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

Bitcoin mining refers to ensuring that transactions are valid and added to the Bitcoin blockchain correctly using a global network of computers running the Bitcoin code. The process of mining is also the means by which new Bitcoins are created.

- The process of bitcoin mining involves the verification of new transactions against the Bitcoin network, which results in the production of new bitcoins.
- Bitcoin mining is the process by which Bitcoin transactions are validated digitally on the Bitcoin network and added to the blockchain ledger.
- It is done by solving complex cryptographic hash puzzles to verify blocks of transactions that are updated on the decentralized blockchain ledger.

Solving these puzzles requires powerful computing power and sophisticated equipment. In return, miners are rewarded with Bitcoin, which is then released into circulation hence the name Bitcoin mining.

To understand bitcoin mining, you have to first understand the three major concepts of blockchain.

1. Public distributed ledger: A distributed ledger is a record of all transactions maintained in the blockchain network across the globe. In the network, the validation of transactions is done by bitcoin users.
2. SHA-256: Blockchain prevents unauthorized access by using a hash function called SHA-256 to ensure that the blocks are kept secure. They are digitally signed. Their hash value, once generated, cannot be altered. SHA-256 takes an input string of any size and returns a fixed 256-bit output, and it is a one-way function—you cannot derive the reverse of the input reverse fully from the output (what you have generated).
3. Proof of work: In blockchain mining, miners validate transactions by solving a difficult mathematical puzzle called proof of work. To do that, the primary objective of the miner is to determine the nonce

value, and that nonce value is the mathematical puzzle that miners are required to solve to generate a hash that is less than the target defined by the network for a particular block.

A bitcoin miner will first select their tools of the trade and set them up. These include:

- Hardware GPU (graphics processing unit), SSD for crypto mining, or ASIC (application-specific integrated circuit)
- Mining software
- A wallet
- Preferred mining pool (if one chooses pool mining option instead of solo mining)

Once all these are set up and the system fired up, it performs the mining process autonomously. Any other human involvement comes in the event of system or network failure, power outage, or regular system maintenance.

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

- Immutable. Immutability means that the blockchain is a permanent and unalterable network.
- Distributed. All network participants have a copy of the ledger for complete transparency.
- Decentralized.
- Secure.
- Consensus.
- Unanimous.
- Faster Settlement.

There are some exciting blockchain features but among them “Immutability” is undoubtedly one of the key features of blockchain technology. But why is this technology uncorrupted? Let’s start with a connecting blockchain with immutability.

Immutability means something that can’t be changed or altered. This is one of the top blockchain features that help to ensure that the technology will remain as it is – a permanent, unalterable network. But how does it maintain that way?

Blockchain technology works slightly different than the typical banking system. Instead of relying on centralized authorities, it ensures the blockchain features through a collection of nodes.

Every node on the system has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it’s valid, then it’s added to the ledger. This promotes transparency and makes it corruption-proof.

So, without the consent from the majority of nodes, no one can add any transaction blocks to the ledger.

Another fact, that backs up the list of key blockchain features is that, once the transaction blocks get added on the ledger, no one can just go back and change it. Thus, any user on the network won’t be able to edit, delete or update it.

The network is decentralized meaning it doesn’t have any governing authority or a single person looking after the framework. Rather a group of nodes maintains the network making it decentralized.

This is one of the key features of blockchain technology that works perfectly. Let me make it simpler. Blockchain puts us users in a straightforward position. As the system doesn’t require any governing authority, we can directly access it from the web and store our assets there.

Blockchain feature is truly making changes –

- **Less Failure:** Everything in the blockchain is fully organized, and as it doesn’t depend on human calculations it’s highly fault-tolerant. So, accidental failures of this system are not a usual output.

