Page No.
Date / /

Q1 BLOCKCHAIN TECHNOLOGY - In simple terms, blockchain technology is defined as a decentralized, distributed ledger that records the provenance of a digital asset

EVOLUTION OF BLOCKCHAIN :

Nakamata conceptualised the first blockchain in 2008

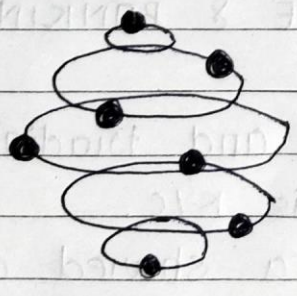
BLOCKCHAIN 1.0 - transactions (2008-2013)
- bitcoin emerges as first application

BLOCKCHAIN 2.0 - smart contracts (2013-2015)
- ethereum development

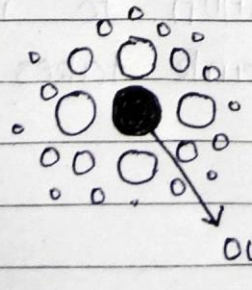
BLOCKCHAIN 3.0 - future
- emergence of NEO and IOTA

TYPES OF BLOCKCHAIN :

(I) PUBLIC BLOCKCHAIN - It removes the problems that come with centralization like less security & transparency
- information is distributed across peer to peer network instead of storing in one place.

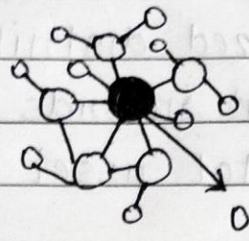


(II) PRIVATE BLOCKCHAIN - blockchain network that works in restrictive environment like a closed network, or is under control of single entity.
- operates on small networks

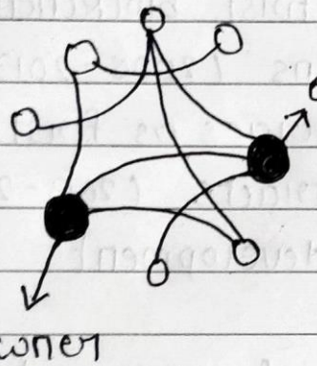


Page No.
Date / /

(III) HYBRID BLOCKCHAIN - combination of both public & private blockchain
- lets organizations setup private permission based systems along with public permissionless systems



(IV) CONSORTIUM BLOCKCHAIN - known as federated blockchain
- similar to hybrid but controled by multiple organizations
- used for member collaboration of members from multiple organizations



→ APPLICATION OF CONSORTIUM BLOCKCHAIN:

One such industry where consortium blockchain is freauently applied is FINANCE & BANKING

This one relates to insance and trading of assets. Another common application is KYC.
A group of banks creates a shared database, where all nelessary information about creditors is commonly collected and stored.
Once a band needs information to identify and ~~cross~~ guess someone, the bank takes it from distributed ledger.

Page No.
Date / /

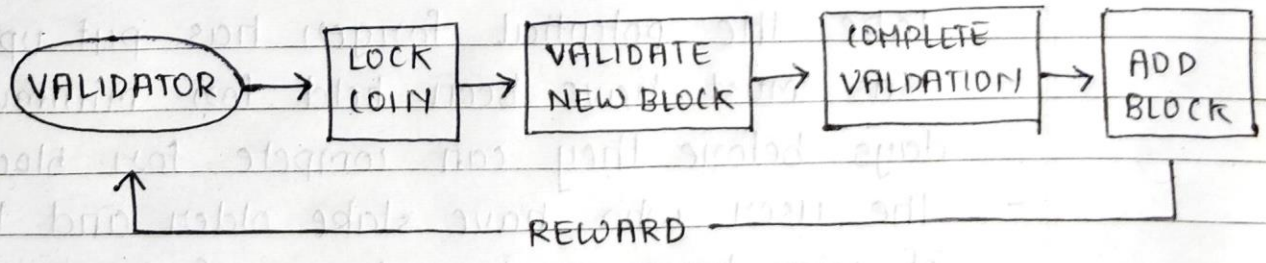
Q2 PROOF OF STAKE (POS) - It is one of the consensus method for creation of block in blockchain.

