Page No.
Date

Module.1

Introduction to blockchain

- Blockchain :

  - Decentralized, secure and efficient (public ledger)
  - Basically database that holds all of informa.

  " It is the technology that constructs a decentralized digital ledger that enables exchanges between multiple parties in a secure, immutable manner"

- Working of blockchain

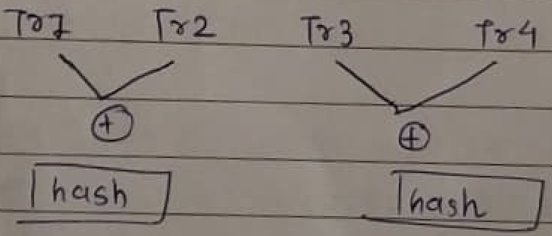
  - A transaction is requested. (sending money) (initialization)
    - (mining) [POW]
  - Transaction is ~~a~~ broadcasted to network
  - Transaction is represented online as a block
    - smart contracts
  - Network is validating the transaction using cryptography
  - Now, block is added to the existing blockchain. (hash value match)
  - Transaction is complete.
  - ledger is updated at all nodes.

Blockchain platform offers users security in a complicated encryption process known as "hashing."

✻ 25th June Blockchain

(5) merkle tree

- Generate hash of data
- Transation should be in even (Balance tree)
- If transaction is in odd then add one dumi node



- Fundamental part of the blockchain technology
- It is a methematical data structure composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block.
- It is also allows for efficient and secure verification of content in a large body of data.

→ how Merkle tree works?

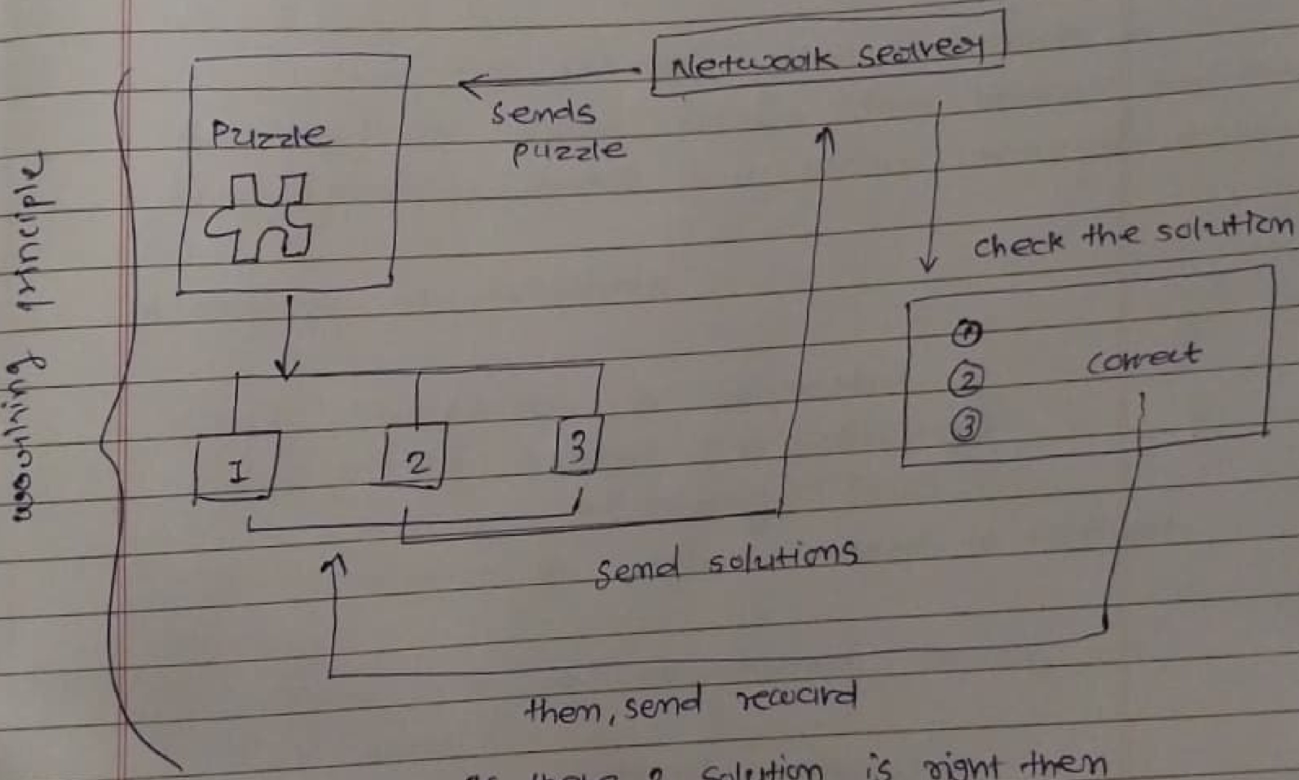
→ Benefits of merkle tree

- maintain integrity and validity of data

- PoW (Proof of work)
- original consensous algorithm

→ mining is the process of adding new block

→ miners : (mining process)



If there 2 solution is right then time used by them is considered to decide the results

→ The most famous application of PoW is bitcoin.

disadvantage :
need highly specialized compute hardware to run the complicated algorithm.

26th June

Page No.
Date

- 51 % attack :

- majority attack
- It is a case . when a user or a group of users control the majority of management.

Q (1-mark)
miners, mining process

- happens when a malicious user in a network acquires control of a given blockchain's mining capabilities.

