BSc (Hons) in IT Specialized in CS

Year 2, 2022

Tutorial 06

SNP **Blockchains**

---

1. What is cryptography? What is its role in Blockchain?

- Blockchain uses cryptography to secure users' identities and ensure transactions are done safely with a hash function. Cryptography uses public and private keys in order to encrypt and decrypt data. In the Blockchain network, a public key can be shared with all the Bitcoin users but a private key (just like a password) is kept secret with the users. Blockchain uses SHA - 256 which is secure and provides a unique hash output for every input. The basic feature of this algorithm is whatever input you pass, it will give you a standard alphanumeric output of 64 characters. It is a one-way function from which you can derive an encrypted value from the input, but not vice-versa.

2. What do you mean by blocks in Blockchain technology?

- Blockchain is a distributed database of immutable records called blocks, which are secured using cryptography. Refer to the video to see the various attributes of a block.
- There are a previous hash, transaction details, nonce, and target hash value. A block is like a record of the transaction. Each time a block is verified, it gets recorded in chronological order in the main Blockchain. Once the data is recorded, it cannot be modified.

3. What is a Genesis Block?

- The genesis block is the first block in the Blockchain which is also known as block 0
- In Blockchain, it is the only block that doesn't refer to its previous block.
- It defines the parameters of the Blockchain such as,
    - level of difficulty,
    - consensus mechanism etc. to mine blocks

4. What is a smart contract and list some of its applications?

- Smart contracts are self-executing contracts which contain the terms and conditions of an agreement between the peers
- Some of the applications are:
    - Transportations: Shipment of goods can be easily tracked using smart contracts
    - Protecting copyrighted content: Smart contracts can protect ownership rights such as music or books
    - Insurance: Smart contracts can identify false claims and prevent forgeries
    - Employment contract: Smart contracts can be helpful to facilitate wage payments

5. What is the nonce and how is it used in mining?

   In Blockchain, mining is a process to validate transactions by solving a difficult mathematical puzzle called proof of work. Now, proof of work is the process to determine a number (nonce) along with a cryptographic hash algorithm to produce a hash value lower than a predefined target. The nonce is a random value that is used to vary the value of hash so that the final hash value meets the hash conditions.