Miners in POW are replaced by validators in POS.

A validator is a crucial part of proof of stake consensus mechanism whose responsibility is to verify blocks to earn rewards.

ROLE OF VALIDATOR

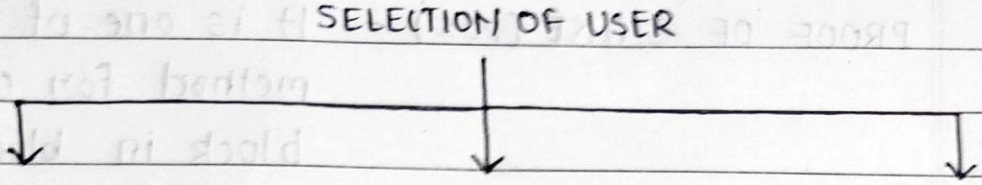
→ Validator locks up some cryptocurrency they own stake
→ It works as a bet
→ Once locking of coin is done, try to look up for new block to be added into the chain and start validating them.
→ Reward is proportionate to efforts and currency put in stake



POS NODE SELECTION METHOD :

To work effectively there should be method to select user are ~~on~~ as follows :

Page No.
Date / /



(1) By amount of stakes (account balance)
- If selection of user is done only on the bases of account balance, then it would result in permeant advantage for the richer forger who decide to forge the more of their cryptocurrency

(2) Randomized Block Selection
- This method uses the lowest hash value and the size of their stakes to select the next validator in chain
- Size of stakes are public, all nodes in the network can predict the next validator.

(3) Coin Age Based Selection
- Selects the validator on basis of "coin age" of the stake the potential forger has put up
- coins must have been held for minimum of 30 days before they can compete for block.
- the user who have stake older and larger sets of coin have greater chance of being assigned to forge next block.
- Once the user has forge block, coin is reset to zero

Page No.
Date / /

Q3 BITCOIN - It is often described as a cryptocurrency, a virtual currency or a digital currency.

It is a decentralized and ~~is~~ distributed consensus network that maintains a secure and trusted distributed ledger through process called PROOF OF WORK (POW)

→ Bitcoin realizes trust and security as it is buit on secure technology called blockchain.

Blockchain keeps bitcoin trustworthy and secure in may ways.

First, new blocks are always stored linearly and chronologically.

They are always added to the 'end' of blockchain. After a block has been added to the end of blockchain it is extremely difficult to go back, and after the contents of blocks unless a majority of network has reached a consensus to do so.

Also, trust in the network is ensured by requiring participants to demonstrate pow, by ~~solidity~~ solving a computationally difficult problems.

~~This~~ There is no central authority or trusted third party in a distributed consensus network

Page No.
Date / /

This leads to the completely new network model, as a result of which network can be open to all, the transactions can be broadcast on any medium, unencrypted, and applications can be added at the edge without getting on approval.

→ Difference between bitcoin and blockchain are:

BITCOIN	BLOCKCHAIN
- A cryptocurrency	- A ledger
- Aims at simplyfying and increasing the speed of transactions without much of restrictions	- Aims to provide a low cost, safe and secure environment for peer to peer transactions
- Limited to trading as a currency	- It is more open to changes & has a hype
- focuses on lowering the cost of influnces and reduces the time of the transaction	- It can be adapted to any change and hence it can be used in different industries
- promotes anonymity	- promotes transparency
- transfers currency b/w users	- transfers everything incl. information on property ownership rights

Page No.
Date / /

Q4 CRYPTOGRAPHY – It is techniaue of securing information and communications through use of codes so that only those person for whom the info. is intended can understand it and process the same.

In cryptography the techniaues which are used to protect information are obtained from the mathematical concepts and a set of rule based calculations known as algorithm to convert messages in ways that make it hard to decode it.

