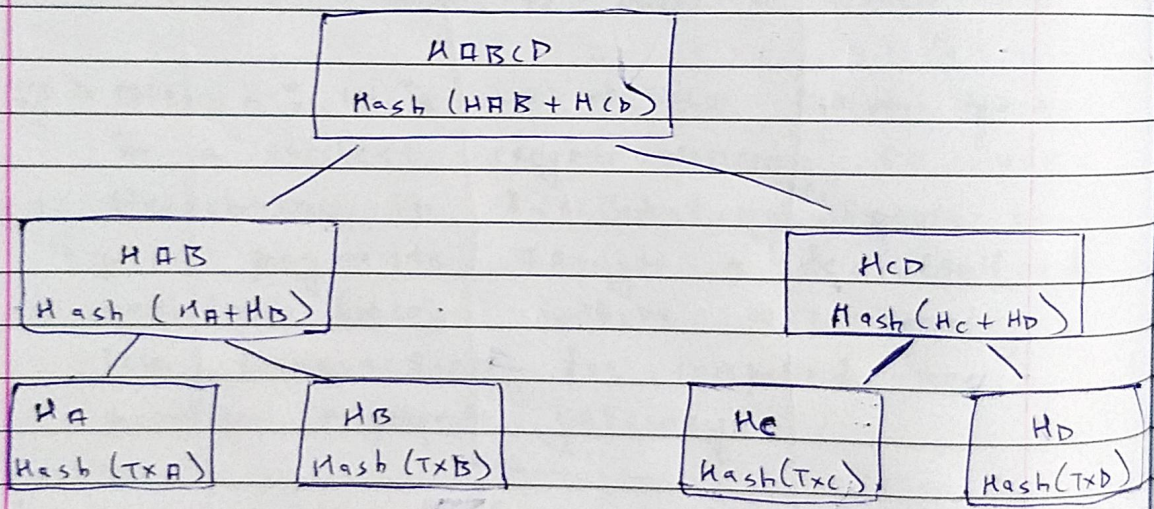
Date :
Page No.

Q1) Hash function :- It is a mathematical function that converts message of arbitary length to fixed length hash value.

-> Properties of hash function :-
- Pre-image Resistance
- Second pre-image Resistance
- Collision Resistance

-> Use of Hash function in Merkel tree structure :-



- Merkle tree is also known as Hash Tree.
- In Merkle tree, every leaf node is a hash of transactional data & non-leaf node is a hash of its previous hashes.
- Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. This hash is called the Merkle root or the root hash.

18PCE115

Date :
Page No.

Q2)

Property	Public Blockchain	Consortium blockchain	Private blockchain
Consensus determination	All Miners	selected set of nodes	one organisation
Read Permission	Public	May be public or restricted	May be public or restricted
Immutability	Almost completely tamper-proof	Potential for tampering	Potential for tampering
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permisionless	permissioned	Permissioned
Transaction Speed	slow	Lighter & Faster	Lighter & Faster
Decentralisation	Completely decentralized	Less decentralized	Less decentralized

Date :
Page No.

Q3) Define the terms :-

i) Nonce : A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing the transmitted of live and protecting against replay attacks.

ii) Hash pointer : It is a data structure that is used as a pointer to the place where some information is stored. It can be used to build a linked list.

iii) Bitcoin : It is one of the ~~first~~ ~~block~~ ~~in~~ a earliest cryptocurrency to use blockchain in facilitating peer to peer payments. Through a decentralized network, bitcoin offers a reasonably low transaction fee compared to popular payment gateways.

iv) Genesis block : Genesis block refers to the first block in a blockchain & is usually handcoded into its application's software.

v) Decentralized : ~~It~~ is the process by which the activities & an organisation, particularly those regarding planning & decision making are distributed or

delegated away from a central, authoritative location or group.

Date :
Page No.

Q4)

Proof of Work (PoW)	Proof of stake (PoS)
- The probability of mining block is determined by how much computational work is done by miners	The probability of validating a new block is determined by how large is a stake of person holds.
- To add each block of chain, miners must compete to solve difficult puzzles using their computers process power.	There is no competition power as block creators is chosen by an algorithm based on users stake.
- Hackers would need to have 51% of computat^{n} power to add malicious block.	Hackers would need to own 51% of all cryptocurrency on network which, is practically impossible.
- Specialized equipments to optimize processing power	standart server grade unit is more than enough
- Initial investment to buy hardware	Initial investement to buy stack & build reputation.

Date :
Page No.

Q5) Practical Byzantine Fault tolerance Algorithm :

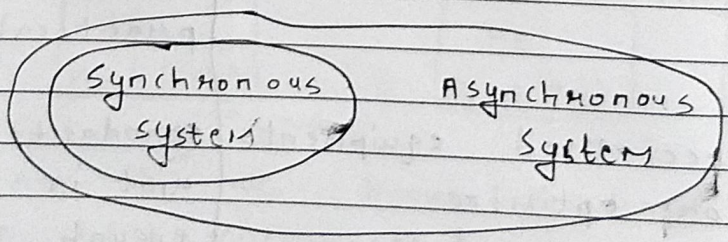
- It is a consensus algorithm introduced in late 90's by Barbara Liskov & Miguel castro.

- PBET was designed to work efficiency in asynchronous system.

- It is optimized for low overhead time.

- It's goal was to solve many problems associated with already available byzantine Fault Tolerance solutions.

