Question 1 :

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

Answer :

Mining is the process that Bitcoin and several other cryptocurrencies use to generate new coins and verify new transactions. It involves vast, decentralized networks of computers around the world that verify and secure blockchains – the virtual ledgers that document cryptocurrency transactions. In return for contributing their processing power, computers on the network are rewarded with new coins. It's a virtuous circle: the miners maintain and secure the blockchain, the blockchain awards the coins, and the coins provide an incentive for the miners to maintain the blockchain.

bitcoin "mining" is a misnomer. When gold is mined, nothing is achieved beyond the discovery of new gold. When bitcoins are mined, however, a valuable service is provided to the Bitcoin network: decentralized transaction recordation and validation.

Double Spending

Bitcoin relies on miners to record and validate transactions because of a problem inherent in any digital currency system: double-spending. Double spending is the high-tech incarnation of counterfeiting. Say, for example, that a currency user, Alice, has a $5 note and she gives it to Bob. Can Bob be sure that he's received $5 rather than a forgery? In the physical world, probably. In the digital world, probably not.

In the physical world, Alice would have to find paper, ink, and machines capable of making a convincing duplicate of her $5. The cost of that activity, alongside moral scruples and the threat of arrest, keeps counterfeiting in check.

In the digital world, however, a computer file version of a $5 note, like an MP3 file or an MS Word document, can be copied perfectly at effectively no cost. There's no way to tell which file is the original, and the ease of copying means counterfeit currency could rapidly overrun the economy.

To fix this, the inventors of Bitcoin designed a system of network interactions, a protocol, that checks each putative Bitcoin transfer against a public ledger called the blockchain. A crook can try and resend already spent bitcoins until they're blue in the face; if those transactions don't check out, however, miners won't record them and the community ignores the attempt at fraud.

How Does Mining Work?

Listening for Transactions

Bitcoin miners connect to the Bitcoin network like telephone operators. Miners use their computers to listen for transaction requests across the entire network and assemble a list of valid transactions.

Bitcoins are not sent and received like file attachments in an email. There are no files at all, only assignments of bitcoins made to various public addresses. Each public address has a matching private key and only the holder of that key is capable of digitally signing a new transaction request. Additionally, the request must have input. Inputs are the previous transactions that the sender is using to fund the new transaction. If you previously received five bitcoins from Alice and four from Bob, you can list these inputs to fund a new transaction to Cynthia of up to nine bitcoins in value.

Miners check two things when they hear your request. First, they check to make sure that your digital signature proves that you were the recipient of those inputs. Second, they check to make sure that you've not already spent those inputs. To perform this second check, miners peak at a public database of all valid past transactions, called the blockchain, to see if those inputs were already used in a transaction or if they are still available. Copies of this blockchain are stored on the computers of all Bitcoin users that connect to the network.

Thus, miners are playing the role of bank tellers: inspecting checks, making sure all the appropriate signatures and account numbers are there, checking the customer's ID, and looking for proof that the customer has enough cash on hand to fund the transaction.

Completing a "Block"

If everything checks out, the miner will add the transaction to their list of all valid transactions over the last few minutes. Every few minutes, one miner will be selected to add their list, a block, to the official blockchain, thus keeping the public record up to date.

To prevent miners from fraudulently corrupting the blockchain, the Bitcoin protocol makes miners compete. A different miner is empowered to write each block, roughly every 10 minutes, and only valid blocks will be accepted by the rest of the mining community. Here's how that works:

Guess and Check the “Nonce”

A miner’s block will become a part of the chain whenever a majority of the community of miners agree (A) that the transactions listed by the miner are valid—no signatures from impersonators and no double spending—and (B) that the miner correctly guessed a special number, the nonce, that solves a particular math problem. Miners perform this check by looking at the proposed block’s particular digital signature. This signature is a computer-generated product of three inputs, (1) the signature of the predecessor block, (2) a list of valid transactions since that predecessor, and (3) a particular random number, called a nonce.

We need a bit more information about digital signatures to understand it all. Signatures operate by using “hash” functions. At their simplest, hash functions are math equations that take any given input and create a seemingly random output that will always correspond to that particular input.

The hash function used by Bitcoin is called SHA256. Using that function, the input text:

“This is a hash!”

will always output this string of characters:

“dcc67309a9c5c4a6d5434de87dbd4162f745f32b2a6aedf89c89d31d863b022b”

You can try it yourself by visiting an online hash calculator; if you type in “This is a hash!” without the quotes you’ll get the same specific string of numbers and letters.

If a hash function is well written, any change to the inputs will drastically change the output string, and different inputs would never output the same string. By that standard, SHA256 is very well written. For example, changing our input “This is a hash!” even slightly results in entirely different outputs:

“This is a hash!” = “dcc67309a9c5c4a6d5434de87dbd4162f745f32b2a6aedf89c89d31d863b022b”

“This is a hash?” = “d43edbde4b15a97e780c1a9e1392b2c4601750fe03db543b3c4c44624d277641”

“This is a hash brown.” = “5692e888b50c526f7eb95342a6fd56760b2ff95a766414562daa4083bab8bcfc”

Therefore, if the inputs for a new block’s signature are the signature of the predecessor block and a list of recent transactions, the output will be a unique string that could only have been made from that exact data. Because it is the unique product of those inputs, that signature can be used to prove that the transactions therein described happened in a given order: within the current block or some previous block. Try and change the order by making up phony past blocks and the signature will no longer match. This allows the particular beneficiary of a transfer to prove that they were the first to receive the coins; any subsequent double spending of those coins is fraud.