These algorithms are used for cryptographic key generation, digital singing, verification to protect data privacy, web browsing on internet & to protect confidential transactions.

HASHING – It is a cryptographic process that can be used to validate the authenticity and integrity of various types of input. It is widely used in authentication systems to avoid storing plaintext password in database

→ Hashing and cryptography are the backbones of blockchain since they constitute the foundation for the blockchain. These features make it possible for blocks to get securly linked by the other blocks, and also ensure the reliability and immutability of the data stored on the blockchain.

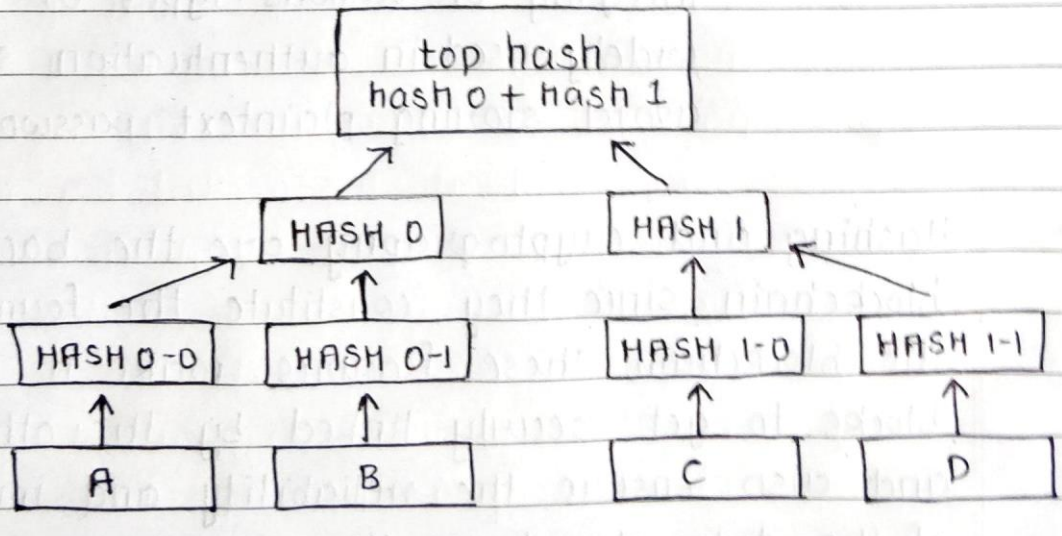
There are a huge number of applications of blockchain technology, and it is cryptography that makes all of them possible. One of the major real-world applications is cryptocurrencies

Cryptographic hash functions is an integral part of blockchain innovation. It is essentially a feature that gives security capabilities to the processed transactions, making them immutable.

Hashing is also at the center of "Merkle Trees", which is an advanced approach to blockchain hashing.

→ MERKLE TREE - It is a fundamental part of blockchain technology. It is a tree data structure where each non-leaf node is a hash of it's child nodes.

It maintains data integrity and uses of hash functions for verification and synchronization.



Page No.
Date / /

→ This structure of the tree allows efficient mapping of huge data and small changes made to data can be easily identified

→ If we want to know where data change has occurred when we can check if data is consistent with root hash and we will not have to traverse the whole structure but only a small part of structure.

→ The root hash is used as the fingerprint for the entire data.

Page No.
Date / /

Qs. A practical byzantine fault tolerance system can function on the condition that the maximum no. of malicious nodes must not be greater than or equal to one third of all the nodes in the system.

Byzantine fault tolerance can be achieved if the correctly working nodes in the network reach an agreement on their values

→ In PBFT system, when a transaction is made, the transaction details are sent to the nodes in the network

→ There may be some nodes that will approve the transactions and some nodes that won't.

→ The majority of nodes have to approve the transactions for transaction to be completed

→ There can be a default value given to missing messages i.e. we can assume that message from particular node is faculty if message is not received within certain time limit

→ We can also assign a default response if majority of nodes respond with correct value.