- **User Control:** With decentralization, users now have control over their properties. They don't have to rely on any third party to maintain their assets. All of them can do it simultaneously by themselves.
- **Less Prone to Breakdown:** As decentralized is one of the key features of blockchain technology, it can survive any malicious attack. This is because attacking the system is more expensive for hackers and not an easy solution. So, it's less likely to breakdown.
- **No Third-Party:** Decentralized nature of the technology makes it a system that doesn't rely on third-party companies; No third-party, no added risk.
- **Zero Scams:** As the system runs on algorithms, there is no chance for people to scam you out of anything. No one can utilize blockchain for their personal gains.
- **Transparency:** The decentralized nature of technology creates a transparent profile of every participant. Every change on the blockchain is viewable and makes it more concrete.
- **Authentic Nature:** This nature of the system makes it a unique kind of system for every kind of person. And hackers will have a hard time cracking it.
- Every information on the blockchain is hashed cryptographically. In simple terms, the information on the network hides the true nature of the data. For this process, any input data gets through a mathematical algorithm that produces a different kind of value, but the length is always fixed.

Usually, a public ledger will provide every information about a transaction and the participant. It's all out in the open, nowhere to hide. Although the case for private or federated blockchain is a bit different. But still, in those cases, many people can see what really goes on in the ledger.

That's because the ledger on the network is maintained by all other users on the system. This distributed computational power across the computers to ensure a better outcome.

Blockchain Important Features?

- **No Malicious Changes:** Distributed ledger responds really well to any suspicious activity or tamper. As no one can change the ledger and everything updates real fast, tracking what's happening in the ledger is quite easy with all these nodes.
- **Ownership of Verification:** Here, nodes act as verifiers of the ledger. If a user wants to add a new block others would have to verify the transaction and then give the green signal. This provides the user with fair participation.
- **No Extra Favors:** No one on the network can get any special favors from the network. Everyone has to go through the usual channels and then add their blocks. It's not like you have more power so you'll get more privileges.
- **Managership:** To make the blockchain features work, every active node has to maintain the ledger and participate for validation.
- **Quick Response:** As I said earlier, removing the intermediates quickens the system response. Any change in the ledger is updated in minutes or even seconds! 1. Immutability

There are some exciting blockchain features but among them "Immutability" is undoubtedly one of the key features of blockchain technology. But why is this technology uncorrupted? Let's start with a connecting blockchain with immutability.

Immutability means something that can't be changed or altered. This is one of the top blockchain features that help to ensure that the technology will remain as it is – a permanent, unalterable network. But how does it maintain that way?

Blockchain technology works slightly different than the typical banking system. Instead of relying on centralized authorities, it ensures the blockchain features through a collection of nodes.

Every node on the system has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof.

So, without the consent from the majority of nodes, no one can add any transaction blocks to the ledger.

Another fact, that backs up the list of key blockchain features is that, once the transaction blocks get added on the ledger, no one can just go back and change it. Thus, any user on the network won't be able to edit, delete or update it.

Fight Corruption?

We know how every year there's a massive amount of money that gets hacked through our regular channels. Many people spend Trillions of money to protect their business from any external hacks. However, we always forget to count the internal cybersecurity risks that come from corrupted people and authorities.

In many cases, there's always an internal link for these hacks to know about all the security measures, so in the end, we pay the price for our trust. As you all know banks aren't that trustable now and the global economy needs a trustless environment to fully overcome this issue.

So, when it comes to a corruption-free environment, you can easily assume that blockchain can definitely change a lot of these scenarios.

If businesses start to integrate blockchain technology to maintain their internal networking system, no one would be able to hack into it or alter or even steal information.

Public blockchains are a perfect example of this. Everyone in the public blockchain can see the transactions, so it is super transparent. On the other hand, private or federated blockchain could be best for enterprises that want to remain transparent among staff and protect their sensitive information along the way from public view.

Decentralized

The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Rather a group of nodes maintains the network making it decentralized.

This is one of the key features of blockchain technology that works perfectly. Let me make it simpler. Blockchain puts us users in a straightforward position. As the system doesn't require any governing authority, we can directly access it from the web and store our assets there.

You can store anything starting from cryptocurrencies, important documents, contracts or other valuable digital assets. And with the help of blockchain, you'll have direct control over them using your private key. So, you see the decentralized structure is giving the common people their power and rights back on their assets.