- It implies that attackers will have more than 50% of mining power.

* Applications :

Business networks
wealth

- Assets

Tangible (cant more) Intangible (can more) Cash

↓ ↓

~~I~~ includes common thing

lands (we have record of it)

buildings ↓

machinery Property papers.

inventory pendrive

- (balance sheet) etc.

- long term asset digital proof / physical

- Ledger :

  - An important log of all transaction
  - Describe input / output

- transaction :

  - An asset transfer between participants

- Contract :

  - The terms and conditions for a transaction.

- Business context of Blockchain :-

- characteristics
  - shared
  - replicated . (duplicate / copy)
  - ledger (database)

- smart contracts
  - mutual agreement, on which every peer node need to accept / agree

* Traditional Business network

Cons

Transperancy is not available
Trust issues

to overcome these problems, blockchain is introduce

- consensus mutual agreement [smart contract]
- provenance Transperancy of history ledger
- immutability (tamper free) [unchangeable]
- finality (once committed, cannot be reversed)

↑

characteristics of blockchain

Que. Traditional v/s Blockchain

Traditional	Blockchain
Transpanency not provided	prevenence of transperency of history
everyone has different database (ledger)	It provides decentralliced public ledger
Individuals are able to change the ledger easily	It is tamper free
There is some chances of compromising ledger (trust issues)	It is ~~cat~~ once committed, then cannot be reversed

→ disadvanteges of current transaction system.

- cash can only be used in low amount transaction locally.
- Huge waiting time in the processing of transaction
- Need of third party for verification and execution of transaction make the process complex.
- If the central server like banks is compromised whole system is affected including the participants.

- Reqirements of blockchain for business

Assests - participants decides which assests to share

Identity - participants know who they are dealing with. KYC (know your customer)

- Smart conteract :

- It is a lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met.

- At the most basic level, they are programs that run as they've been set up to run by the people who developed them.

- language; solidity

5th July

Page No.
Date

How Bitcoin works ?

- **Bitcoin** (most popular)

abbreviation - BTC
sign - B

- It is a decentralized digital currency that can be transformmed on the peer-to-peer bitcoin network.

- The word bitcoin was defined in a white paper published on 31 October 2008. The currency began use in 2009.

- the purpose of bitcoin was to replace national currencies during the financial crisis of 2008.

- **Ethereum** (Second popular)

- Ethereum is a decentralized global software platform powered by blockchain technology.

- The block time of ethereum is 10 to 15 seconds.

- It has no limit for creating the block.

- It is a blockchain-based platform with the cryptocurrency Ether(ETH).

Bitcoin vs Ethereum

Bitcoin and Ethereum have many similarities but there are some long-term different visions and limitations that make them two different blockchain networks that have their pros and cons and are suitable for varying user requirements. Below are some of the differences between Bitcoin and Ethereum:

Basis	Bitcoin	Ethereum
Definition	Bitcoin (abbreviation: BTC; sign: ₿) is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network.	Ethereum is a decentralized global software platform powered by blockchain technology. It is most commonly known for its native cryptocurrency, ether (ETH).
History	The word bitcoin was defined in a white paper published on 31 October 2008. The currency began use in 2009.	Ethereum was conceived in 2013 by programmer Vitalik Buterin, and then went live on 30 July 2015.
Purpose	The purpose of bitcoin was to replace national currencies during the financial crisis of 2008.	The purpose of Ethereum was to utilize blockchain technology for maintaining a decentralized payment network and storing computer code.
Smart Contracts	Although bitcoin do have smart contracts, they are not as flexible or complete as Ethereum smart contracts. Smart contracts in Bitcoin does not have all the functionality that a programming language would give them.	Ethereum allows us to create smart contracts. Smart contracts are computer codes that is stored on a blockchain and executed when the predetermined terms and conditions are met.
Smart Contract Programming Language	Smart contracts on Bitcoin are written in programming languages like Script, Clarity.	Smart contracts on Ethereum are written in programming languages like Solidity, Vyper, etc.
Transactions	Generally, bitcoin transactions are only for keeping notes.	Ethereum transactions may contain some executable code.
Hash Algorithm	Bitcoin runs on the **SHA-256** hash algorithm.	Ethereum runs on the **Keccak-256** hash algorithm.
Consensus Mechanism	The Proof-of-Work (PoW) is the consensus mechanism used by the Bitcoin network.	The Proof-of-Stake is the consensus mechanism used by Ethereum.
Block Time	The block time of bitcoin is 10 minutes.	The block time of Ethereum is 14 to 15 seconds.
Block Limit	The bitcoin blockchain has a block limit of 1 MB.	The Ethereum blockchain does not have a block limit.
Popularity	Bitcoin is the most popular digital currency in the market to date.	Ether, native currency of Ethereum is the second-largest cryptocurrency after bitcoin to date.
Energy Consumption	Energy consumption is very high.	Energy consumption is very low as compared to bitcoin
Energy Consumption rate	Energy consumption rate of bitcoin mining system 3.2 Million household.	Energy consumption rate of bitcoin mining system 1.2 Million household.
Structure	Structure of bitcoin is simple and robust.	Structure of Ethereum is complex and feature rich
Rewards	Miner got nearly 6.25 BTC on successfully adding new block in network.	Miner got nearly 5 BTC along with same additional rewards on successfully adding new block in network.
Assets	Assets of Bitcoin is BTC.	Assets of Ethereum is Ether.