→ There are 2 possible problems that can arise when a node undergoes byzantine failure.

Page No.
Date / /

→ First problem is not sending a message at all.

→ In distributed system, in order for N nodes to function properly, having F nodes suffering from byzantine N-F nodes are required for quorium.

→ The second problem is when a node maliciously sends different messages.

→ let's say, among N-f nodes that achieved quorum, f were sent by byzantine failure

→ In that case, system has to be operate normally, so (N-F)-f messages should be greater than f.

$(N-f)-f > f$

$N > 3f$

→ $1/3$ is the greatest amount of faulty nodes that the system can handle.

Page No.
Date / /

Q6 HYPERLEDGER- Hyperledger is a global enterprise blockchain project that offers the necessary framework, standards, guidelines, and tools to build open source blockchains and related application for use across various industries.

Hyperledger was set up with the aim of accelarating industry wide collaboration for developing high-performance and reliable blockchain and distributed ledger based technology framework that could be used across the various industory sectors to enhance the efficiency, performance, and transaction of various industry proiesses.

Hyperledger is applied to the the industry in the following ways:

→ . Create Online Parts Marketplace by Honeywell

This is done to improve the purchasing time by cutting them to days instead of weaks.
Honeywell Aerospace has created an online part marketplace due to which now buyer needs to buy parts just like they do from an e commerce site. It also helps boost anti-contorfeit measures.

→ Cut Onboarding by IBM

IBM utilized hyperledger in their manufacturing

sector. They were able to reduce new vendor risk and improve the onboarding time from 60 days to 3 days. With it, they now onboard B2B suppliers much faster with better risk management.

→ Improve claims lifecycle by Change Health ~~culture~~ care

Healthcare claims have always been challenging experience for patients. Change healthcare have started to do it with the help of hyperledger. They want to improve transparency and also throughput of the claims process and also improve overall feasibility

→ Next Generation Credentials Platform by Sony Global Education

To take an advantage of distributed ledger technology such as hyperledger, sony is aiming to manage there credentials platform.
It will enable organizations and government agencies consortium to improve training data and education with centralized approach.

→ Improving transparency to the food supply chain by walmart.

The food supply chain is currently being transform

Page No.
Date / /

by walmart as they are bringing unprecedented transparency with hyperledger. This is one of the re renowned hyperledger fabric supply chain use case.
By using hyperledger, walmart will enable the food to be tracked at every step of the journey, bringing transparency and authenticity to the food we eat.

→ Banking Security

It can help banks to be well-equipped with the latest technologies and protect their transactions from any cyber-attacks.
It can also be used to provide seamless user experience to the user.

