Blockchain Technology

Prepared by Sivasankar Rao Kunchala on 2022-Nov-07

Assignment 1

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

Answer:-

Mining is a process of creating new digital coins.

The process of recovering these coins requires solving complex puzzles, validating cryptocurrency transactions on a blockchain network and adding them to a distributed ledger to locate them.

Solving these puzzles requires powerful computing power and sophisticated equipment. You need either a graphics processing unit (GPU) or an application-specific integrated circuit (ASIC) in order to set up a mining rig.

By mining, you can earn cryptocurrency without having to put down money for it.

Bitcoin is the first decentralized digital currency that allows peer-to-peer transfers without any intermediaries such as banks, governments, agents, or brokers, using the underlying technology of blockchain.

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. It is done by solving complex cryptographic hash puzzles to verify blocks of transactions that are updated on the decentralized blockchain ledger. In return, miners are rewarded with Bitcoin, which is then released into circulation hence the name Bitcoin mining.

Mining rewards are paid to the miner who discovers a solution to a complex hashing puzzle first, and the probability that a participant will be the one to discover the solution is related to the portion of the network's total mining power.

The rewards for Bitcoin mining are reduced by half roughly every four years. When bitcoin was first mined in 2009, mining one block would earn you 50 BTC. In 2012, this was halved to 25 BTC. By 2016, this was halved again to 12.5 BTC. On May 11, 2020, the reward halved again to 6.25 BTC.

The Digiconomist's Bitcoin Energy Consumption Index estimated that one bitcoin transaction takes 1,449 kWh to complete or the equivalent of approximately 50 days of power for the average US household.

Bitcoin mining uses around as much energy as Argentina, according to the Bitcoin Energy Consumption Index, and at that annualized level of 131.26 terawatt-hours, crypto mining would be in the top 30 of countries based on energy consumption. Energy consumption for bitcoin mining was at its highest at the end of 2021 and the early months of 2022, consuming more than 200 terawatt-hours.

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

Answer:-

A BLOCKCHAIN is a decentralized ledger that records all transactions. A BLOCKCHAIN'S architecture allows these transactions to be autonomous and immutable while using cryptography and a decentralized network design for security. Every transaction is permanently recorded to the blockchain and cannot be altered in any way.

The name blockchain largely refers to the structure of the technology. Blocks contain data that represents transactions, and when a block is created or "mined," all the data contained in the block (several transactions) is added to the chain. Permanently all ledgers are updated to recognize this new consensus. Blocks are then linked together to form a chain and can be referred to at any time, hence the name blockchain.

Because a blockchain is designed as a distributed ledger, many computers (nodes) are connected to form a network. As previously mentioned, this structure is referred to as a decentralized or a peer-to-peer (P2P) network. If someone wants to hack the network, they must hijack the entire consensus process. The chances of this occurring are extremely low, which is a testament to the security inherent to blockchain technology.

The following are the main properties of blockchain technology:-

SECURITY

Blockchain have two primary security mechanisms: network structure and cryptography. In blockchain technology, cryptography is used extensively to sign data in order to prove that a transaction was approved by the owner of the funds. The decentralized structure of network eliminates any central points of failure. To compromise an open blockchain network, a hacker would have to control a majority of the nodes at the same time. This makes a network attack very expensive and impractical.

TRANSPARENCY

All transactions on a public blockchain, like Bitcoin, are viewable to anyone with an internet connection. Each transaction is assigned its own unique ID known as a transaction hash. These identifiers can be used to look up a public record of the transaction, also known as a transaction receipt. A transaction receipt includes the addresses involved, the amount transferred, a timestamp, transfer fees and more. All computers on the network have access to all transactions records, ensuring a high level of transparency. Because of the transparency provided, many institutions, including nonprofits, can use blockchain to instill confidence in their financial practices.

IMMUTABILITY

Once a block is confirmed, the data recorded to the blockchain cannot be removed or edited. Each block is stacked upon the previous block. The next block must have the preceding block's hash in order to be added to the chain. This assures that the blockchain stays in chronological order, effectively making it tamper-proof.

DISTRIBUTED

Each computer running the blockchain's software has a copy of all the information contained in that blockchain. Information isn't processed through a central server, but is transmitted and verified by nodes in parts of the network. The network functions based on a set of rules that every client must follow exactly; if blocks are broadcast to the network and do not follow the validity rules, the block will be rejected. A blockchain's network is distributed, allowing for an egalitarian, peer-based network that can self-check

CONSENSUS

Every node on the Bitcoin network contributes to consensus, the process by which the data is agreed upon and becomes the truth on the network. However, certain nodes called miners play a very important role in this process. Nodes work together to verify the information being transmitted by other nodes without relying on a central bookkeeper. Each consensus mechanism has its own set of rules; it might help to think of them like sealing an envelope. Once all the messages (transactions) are inside, there is a set of rules that dictate who may seal the envelope (block) and under what conditions.

So these properties are what make blockchain interesting. Without these properties, blockchain is just like any other place where you can store data.

The "IMMUTABILITY" property is very interesting, it means that if you have stored data on the blockchain it is guaranteed that data cannot be changed later. This is very important when you want to trust something or when you want to make something more trustable. Because if I am building an application and if I want to change data because everything is in my control, I can change the data and change the data in any way I want to. But with blockchain, that is not possible.