Blockchain feature is truly making changes –

- **Less Failure:** Everything in the blockchain is fully organized, and as it doesn't depend on human calculations it's highly fault-tolerant. So, accidental failures of this system are not a usual output.
- **User Control:** With decentralization, users now have control over their properties. They don't have to rely on any third party to maintain their assets. All of them can do it simultaneously by themselves.
- **Less Prone to Breakdown:** As decentralized is one of the key features of blockchain technology, it can survive any malicious attack. This is because attacking the system is more expensive for hackers and not an easy solution. So, it's less likely to breakdown.
- **No Third-Party:** Decentralized nature of the technology makes it a system that doesn't rely on third-party companies; No third-party, no added risk.
- **Zero Scams:** As the system runs on algorithms, there is no chance for people to scam you out of anything. No one can utilize blockchain for their personal gains.

- **Transparency:** The decentralized nature of technology creates a transparent profile of every participant. Every change on the blockchain is viewable and makes it more concrete.
- **Authentic Nature:** This nature of the system makes it a unique kind of system for every kind of person. And hackers will have a hard time cracking it.

Enhanced Security

As it gets rid of the need for a central authority, no one can just simply change any characteristics of the network for their benefit. Using encryption ensures another layer of security for the system.

But how does it offer so much security compared to already existing techs?

Well, it's extremely secure because it offers a special disguise – Cryptography. Added with decentralization, cryptography lays another layer of protection for users. Cryptography is a rather complex mathematical algorithm that acts as a firewall for attacks.

Every information on the blockchain is hashed cryptographically. In simple terms, the information on the network hides the true nature of the data. For this process, any input data gets through a mathematical algorithm that produces a different kind of value, but the length is always fixed.

You could think of it as a unique identification for every data. All the blocks in the ledger come with a unique hash of its own and contain the hash of the previous block. So, changing or trying to tamper with the data will mean changing all the hash IDs. And that's kind of impossible.

You'll have a private key to access the data but will have a public key to make transactions.

Blockchain Security provides premium protection for enterprises. Learn more about Blockchain Security.

Hashing is Irreversible!

Hashing is quite complex, and it's impossible to alter or reverse it. No one can take a public key and come up with a private key. Also, a single change in the input could lead to a completely different ID, so small changes aren't a luxury in the system.

If someone wants to corrupt the network, he/she would have to alter every data stored on every node in the network. There could be millions and millions of people, where everyone has the same copy of the ledger. Accessing and hacking millions of computers is next to impossible and costly.

That's why it's one of the best blockchain features. As it's too hard to bypass, you won't have to worry about hackers taking all your digital assets from you.

Distributed Ledgers

Usually, a public ledger will provide every information about a transaction and the participant. It's all out in the open, nowhere to hide. Although the case for private or federated blockchain is a bit different. But still, in those cases, many people can see what really goes on in the ledger.

That's because the ledger on the network is maintained by all other users on the system. This distributed computational power across the computers to ensure a better outcome.

This is the reason it's considered one of the blockchain essential features. The result will always be a higher efficient ledger system that can take on the traditional ones.

The Blockchain Important Features.

- **No Malicious Changes:** Distributed ledger responds really well to any suspicious activity or tamper. As no one can change the ledger and everything updates real fast, tracking what's happening in the ledger is quite easy with all these nodes.
- **Ownership of Verification:** Here, nodes act as verifiers of the ledger. If a user wants to add a new block others would have to verify the transaction and then give the green signal. This provides the user with fair participation.
- **No Extra Favors:** No one on the network can get any special favors from the network. Everyone has to go through the usual channels and then

add their blocks. It’s not like you have more power so you’ll get more privileges.

- **Managership:** To make the blockchain features work, every active node has to maintain the ledger and participate for validation.
- **Quick Response:** As I said earlier, removing the intermediates quickens the system response. Any change in the ledger is updated in minutes or even seconds!

Consensus

Every blockchain thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

In simple terms, the consensus is a decision-making process for the group of nodes active on the network. Here, the nodes can come to an agreement quickly and relatively faster. When millions of nodes are validating a transaction, a consensus is absolutely necessary for a system to run smoothly. You could think of it as kind of a voting system, where the majority wins, and the minority has to support it.

The consensus is responsible for the network being trustless. Nodes might not trust each other, but they can trust the algorithms that run at the core of it. That’s why every decision on the network is a winning scenario for the blockchain. It’s one of the benefits of blockchain features.