Page No.
Date / /

Q7.

```
pragma solidity ^0.4.16;
contract token {

    function totalSupply()
    constant returns ( uint256 supply ) {}

    function balanceOf (address _owner)
    constant returns (uint256 balance) {}

    function transfer (address _to, uint256, _value)
        returns (bool success) {}

    function transferFrom (address _from, address _to,
                           uint256 _value )
        returns (bool success ) {}

    function approve (address _spender, uint256 _value )
        returns (bool success) {}

    function allowance (address _owner, address _spender)
        constant returns (uint256 remaining) {}

    event Transfer ( address indexed _from, address indexed
                     _to, uint256 _value );

    event Approval (address indexed _owner, address
                    indexed _spender, uint256 _value );

}
```

```
contract StandardToken is Token {

  function transfer (address _to, uint 256 _value)
    returns (bool success) {

      if (balance [msg.sender] >= _value && _value > 0) {
          balance [msg.sender] -= _value ;
          balance [_to] += _value ;
          Transfer ( msg. sender, _to, _value ) ;
          return true ;
        } else { return false ; }
  }
  function transferFrom (address _from, address _to,
                         uint 256 _value)
    returns (bool success) {

      if (balance [_from] >= _value && allowed [_from]
                [msg.sender] >= _value && value > 0 ) {
          balance [_to] += _value ;
          balance [_from] -= _value ;
          allowed [_from] [msg.sender] -= _value ;
          Transfer (_from, _to, _value ) ;
          return true ;
        } else { return false ; }
    }
    function balanceOf (address _owner, uint 256 _value)
    { return balance [_owner] ;
    }
```

```
    function approve (address _owner, uint256 _value) {
        allowed [msg.spender][_spender] = _value;
        Approval [msg.spender, _spender, _value);
        return true;
    }
    function allowance (address _owner, address _spender)
    constant returns (uint256 remaining) {
        return allowed [_owner][_spender];
    }

    mapping (address => uint256) balances;
    mapping (address => mapping (address => uint256));
    uint256 public totalSupply;
}

contract ERC20Token is StandardToken {

    function () {
        throw;
    }
    string public name;
    uint8 public decimals;
    string public symbol;
    string public version = 'H1.0';

    function ERC20Token () {
        balances [msg.sender] = NUMBER_OF_TOKEN_HERE;
        totalSupply = NUMBER_OF_TOKENS_HERE;
        name = "NAME OF YOUR TOKEN HERE";
        decimals = 0;
        symbol = "SYM"; }
```

```
function approveAndCall(address _spender, uint
    256 _value, bytes _extraData)

returns(bool success) {

    allowed[msg.sender][_spender] = _value;
    Approval(msg.sender, _spender, _value);

    if(!_spender.call(bytes4(bytes32(sha3
    ("receiveApproval(address,uint256,address,
    bytes)"))), msg.sender, _value, this,
    _extraData))    { throw; }

    return true;

  }
}
```

Page No.
Date / /

Q8 Use case of blockchain technology in supply chain management with appropriate examples are:

→ SUPPLY CHAIN LOGISTICS

Friction is a major problem for modern supply chains with many go-betweens and much back and forth between partners. The result is that suppliers, providers and customers interact via 3rd party entities rather than directly with each other.

For eg. according to DHL, the promise of blockchain in supply chain logistics is that the transactions can be verified, recorded and coordinated autonomously, eliminating an entire layer of complexity from global supply chains.

→ SUPPLIER PAYMENTS

Blockchain technology promises to facilitate fast, secure, low cost international payment processing services through the use of encrypted distributed ledgers that provide trusted real-time verification of transactions without the needed for intermediaries such as correspondent banks and clearing houses.

For eg. Bext360 is using BT to better track all elements of worldwide coffee trade - from farmer to consumer. This ensures payment directly to the farmers immediately as their products are sold.

Page No.
Date / /

→ COLD CHAIN TRACEABILITY

Food and pharmaceutical products often have similar storage and sheeping needs. Blockchain allied to IOT sensors on product can record temprature, humidity, vibration and other environ--mental metrics.
For eg. one early example of blockchain ~~and~~ for food supply chain is Walmart's innovative use of technology to track the provenance and condition of its pork products coming from China. It now requires all its spinnach and lettuce suppliers to deploy the technology.

→ FOOD SAFETY

Many food safety issues, such as cross-contamina-tion, are difficult to track and isolation.
The lack of data and supply chain visibility leads to slow action when arises and well as unnecessary waste and the economic and reputational cost of recalls.
A consontium is using blockchain within supply chain tracking to ensure the supply chain has trasparency of all product movements and status
For eg. Nestle and Unilever are using blockchain to reduce time it ~~took~~ takes to pinpoint and remove the source of foodborne illness within the supply chain.

Page No.
Date / /

→ SUPPLY CHAIN FINANCE

Recently, there has been a good deal of interest around blockchain supply chain finance solutions because it can increase the efficiency of invoice processing and provide more transparent and secure transactions while increasing efficiency of invoice processing.

For eg. invoice payment terms are usually 30 days and often much longer. By combining supply chain finance and blockchain technology, you can apply smart contracts that trigger immediate payments as soon as the product is delivered and signed for.