

## **Blockchain Essentials | Day-1 | Assignment**

### **Question 1 : What is your understanding of blockchain?**

A blockchain is a completely growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure, chronological and immutable way in decentralized distributed network. Blockchain is created by the anonymous Satoshi Nakamoto. In blockchain, Each block refers to the previous block and together make the Blockchain. A Blockchain is effective as it is spread over many computers, each of which have a copy of the Blockchain. Blockchain is a mix of technology. Distributed and Cryptography where information is: Verifiable, Unchangeable, tamper-proof, immutable. This mix of technologies will create much wanted transparency and trust in system by eradicating middle man. A blockchain is type of ledger or diary containing information about transactions. Each transaction generates a hash. Hash is a string of numbers or letters. The hash depends not only on the transaction but the previous transaction's hash. Even a small change in a transaction creates a completely new hash. Transactions are entered in the order in which they occurred. Order is very important.

### **Question 2 : What is the core problem blockchain trying to solve?**

Blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically.

Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes. Every transaction and its associated value are visible to anyone with access to the system.

Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.

Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, because they are linked to every transaction record that came before them.

Various computational algorithms are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.

The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. so users can set up algorithms and rules that automatically trigger transactions between nodes.

**Question 3 : What are the features which blockchain will give you?**

1.We have public distributed ledger, which works using a hashing encryption. A public distributed ledger is a collection of digital that is shared, synchronized and replicated around the world, across multiple sites, countries and institutions. If someone tries to alter data in one of the blocks, everyone in the network has a copy of the ledger. In this way, data tampering is prevented.

2.Every block has a hash value, which is the digital signature of the block. To ensure that all the data in the blocks is kept secure from unauthorized access and is not altered. Blockchain uses SHA-256 for encryption. This cryptographic hash algorithm generates an almost unique 256 bit signature for text.

3.All the transactions are approved and verified on the blockchain network using a proof-of-work consensus algorithm. Bit coin uses a Proof of Work System.

4. The blockchain network utilizes the resources of the miners, who are there to validate the transaction rewards. Mining is the process of a miner being rewarded for finding the appropriate nonce first. Miners get paid in Bit coins, and a successful verification is the only way the bit coins get added to the network. that is the concept of mining, and when a miner has completed the proof of work consensus, he is rewarded.

**Question 4 : What all things does a block contain?**

A block contain : 1.Block Number

2.Transaction Records

3.Previous Block Signature

4.Mining Key

1.Each block in a blockchain has different no.

2.Transaction record is any important data which you want to store.

3.To identifying block there is cryptographic hash. A digital signature. Created by hashing the block header twice with the SHA256 algorithm. Every block uses a previous block's hash to create its own hash. block hash is a unique identifier.

4. A hash is like a fingerprint. Each block hash is generated with the help of a cryptographic hash algorithm (SHA 256). Consequently, this helps to identify each block in a blockchain structure easily.

The moment a block is created, it automatically attaches a hash, while any changes made in a block affect the change of a hash too. hashes help to detect any changes in blocks.

**Question 5 : How is the verifiability of Blockchain is been attained?**

In blockchain, once data entered then the data is hard to tamper with due to the blockchain's nature. If someone tries to alter data in one of the blocks, everyone in the network has a copy of the ledger. In this way, data tampering is prevented.

It takes time to proceed with record validation, since the process occurs in each independent network rather than via compound processing power. This means that the system sacrifices performance speed, but instead guarantees high data security and validity.