quickly and faster and for the smooth functioning of the system. Nodes might not trust each other but they can trust the algorithm that runs at the core of the network to make decisions. There are many consensus algorithms

available each with its pros and cons. Every blockchain must have a consensus algorithm otherwise it will lose its value.

6. Unanimous

All the network participants agree to the validity of the records before they can be added to the network. When a node wants to add a block to the network then it must get majority voting otherwise the block cannot be added to the network. A node cannot simply add, update, or delete information from the network. Every record is updated simultaneously and the updations propagate quickly in the network. So it is not possible to make any change without consent from the majority of nodes in the network.

7. Faster Settlement

Traditional banking systems are prone to many reasons for fallout like taking days to process a transaction after finalizing all settlements, which can be corrupted easily. On the other hand, blockchain offers a faster settlement compared to traditional banking systems. This blockchain feature helps make life easier.

Blockchain technology is increasing and improving day by day and has a really bright future in the upcoming years. The transparency, trust, and temper proof characteristics have led to many applications of it like bitcoin, Ethereum, etc. It is a pillar in making the business and governmental procedures more secure, efficient, and effective.