# ASSIGNMENT :- 1

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

Mining is the process by which networks of specialized computers generate and release new Bitcoin and verify new transactions.

Miners use huge computational power(Mining Rigs) to MIne the block, they verify the transactions and make a block with n number of transactions which will be added to the existing continuation block. Once the block is added to the existing ledger it becomes immutable (which cannot be tampered with or changed once added). And they get rewards for validating the transactions.

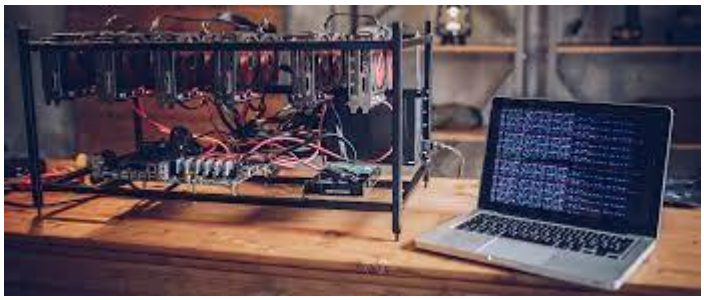
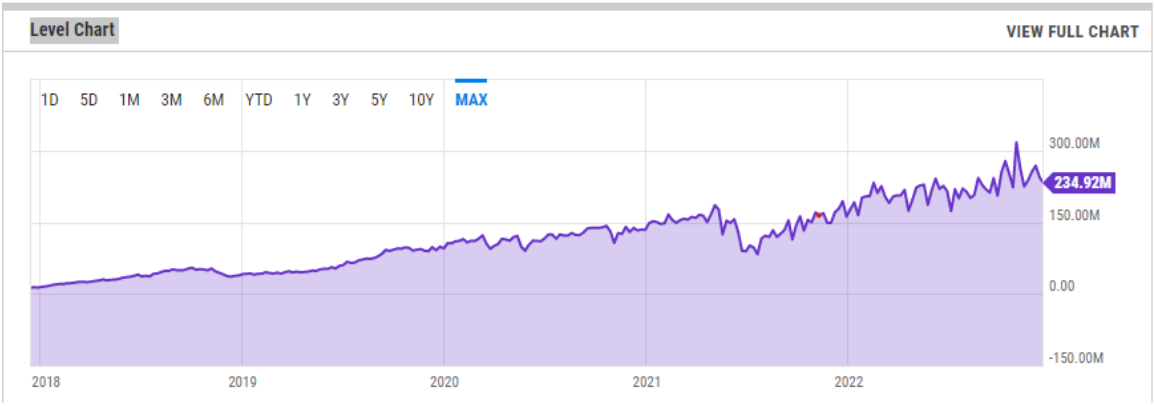


**Fig:- (Mining Rig)**

**Bitcoin Hashrate :-**

Hashrate is the measure of computational power used to verify transactions and add blocks in a Proof-of-work (PoW) blockchain.




**---(Fig: Bitcoin Hashrate)**

There are total of 21 million bitcoins. As of Today(17/12/2022), 19 million bitcoins are mined. Only 2 million bitcoin remained to mine.

**Bitcoin Halving:-**

After every 210,000 blocks mined, or roughly every four years, the block reward given to Bitcoin miners for processing transactions is cut in half. This event is referred to as halving because it cuts in half the rate at which new bitcoins are released into circulation. This is Bitcoin's way of enforcing synthetic price inflation until all bitcoins are released.

This rewards system will continue until around the year 2140, when the proposed limit of 21 million coins is reached. At that point, miners will be rewarded with fees, which network users will pay, for processing transactions. These fees ensure that miners still have the incentive to mine and keep the network going.

Time Span: January 9th, 2009 to November 28th, 2012.

Block Span: 0 to 210,000.

Block Reward: 50 BTC per block mined.

**First halving:**

The 2012 bitcoin halving was the first halving and happened on November 28th, 2012.