- Application areas include distributed computing & blockchain



- Byzantine Fault tolerance is the first future of a distributed network to reach consensus even when some of the nodes in the network fail to respond with incorrect information. The

18DCE115

Date :
Page No.

object of BFT mechanism is to safeguard against the system failures by employing collective decision making which aim to reduce to influence of the faulty nodes.

- Advantages of PBFT:
  - Energy efficiency
  - Transmission finality
  - Low reward variance
- Limitations of PBFT:
  - Sybil attacks
  - scaling

Date :
Page No.

a6) Double spending means spending the same money twice. Transaction can be processed in two ways:-

offline : A transaction which involves physical currency or cash.
Online : A transaction which involves digital cash.

- Example: We pay Rs.5 for tea to waiter & get our tea now it is not possible for other person to use that same Rs.5. In physical currency, double spending problem can never arise but in digital cash like Bitcoin, this may occur. It opens up the possibility that the same BTC could be spent twice by its owner.

Sybil Attack is a type of attack seen in peer-to-peer networks in which a node in the network operates multiple identities actively at the same time & undermines the power in reputation systems. The main aim of this attack is to gain the majority of influence in network to carry out illegal actions in the system.

∴ Example : The recent alleged Russian interference in the US election is a type of sybil attack in which multiple fake accounts on Facebook was were operated.

Date :
Page No.

Q6) This attack falls in category of pseudo-sybil attack because the platform used (Facebook) was not compromised itself.

51% attack : When a single person or group of people gains control of over 50% of a blockchain's hashing power, it is known as 51% attack.

- Example : One can send 5 bitcoins to purchase a bike. Once the bike is delivered, logic dictates that bitcoins are to be transferred to cater for the cost of bike & can activate the attack.

On performing 51% attack ; an attacker would be able to reverse a transaction resulting in all coins used to fund the transaction being refunded.

Thus in the end, the attack will be the owner of the bike as well as the bitcoins used to buy it.

Q7) Hyperledger Fabric :

- It is an open source project from the linux foundation, is the modular blockchain framework & de facto standard for enterprise blockchain platform.

- Intended as a foundation of developing enterprise grade application & industry solutions, the open modular architecture use plug-and-play components to accomodate a wide range of use case.

-> How it works :-

- Hyperledger fabric has advanced privacy controls so only the data you want shared gets shared among "permissioned" network.

- Smart contract document the business processes which you want to accomodate with self executing terms between parties writen into lines of code.

- The code & the agreements contained there in exist across the distributed decentralized blockchain network. Transactions are trackable & irreversible creating trust between organisation.

Date :
Page No.

- This enables businesses to make more informed day-to-day decision, quicker saving time, reducing risk, etc.

-> Benefits of Hyperledger Fabric :-

- Permission network
- Confidential transactions
- Pluggable architecture
- Easy to get started.

Q8) Define the terms :

i) Ethereum :
It is a decentralized, open-source blockchain with smart contract functionality. Ether is the native cryptocurrency of the platform.

ii) ERC-20 :
It is an official protocol for proposing improvements to the Ethereum (ETH) network. ERC stands for Ethereum Request For Comment, & 20 is the proposal identifier

iii) Chain code :
It is a program, written in Go, node.js or java that implements a prescribed interface. Chain code runs in a secured Docker container isolated from the endorsing peer process.

iv) Bitcoin Script:

It is the language Bitcoin uses to do everything it can do, from sending funds from a wallet to allowing the creation of Multi-user accounts.

v) Smart Contract:

It is a computer program or transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.

Q9) Solidity is an oop language for writing smart contracts. It basically creates the trust among the peers in blockchain. The program which are compiled by solidity are intended to be run on Ethereum virtual machine.

- A Function in solidity can be difined as group of reusable code which can be called anywhere in your program.
- A function in solidity can be defined using 'function' keyword, followed by function name which is unique, list of parameters & a block of statement.
- Syntax:

```
Function Function_name (Parameters) scope returns()
{
        // block of statements
}
```

=> Pure Function:

- It ensures that they do not read or modify statement
- If a function is defined pure, then it can use revert() & require() functions to revert potential, state change if an error occurs.

Eg:

```
program solidity ^0.5.0
contract pure_demo {
    function result() public pure returns(uint sum)
    {
        uint x=5;
        uint y=10;
        sum = x+y;
    }
}
```

- View Function:
  - It ensures that they will not modify the state.
  - A view Function cannot modify the state but can look it up. Getter Methods are used by default in this.

Eg:

```
program solidity ^0.5.0
contract view_demo {
    Function result() public view returns (uint sum)
    {
        uint a=1;
        uint b=2;        // local variable
        sum = a+b;
    }
}
```

Date :
Page No.

Q10) Blockchain 4.0 is a new generation of block-chain technology. It promises to deliver blockchain as a business-usable environment for creating & running applications, bringing the technology fully mainstream.

→ Suitability of blockchain with :-

1) Smart Healthcare :
- Blockchain has a wide range of applications & uses in healthcare.
- The ledger technology facilates the secure transfer of patient Medical Records, Manages the medicine supply chain & helps healthcare researchers unlock genetic code.

2) Supply chain Management :
- Blockchain can be very helpful in the traceability & security of supplychain
- It can be used to trace a product from farm or factory to wholesalers to retailers to customers. This will improve quality of the product.

3) Education Sector :
- Aside from maintaining student records, blockchain system can be used to supervise & facillitate accredition of schools, colleges & universities, protect individual rights, and eliminate the falsification of degrees.