All miners, however, are capable of writing a signature composed of the previous block’s signature and the new transaction list very quickly using their powerful computers. How do we pick a winner at regular intervals to make them compete? The solution is to ask for a string that will be difficult to generate quickly, a specific sort of output string, one that starts with a certain number of zeros, like this:

“0000000000000xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx”

That long line of zeros at the start of the hash is statistically improbable, like flipping a coin and getting heads thirteen times in a row. Nonetheless, a particular combination of inputs will result in a hash output that starts with all those zeros. The combination will involve a particular random number called the “nonce” that miners will have to guess.

The miners repeatedly hash their two known inputs (the previous block signature and the list of new transactions), along with guesses at the random nonce. Eventually, one miner will happen upon a nonce that will give them a signature with the requested number of zeros at the start.

Miners that use more powerful computers can make guesses faster, and, like buying more lottery tickets, these miners will be more likely to win the race to find a particular hash. This is why miners can compete with each other by investing in more powerful computers. More tries at the hash equal more blocks written to the blockchain over time. To prevent blocks from being written too quickly or too slowly as more or less computing power is used by miners, the protocol is adjusted every two weeks to demand a longer, harder-to-guess, or shorter, easier-to-guess, string of zeros at the front of the hash. The target for those adjustments is the generation of a new block every ten minutes.

Whenever a miner solves a block by writing a signature with enough zeros, they broadcast it and the other miners validate the solution and check to make sure that the transactions listed are all valid. If it all checks out, miners will begin competing to solve a new block using the last block's signature as input.

Rewards

That brings us, at last, to the question of why miners mine. This answer is simple, miners mine because the writer of a new block in the blockchain has permission from the protocol to give herself a reward of brand new bitcoins, called a coinbase transaction. That reward started at 50 bitcoins per block. Every four years the protocol is adjusted, reducing the reward by half. One day the reward will be very small, but miners can also be rewarded by collecting fees volunteered by users who request transactions.

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

1)Hardware GPU (graphics processing unit), SSD for crypto mining, or ASIC (application-specific integrated circuit)

2)Mining software

3)A wallet

4)Preferred mining pool (if one chooses the 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.

The price of electricity changes every season. Electricity is consumed not only to mine Bitcoins but also to prevent them from overheating and cooling them down. There is no time length for mining. Many miners mine 24x7 as they can afford the mining cost. Changes in the Bitcoin value are ascertainable, affecting your Bitcoin profit and return on investment. Difficulty in mining can arise due to slow computers, low voltage, or any other factor, affecting efficiency.

Bitcoin mining requires specialized tools, including:

1)Hardware such as GPU (graphics processing unit), SSD for crypto mining, ASIC (application-specific integrated circuit), or the latest FPGA (Field Programmable Gate Array) chips. When purchasing mining hardware, it is important to consider two factors, their hash rate (performance) and electricity consumption.

2)Mining software such as ECOS, BeMine, and Kryptex Miner

3)A bitcoin wallet from which an individual performs bitcoin transactions

4)Preferred mining pool (if one chooses the pool mining option instead of solo mining)

Bitcoin mining hardware performance is measured in terms of hash rate. Current new-generation ASIC miners produce 100 TH/s (trillion hashes per second) and cost somewhere between $8,000 - $10,000. Ordinary CPUs do not have the capacity to produce such fast hash rates. Developed nations may well have an edge when it comes to location because of the low cost of power. Bitcoin is quite power-intensive. It was estimated that one bitcoin transaction requires approximately 1,544 kWh of power to complete, which is equivalent to around 53 days of normal power consumed in an average American household which translates to an average of $200 in cost for a single transaction at 13 cents per kWh.

Question 2 :

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

Answer :

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.

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. A distributed ledger is one of the important features of blockchains due to many reasons :

1) In distributed ledger tracking what's happening in the ledger is easy as changes propagate really fast in distributed ledger.

2) Every node on the blockchain network must maintain the ledger and participate in the validation.

3) 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.

4) 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.

5) 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.

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:

1) As a blockchain network does not depend on human calculations it is fully organized and fault-tolerant.

2) 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.

3) There is no third-party involved hence no added risk in the system.

4) The decentralized nature of blockchain facilitates the creation of a transparent profile for every participant on the network. Thus, every change is traceable and more concrete.

5) Users now have control over their properties and they don't have to rely on third-party to maintain and manage their assets.

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.

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.

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.

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 business and governmental procedures more secure, efficient, and effective.

Consensus mechanisms in the blockchain are one of the properties which would make the network authentication greater transparency. In a blockchain network that agrees on a single version of history, blockchain networks like Bitcoin and Ethereum implement what is known as consensus mechanisms (also known as consensus protocols or consensus algorithms). These mechanisms aim to make the system fault-tolerant. Consensus mechanisms form the backbone of all cryptocurrency blockchains and are what makes them secure.

Consensus is the process by which a group of peers – or nodes – on a network determine which blockchain transactions are valid and which are not. Consensus mechanisms are the methodologies used to achieve this agreement. It’s these sets of rules that help to protect networks from malicious behavior and hacking attacks.

There are many different types of consensus mechanisms, depending on the blockchain and its application. While they differ in their energy usage, security, and scalability, they all share one purpose: to ensure that records are true and honest. Here’s an overview of some of the best-known types of consensus mechanisms used by distributed systems to reach consensus.

Types of Consensus Mechanisms :

1) Proof of Work (PoW)

2) Proof of Stake (PoS)

3) Delegated Proof of Stake (DPoS)

4) Proof of Activity (PoA)

5) Proof of Authority (PoA)

6) Proof of Burn (PoB)

7) Proof of Capacity / Proof of Space (PoC / PoSpace)

8) Proof of Elapsed Time (PoET)

9) Proof of History (PoH)

10) Proof of Importance (PoI)