- New BTC Per Block Before: 50 BTC per block
- New BTC Per Block After 25 BTC per block

**Second halving:**

The second halving occurred on July 9th, 2016.

● New BTC Per Block Before: 25 BTC per block

● New BTC Per Block After: 12.5 BTC per block

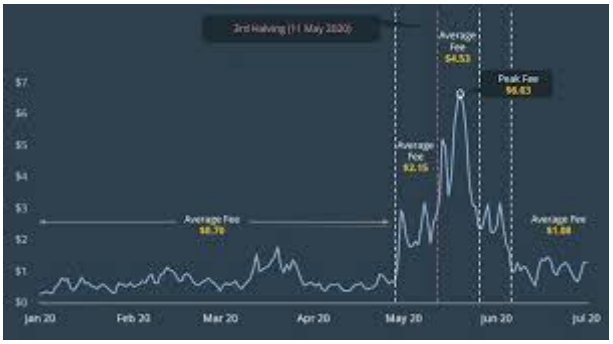
**Third halving:**

The third halving occurred on May 11, 2020.

● New BTC Per Block Before: 12.5 BTC per block

● New BTC Per Block After: 6.25 BTC per block

The next halving will likely occur between February 2024 and June 2024. Mining requires a lot of computational power. It depends upon the difficult rate of the bitcoin which will adjust for every 2016 block (Two weeks).




**(Fig: Average Hashrate to mine a block)**

**Properties of Blockchain:**

● Immutable

● Decentralized

● Secure

● Transparency

● Consensus

**Immutable:**

● Once the data is added to the blockchain ledger it is Immutable it can't be changed or modified further.

● Every node in the network has a copy of the ledger. To add a transaction to the ledger every node checks the validity of the transaction if the majority of the nodes think that is a valid transaction then it will be added to the ledger. Once added it can't be changed

● Each block will have the hash of the transactions and the hash of the previous block. So it's impossible to change a single transaction in any block of the blockchain.

**Decentralized:**

● The public blockchain is a Decentralized blockchain where there is no central authority that is responsible for the decisions taken. The nodes or the community are responsible for taking decisions using DAO(Decentralized Autonomous Organization).

● The blockchain network is a hacker prof due to its decentralized nature. It is impossible to hack a fully decentralized network. The attacker has to control 51% of nodes to modify anything in the blockchain.

**Secure:**

● Each piece of Information on the blockchain is cryptographically linked with each other. One attempt to modify data will change all hash ids of the blockchain.

● Each blockchain has the hash of the transactions and the previous hash of the block. So it's impossible to tamper with data in the blockchain.

**Transparency:**

● All the transactions on the public blockchain are accessible to everyone, anyone can verify the transaction that happened on the blockchain.

● A transaction receipt includes the addresses involved, the amount transferred, a timestamp, transfer fees, etc. Because of the transparency provided, many institutions can use blockchains to instill confidence in their financial practices.

**Consensus:**

Consensus mechanism is set of rules has to be followed before adding data into the blockchain Public blockchain are decentralized which works without any central authority. They involve contribution from thousands of nodes, in such scenarios publicly shared ledgers need an efficient,fair,real-time, functional, reliable, and secure

mechanism to ensure that all the transactions occurring on the network are genuine and all participants agree on a consensus on the status of the ledger

There are different types of mechanism in which these 2 are most used for now.

- POW(Proof of work)
- POS(Prof of stake)

**Proof of Work:**

The POW is a common consensus mechannism used by the most popular cryptocurrency Bitcoin. It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain. The whole mining mechanism of bitcoin needs high energy consumption and a longer processing time as it uses Computation power to mine blocks.

**Proof of Stake:**

The POS consensus mechanism used by Etherum 2.0 that evolved as a low-cost, low-energy consuming alternative to the PoW mechanism. It involves the allocation of responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens staked by the node.

From the above Blockchain all properties i like the Decentralized feature of blockchain, As it is not giving power to a single emtitiy to make decisions. Every node or who participate in it will get equal rights in making decisions. So a single person or authority cant use there agendas or thought here.