Title: Cryptocurrency using blockchain
Group Number: G-62

Name: Rishika Gudla
Roll no: 22BD1A051H
Date: 7th October 2023

- ➢ Definition of blockchain, database limitations.
- ➢ Importance of Blockchain.
- ➢ Advantages of blockchain.
- ➢ Decentralization and distribution (P2P).
- ➢ Nodes,hash,pre hash.
- ➢ Proof of work.
- ➢ Consensus algorithm.

1. https://youtu.be/uULy2rc6YDc?si=r8XOz2sEYb7QFZ2r

- Database is not secure,password can be changed or any other information can be changed. Blockchain is a secured data that cannot be altered and any change of data can be known to everyone. Once the chain is corrupted it is known to everyone who is on that network.
- Blockchain is **immutable.**
- It is distributed(P2P). Peer to Peer network, no centralized authority

2. https://youtu.be/YJyXfjbBmc8?si=KQTWXtbihrMhPvGz

- Block chain contains blocks. Each block contains data,hash and pre hash of the previous block.By this the blocks are linked to each other. The first block which does not contain any previous block hash is called genesis block
- Tampering of information in block chain is difficult because the authority is not with a single person and changing is near to impossible.

- Ledger is something where all records are stored.Similarly the block chain contains blocks of records.
- Once the data is tried to change its hash gets changed and the data after the change becomes invalid

3. https://youtu.be/ENrjn-lD1e8?si=DMaWaLZlCzki0wmt

- Block chain is present in the network of computers. The people who are connected to the blockchain through their computers and those who allow the blockchain to run on their computers are known as nodes.
- Whenever new data is added to the blockchain ,it's the work of the miners to verify whether the person adding the data has done it properly or not.
- No 3rd party is involved here.
- It is secure and protects privacy. It can be because each computer in the network has its own private key and a public address. User shares his public address, not his private key. This public address is random combination of numbers and digits
- As the number of nodes increases , hacking becomes difficult.
- Miners verify these transactions and punishment is given for false verification

4. Smart contracts:

- A smart contract is a **self-executing contract** with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

Key concepts

- Cryptographic hash and digital signature
- Immutable ledges
- P2P network
- Consensus algorithm
- Block Verification(Mining ,Forging)

Sample practice codes:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract twitter{
   mapping(address => string[]) public tweets;

   function create(string memory _tweet) public{
      tweets[msg.sender].push(_tweet);
   }

   function get(address _owner,uint i) public view returns (string memory){
      return tweets[_owner][i];
   }

}
```

Sources:

solidity documentation : https://docs.soliditylang.org/en/v0.8.21/types.html
Smart contract : https://youtu.be/pyaIppMhuic?si=w00H-Lzbm5WmY0Wf
Solidity for beginners: https://youtu.be/AYpftDFiIgk?si=HrSrJ1GvX61G5pfu
Solidity basics by rithesh modi : https://www.youtube.com/watch?v=EhPeHeoKF88&t=140s